K4

OneDome

Installation Guide

Revision History

Date	Version	Remark
Sep-24-2021	1.0	Created K4 OneDome installation guide.
Feb-08-2022	1.1	Updated for addition of Wi-Fi Interface, AP Mode, Captive Portal and LTE Controller updates. Added sample csv for Domain and Application Policies, IP Reservations.
Mar-18-2022	1.2	Updated installation rules for Radar and Spacing.

Table of Content

List of Figures

List of Tables

About OneDome Installation Guide

The K4 OneDome Installation Guide provides information on how you can install and manage the K4 OneDome.

Intended Audience

This guide is helpful for both beginner and experienced system hardware engineers who will be installing the K4 OneDome, commissioning, and monitoring the K4 OneDome.

How this Guide is Organized

This guide includes the following chapters.

1. Installing K4 OneDome. This chapter provides an introduction to the K4 OneDome and its interfaces. In addition to this, the chapter provides steps to install the K4 OneDome.
2. Commissioning K4 OneDome. This chapter provides the steps to commission the K4 OneDome.
3. Monitoring. This chapter provides the steps to monitor the K4 OneDome after the K4 OneDome physical installation.
4. Installing K4 OneDome Ethernet to SDWAN System. This chapter the information on installing the K4 OneDome Ethernet to SDWAN.
5. Debugging. This chapter provides the steps to debug and resolve issues raised by users and clients.

Convention used in this Guide

The following conventions are used throughout the guide.

1. *Italic* Figures and tables links are in *italic*.
2. **Bold** Buttons and the name of the pages are in **bold**.
3. *Reference* Reference to the section is in *italic*.

K4 Support

If you face a problem while installing or commissioning the K4 OneDome, then you can connect to the K4 support through the following channels:

- ***Mail***. Please send your detailed issues and requests to ***support@k4mobility.com***
- ***Phone Call***. To talk directly with the K4 support, call ***1-800-964-2084***.

1 Installing K4 OneDome

1.1 About K4 OneDome

The K4 OneDome is a single enclosure and independent dome. The K4 OneDome provides superior LTE and Marina Wi-Fi connectivity and magnifies the LTE / Wi-Fi radio performance up to 5x over the counterpart LTE systems. Additionally, the unique K4 SIM Selector feature and Mobility logic boost the performance up to an average of 10x more than the traditional mobile marine LTE systems. The K4 OneDome comes with the preinstalled K4 Edge service.

The single Ethernet and DC power line requirement and aptness to run below the deck without LMR cables characterizes the K4 OneDome. For more details about the K4 OneDome, see *Figure 1-1* and for the architecture, see *Figure 1-2*.

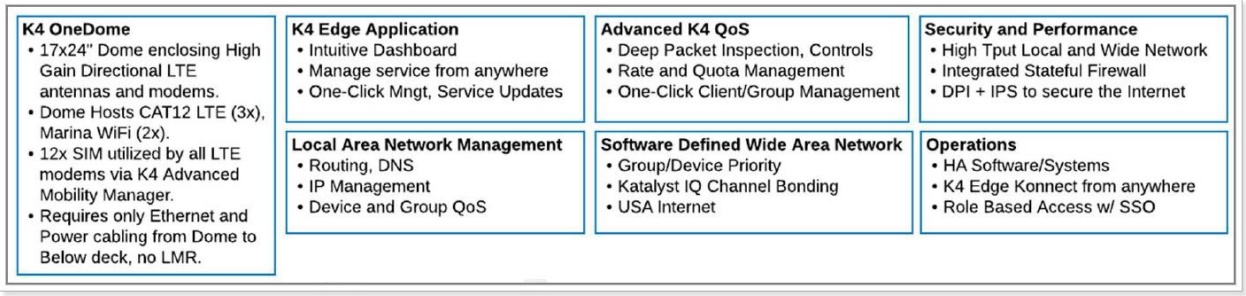

Figure 1-1 K4 OneDome Features

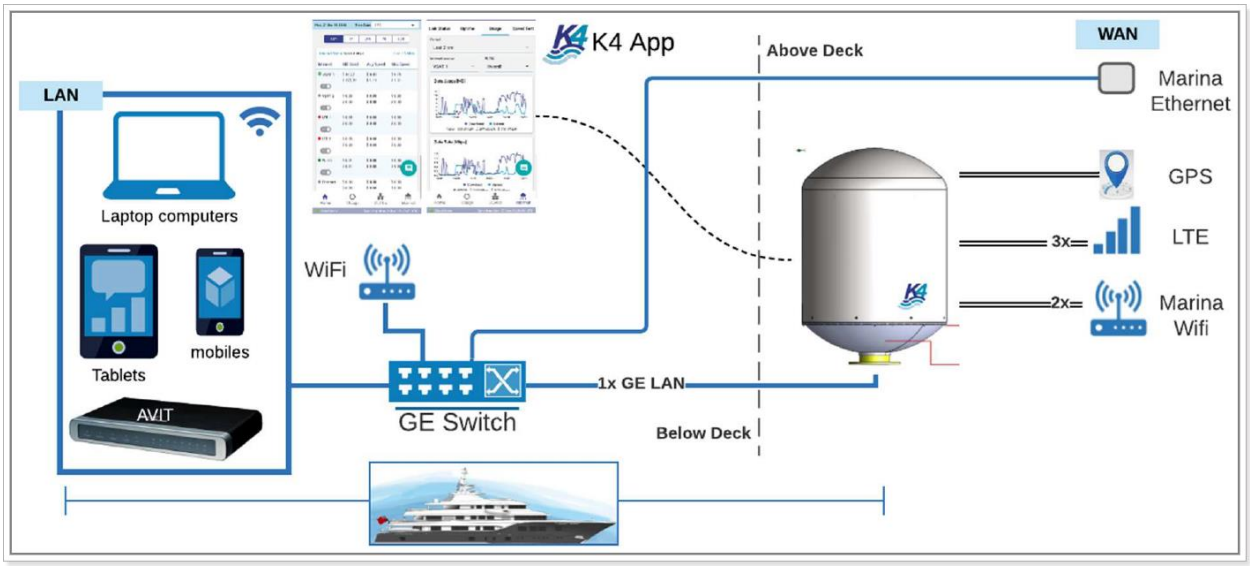

Figure 1-2 K4 OneDome Architecture

1.1.1 WAN Manager and Firewall Appliance

The K4 team will install the K4 OneDome LTE system. The K4 OneDome supports the K4 Edge service for the WAN service management. The K4 Edge is the advanced maritime WAN/Internet management system and provides an integrated platform for LAN, WAN, QoS, and Security management. You can manage the Edge service on the vessel and away from the yacht/vessel through the IOS/Android application. The K4 Edge service provides system performance visibility and traffic congestion management. The solution provides the following features:

4. Integrated WAN Radio systems with 3x LTE with 12x SIM, 2x Wi-Fi, and 1x Ethernet for Internet access. Configure the Wi-Fi as a local AP, or connect to Marina Wi-Fi to connect to the vessel.
5. Intelligent SIM selector logic supports the global LTE coverage with or without SIM change.
6. WAN channel bonding and distribution.
7. Application recognition and management.
8. QoS and Priorities for vessel access groups
9. Provides Stateful Firewall to secure the vessel.
10. Provides USA Internet access.
11. Provides IPS, Malware, Virus and Bad Actor Detection with USA Internet
12. Remote vessel access to manage the vessel by the K4 or third party.

1.2 K4 OneDome Package

The following components are packed and shipped in the corrugated cardboard box.

13. Single unit of the K4 OneDome, see *Figure 1-9*.

- Single APC BE550G Back-UPS 550VA 8-outlet Uninterruptible Power Supply (UPS) UPC.
- Two (2) cables. The K4 OneDome will have both the cables pre-terminated in the dome and run through the K4 OneDome mounting flange feedthrough. The cables will be between 10’ to 20’ in length.
- AC-DC Power Supply – MEAN WELL ENP-240 Series. 13.8VDC 17.4A – Screw Terminal module / UPC – Input 100-240VAC ~2.8A 190mm x180mm x50mm, see *Figure 1-3*.

Figure 1-3 Plug/Connector

14. 2x waterproof cord grips

15. Installation Literature

1.3 Prerequisites

Four (4) mounting studs must be available on the vessel to bolt the K4 OneDome mounting flange to the vessel. For hardware requirements, see *Table 1-1*.

Table 1-1 Requirements

Hardware	Required For	Description
1x CAT6 Ethernet cable for	IP connectivity	• For the cable specification, see MPS24A4-CMRL6-spec.pdf (showmecables.com) • The diameter of the cable cannot exceed 0.31”.
1x 2-wire 18AWG	DC power	The 2-wire DC power will connect to the K4 to provide the AC/DC Power terminal (wall wart). • For the wire specification, see M3242 SL005 Alpha Wire | Cables, Wires | DigiKey • Braided 2 wire supports easier bend and termination. • The maximum power usage is 75 watts while the average power usage is 15 watts.

1.4 Hardware Configurations

The K4 OneDome is available as a mast mounted solution, with adapter plates that interface to a variety of existing square mounting patterns. Contact your sales representative for more details about optional mounting hardware

K4 OneDome i5 Radome Mount – see Figure 1-10

The K4 OneDome is available in a flush mount radome, in the i5 form factor. This dome style can match existing TVRO domes or provides an alternate means to mount the OneDome if the additional height of a mast is undesirable.

K4 OneDome Flat Mount (Available Q3 2022)

The flush mount option allows the OneDome to be mounted directly to the deck using bolts fed from underneath or studs mounted directly to the dome base. A watertight seal is provided using a crosslinked polyethylene foam ring.

1.5 K4 OneDome Mounting Locations

The OneDome installation is straight forward, however consider the following guidelines.

1. Minimize blockage. The antenna requires a clear view of the horizon to best communicate to cellular towers. The fewer obstructions, the better the system will perform.
2. Consider the distance between your antenna and any radar. The OneDome requires that you do not mount the antenna on the same level as the radar, because the radar's energy may damage the OneDome and/or desensitize the OneDome for normal communication purposes. Most radar transmitters emit RF energy within an elevation range of -15º to +15º (see Figure 1-4). Therefore, mount the antenna outside of this elevation range and at least 3 ft (1 m) away from the radar.
3. Finally consider the OneDome antenna installation in relation to the GPS antenna, the OneDome can interfere with the GPS Antenna system. The GPS antenna should be positioned -30º to +30º above or below the radiation line of the OneDome.
4. Make sure the mounting surface is wide enough to accommodate the antenna's base (see Figure 1.5 to 1.7). Also make sure it is flat, level (within ±1°), strong enough to support the antenna's weight, and rigid enough to prevent antenna vibration.

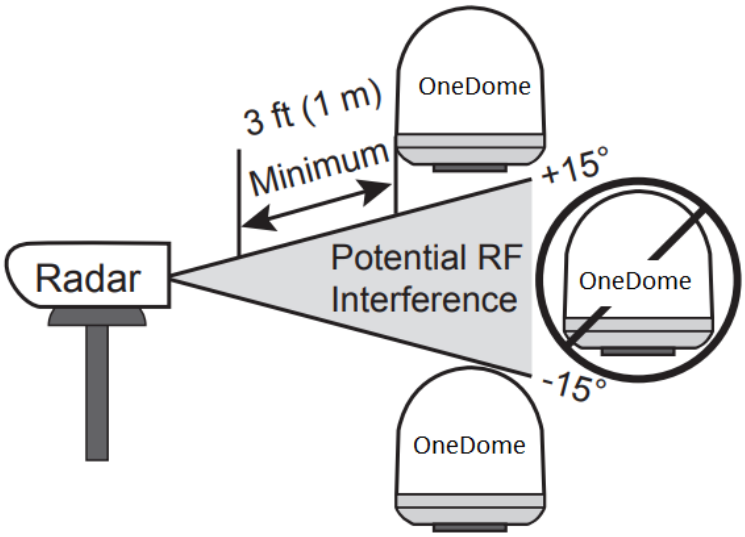

Figure 1-4 K4 OneDome installation in relation to the vessel radar.

1.6 K4 OneDome Radome Mast Mount

Figure 1-5 K4 OneDome, K4 configuration - final installed view (mounting post is powder coated gloss white).

1.6.1 K4 OneDome Specification

For specification of the K4 OneDome, see *Table 1-2*.

Table 1-2 K4 OneDome Specification

External Interfaces		Primary Limit or Specification
Dimensions		17” x 25.2” (W x H) **NOTE:** The height of the K4 OneDome is measured with the mounting post.
Weight		45 lbs
Antenna RADOME base plate		16.94” (430 MM)
RADOME curvature height		5.7” (145 MM)
RADOME height	Without curvature	15.5” (394 MM)
	With curvature	21.2” (539 MM)

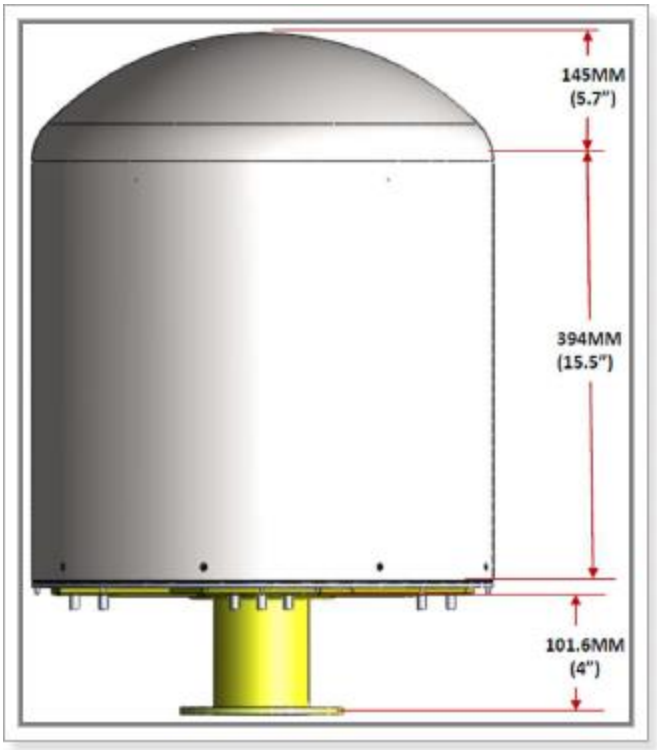

Figure 1-6 K4 OneDome Side-View[1].

The OneDome out-of-the-box comes fully pre-assembled, as shown in *Figure 1-6*. Additionally, the Ethernet (RJ45 male terminated) and Power cabling will be pre-terminated and coiled up in the box as well.

1.7 K4 OneDome Mounting Flange Specification

For specification of the K4 OneDome Mounting Flange, see *Table 1-3*.

Table 1-3 K4 OneDome Mounting Flange Specification

External Interfaces	Primary Limit or Specification
The mounting post baseplate flange	0.4” (6 MM) Thickness
Bolt/stud holes	0.5” in diameter

[1] Note that the Stainless steel mounting flange is painted gloss white.

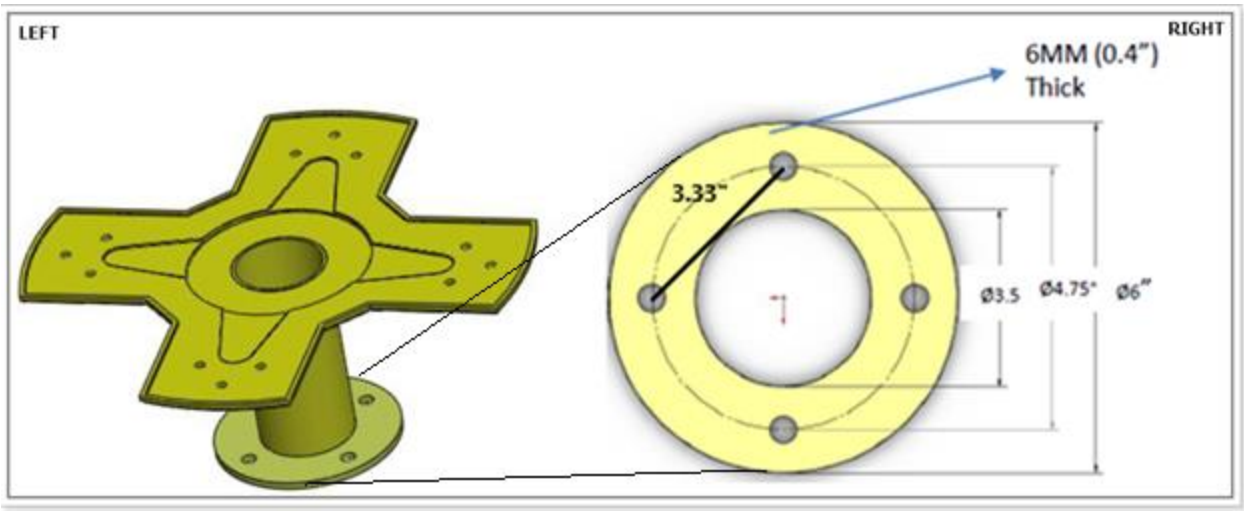

Figure 1-7 LEFT: The Mounting post/mast and RIGHT: The mounting post baseplate flange

1.8 Installing K4 OneDome

To install the K4 OneDome, perform the following steps.

1. Mount the K4 OneDome to the vessel at the mounting flange points. For dimensions, see *Figure 1-7*. The mounting flange is white powder-coated stainless steel.
2. The K4 OneDome Radome Baseplate has 2x cord-grip feedthrough cables [CAT6 Ethernet and DC Power line] and fed-through the mounting mast post with 15' to 20' outside of the K4 OneDome, see *Figure 1-8*.
3. The OneDome has a "Forward" Arrow under the Radome Baseplate, ideally this arrow and thus OneDome is positioned toward the front of the vessel, i.e., pointing to the bow of the vessel. IF this cannot be accounted for, the installer should note the "angular offset" from forward within a 10 degree of accuracy, this offset will be entered into the OneDome Management system.

   a. The Angle of the "Forward" arrow from the Bow is entered into the OneDome LTE controller page to help with LTE management.

4. The K4 OneDome Radome Baseplate has 2x cord-grip feedthrough cables [CAT6 Ethernet and DC Power line] and fed-through the mounting mast post with 15’ to 20’ outside of the K4 OneDome, see *Figure 1-8*.

NOTE: There is a punchout in which the cabling can be fed-through the side of the mounting mast.

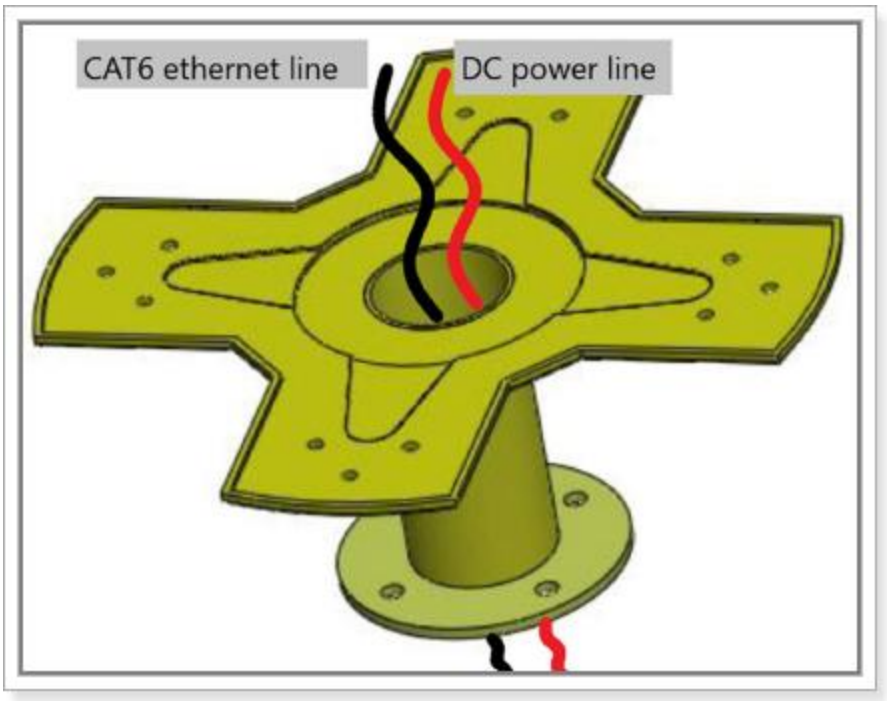

Figure 1-8 Cable fed through the K4 OneDome mounting post

NOTE: The single CAT6 Ethernet cable will terminate with a Male RJ45.

5. Run the CAT6 cable below deck and connect the below deck to the WAN access systems.

NOTE: The OneDome Ethernet interface is configured as a DHCP server providing an IP to the SDWAN system, with the SDWAN access system can include the Ethernet Switch or a core K4 Edge Server.

6. Attach/Bolt-on the OneDome mounting flange to the vessel mounting point.
7. Run the DC Power cable below deck and connect/terminate to the DC power block supplied by the K4.

NOTE: The power-block has an AC side that terminates to the K4-provided UPS system. The UPS should be connected to the vessel's AC power.

The maximum length/run of the cable should be 50'.

CAUTION: You must not plug in the OneDome AC power into the UPS until the OneDome is fully/physically installed and the AC power framework is in place. Once the OneDome is completely or physically installed, then plugin the OneDome AC power into the UPS.

The K4 OneDome is installed, see *Figure 1-9*.

Figure 1-9 K4 OneDome final installed view (mounting post is gloss white).

1.9 K4 OneDome i5 Radome Mount

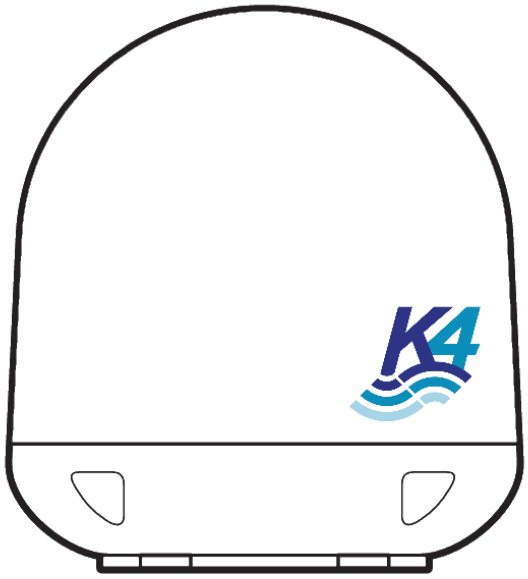

Figure 1-10 K4 OneDome, i5 configuration

1.9.1 Physical Specifications

For specification of the K4 OneDome in the i5 configuration, see Table 1-4

Table 1-4 K4 OneDome i5 Specification

External Interfaces	Primary Limit or Specification
Dimensions	24” x 25” (W x H) 61cm x 62.7cm
Weight	48 lbs.

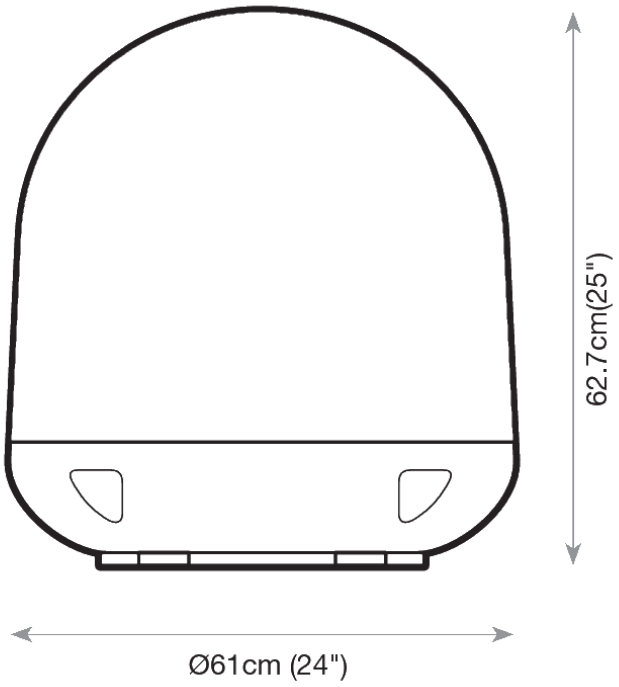

Figure 1-11 K4 OneDome i5 Configuration Dimensions

The OneDome comes fully assembled out of the box, as shown in Figure 1-10. Additionally, the Ethernet (RJ45 male terminated) and power cabling will be pre-terminated and coiled inside of the i5 dome.

NOTE: Before installing the antenna, open the radome and feed the power and data cables through the opening in the mast and out of the bottom of the i5 dome.

1.9.2 K4 OneDome i5 Mounting

For specification of the K4 OneDome i5, see *Table 1-5*. Use the dimensions to create a mounting template with 5 holes. Create a square the size of the mounting hole spacing, then draw straight lines from opposite corners to find the center.

Table 1-5 K4 OneDome i5 Mounting Specification

External Interfaces	Primary Limit or Specification
Mounting hole spacing	9” square (22.86cm)
Mounting hole diameter	(10mm)
Center hole diameter	(80mm)
Bolt	4x M8 – length determined by installer

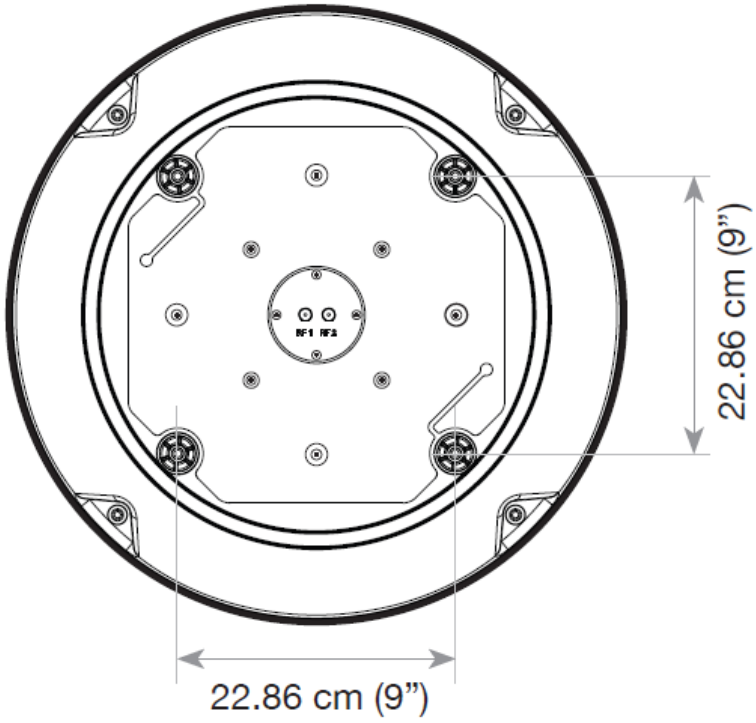

Figure 1-12 i5 dome mounting dimensions

Referring to the mounting template, mark where antenna will be mounted on board (it must be a flat surface) or on a separate power tower. Drill 5 holes per the mounting template, as shown in

the following figure. Use a hole saw to create a hole large enough for the cables to pass through in the center hole.

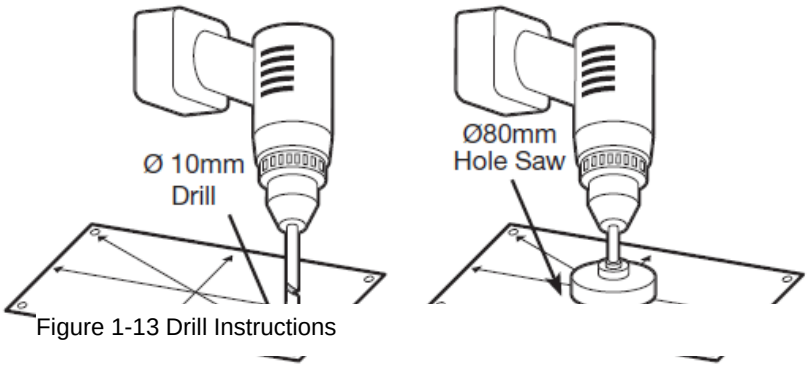

Figure 1-13 Drill Instructions

1.9.3 Installing K4 OneDome i5

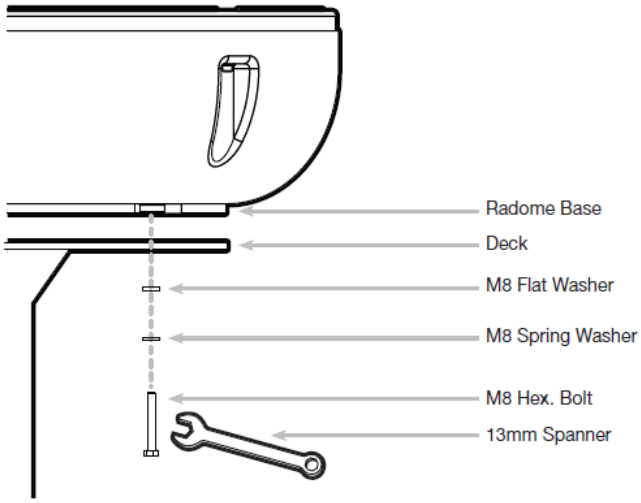

Figure 1-14 i5 dome mounting

To install the K4 OneDome i5, perform the following steps.

1. Mount the K4 OneDome as shown in Figure 1-14 i5 dome mounting*Figure 1-14,* passing M8 bolts through the deck or mounting surface and into the threaded holes in the base of the i5 dome.

2. 4x Bolts are required to attach the OneDome to the Vessel. Utilize stainless steel M8 Bolts/Nuts with locking washers, and with the length determined by the installation requirements. The 4x Holes are nominally 10mm in size.
3. The OneDome has a “Forward” Arrow on top of the Radome Baseplate, ideally this arrow and thus OneDome is positioned toward the front of the vessel, i.e., pointing to the bow of the vessel. If this cannot be accounted for, the installer should note the “angular offset” from forward within a 10 degree of accuracy, this offset will be entered into the OneDome Management system.

NOTE: When the dome is off, note the location of the bow/forward label.

   a. The Angle of the “Forward” arrow from the Bow is entered into the OneDome LTE controller page to help with LTE management.

4. The K4 OneDome Radome Baseplate has 2x cord-grip feedthrough cables [CAT6 Ethernet and DC Power line] and fed-through the mounting mast post. These cables should pass through the mast post and out the bottom of the i5 dome.

NOTE: The single CAT6 Ethernet cable will terminate with a Male RJ45.

5. Run the CAT6 cable below deck and connect the below deck to the WAN access systems.

NOTE: The OneDome Ethernet interface is configured as a DHCP server providing an IP to the SDWAN system, with the SDWAN access system can include the Ethernet Switch or a core K4 Edge Server.

6. After cables are connected, attach/Bolt-on the OneDome mounting to the vessel mounting pointS.
7. Run the DC Power cable below deck and connect/terminate to the DC power block supplied by K4.

NOTE: The power-block has an AC side that terminates to a UPS system. The UPS should be connected to the vessel’s AC power.

The maximum length/run of the cable should be 50’. Longer distances require a power supply capable of sourcing more current. Contact for sales manager to learn more about these install options.

CAUTION: You must not plug in the OneDome AC power into the UPS until the OneDome is fully/physically installed and the AC power framework is in place. Once the OneDome is completely or physically installed, then plugin the OneDome AC power into the UPS.

The K4 OneDome is installed.

1.10 K4 OneDome Radome Flush Mount

The OneDome flush mount configuration will be available Q3 2022.

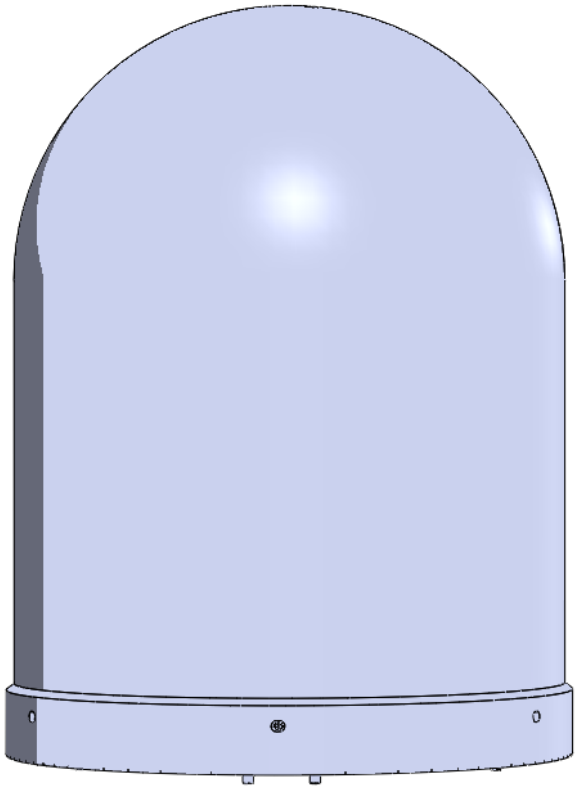

Figure 1-15 OneDome Flush Mount

2 Commissioning K4 OneDome

The OneDome is designed to provide high performing LTE connectivity while providing simple installation steps to add to your vessel SDWAN systems. The OneDome has limited configurability, however does provide extensive monitoring of IP and LTE data usage. To access the OneDome one must use a laptop with using a common Web Browser, or can utilize the K4 Edge App that runs on IOS/Android platforms.

The steps specified to commission the OneDome are defined here and performed using a subset, the Configuration Wizard. The OneDome is pre-configured such that the installer can plug in the OneDome and go.

However, to login to the OneDome, the technician must have credentials. Please, ask K4 or the Distributor for the information and then you can proceed.

2.1 Getting Started

2.1.1 Verifying OneDome Power and Ethernet

Before getting started, you must ensure that the OneDome is installed and powered up as defined in the previous section. If there is some doubt, then audit the system, and it is reasonable to power cycle the OneDome before starting. The proper power cycle procedure is to disconnect the OneDome AC Power plug from the UPS for 20 seconds and then re-insert. The OneDome will take 5 minutes to power up. The step assures a clean reboot and power up; short power loss/hits will not provide a clean restart of the system.

If the K4 OneDome is properly powered up, then you must verify the Ethernet link from the OneDome is operating as intended.

To verify the Ethernet link, perform the following steps.

1. Connect a laptop Ethernet port to the K4 OneDome RJ45 Ethernet cable, see *Figure 2-1*.

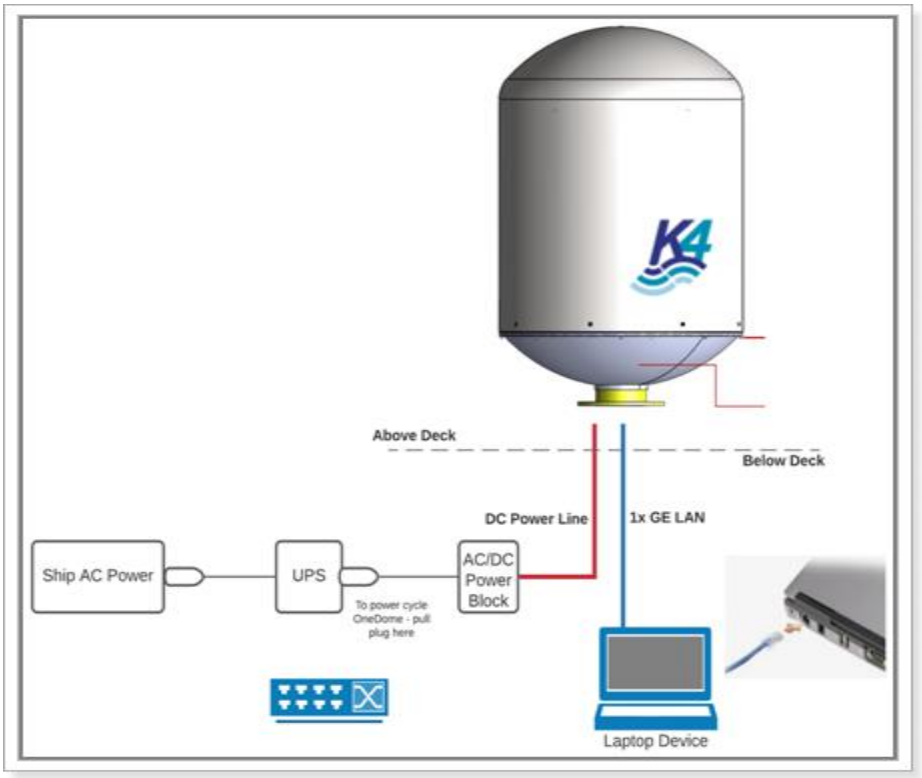

Figure 2-1 K4 OneDome Connection

The laptop Ethernet port should be configured for DHCP Client services and will request an IP from the OneDome.

2. To verify whether the Ethernet link is active in windows, click the **Internet Access** icon, and then click **Network Status**, check the **Ethernet** status; the Ethernet link should be up and 1000 Mbps.

   The K4 OneDome by default will assign the IP address within the 192.168.231.0/24 space.

3. To verify the IP address in Windows, click the **Internet Access** icon, click **Network Status** and then click on the active connection. The IP information is displayed.

If the Ethernet link and IP are assigned, then the technician can now login to the K4 OneDome.

2.1.2 Log On to K4 OneDome

This section describes how to log on to the K4 OneDome Edge Portal.

To log on to the K4 OneDome Edge Portal, perform the following steps.

1. You must ensure that the laptop is connected directly to the K4 OneDome Ethernet cable. For details, see *Verifying OneDome Power and Ethernet* on page *31*.
2. Open a modern web browser.
3. Enter the authentic URL of the K4 Edge Configuration Wizard in the address bar of a browser.

   Or,

   Enter http://10.255.1.254/ in the address bar of a browser.

   The **Login** page appears, see *Figure 2-2*. To enter data in the respective fields, see *Table 2-1*.

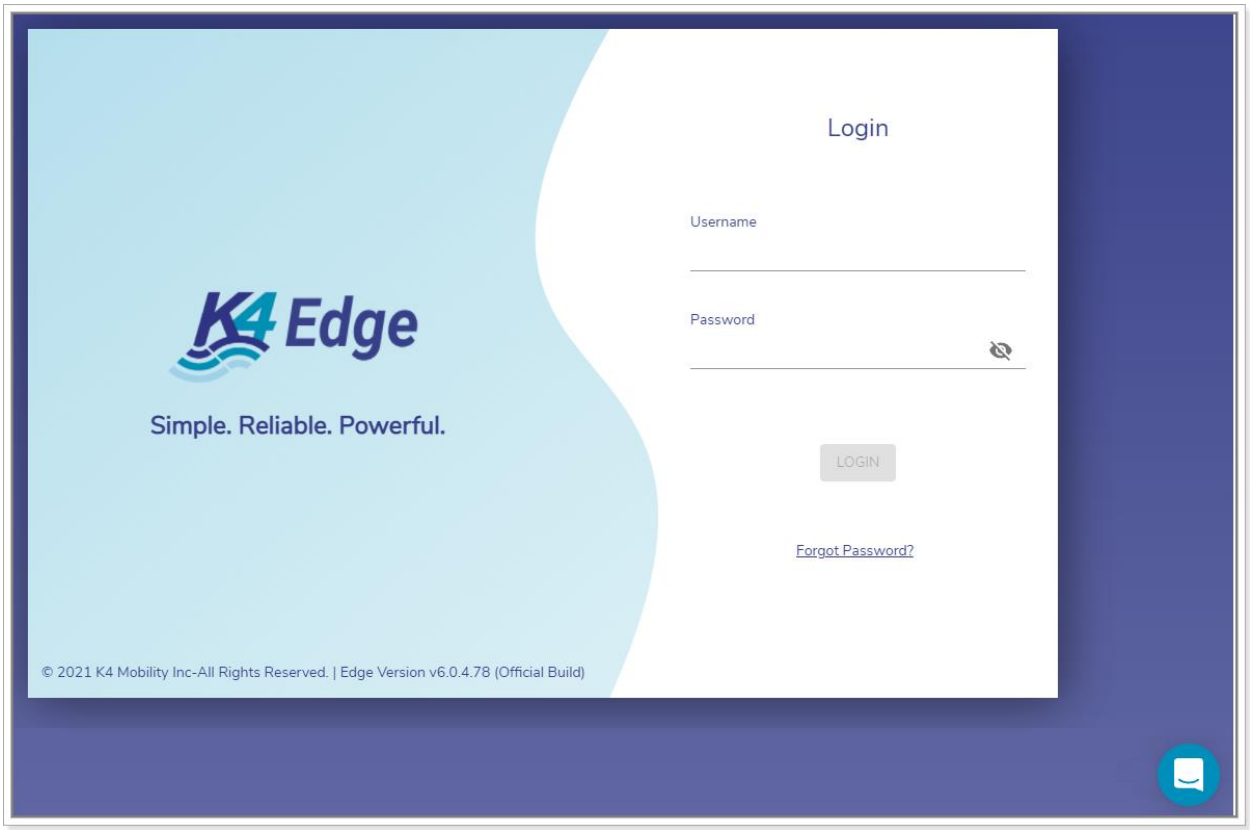

Figure 2-2 Login Page

Table 2-1 Login Information

Fields	Description
Username	Enter your username or login ID.
Password	Enter your login password

The **LOGIN** button becomes available.

4. Click **LOGIN**.

If this is your first time logging into the K4 OneDome with the given credentials, it is mandatory to configure the security questions. Therefore, the **Security Questions** pop-up window appears, see *Figure 2-3*.

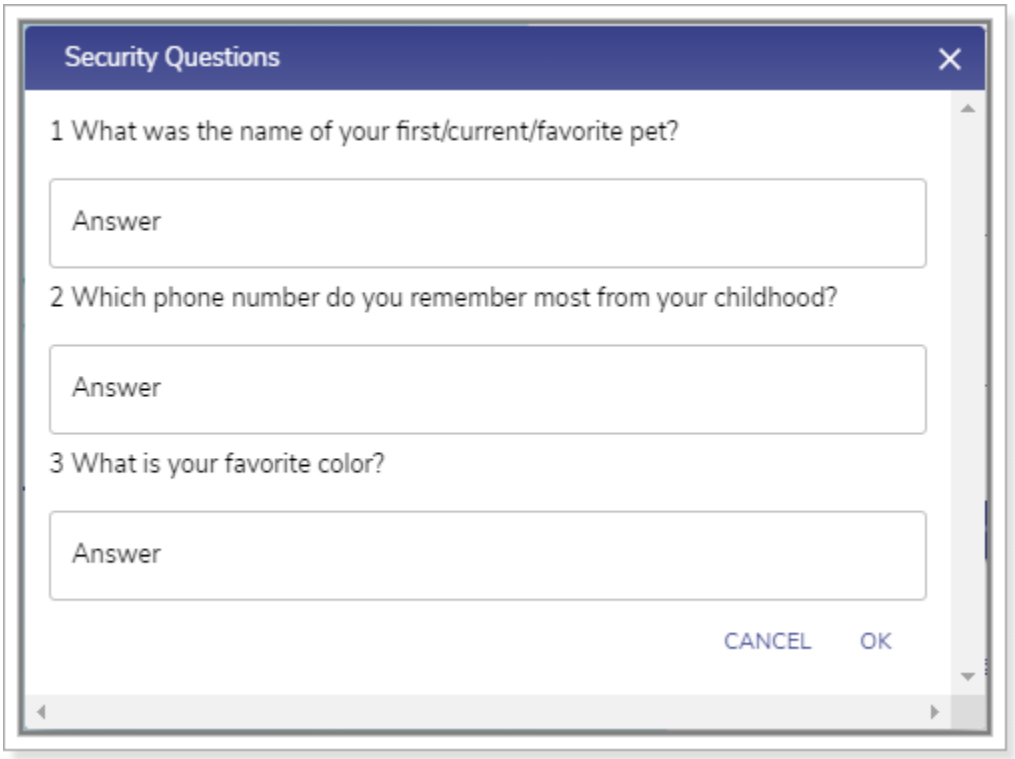

Figure 2-3 Security Questions

It is mandatory to answer the entire security question. Once the security questions are answered, save the answers or note down the answers or remember the answers and then click **OK**.

NOTE: Security questions intend to validate the user. While resetting the login password, you will be asked the security questions. You are required to answer the security questions correctly. You can refer to the answers that you have saved. An incorrect answer may lead to restricting the access of the K4 Edge server.

Figure 2-4 Home Page

Once you complete the security questions/login, the landing/homepage for the k4 OneDome, the K4 Edge Configuration Wizard appears. The OneDome comes pre-configured. Therefore, it does not require customization to the vessel outside of possible changes to the “Access Network” configuration (the 192.168.231.0/24 network). This may need change if that network conflicts with other vessel networks.

All other configurations are standard and should not be changed without consultation with K4 Mobility.

To understand the home page, see *Figure 2-5*.

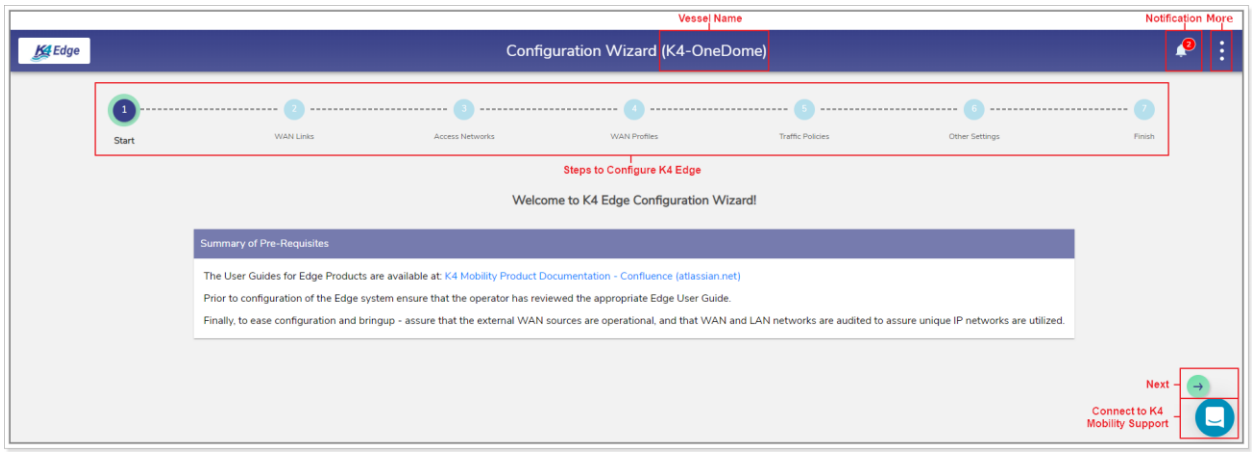

Figure 2-5 Classification of Home Page

The K4 Edge Configuration Wizard page includes the following sections.

- Vessel Name. The name of your vessel is displayed at the top of a page.
- Notification. This displays the system alerts.
- More. This includes additional configuration options.
- Steps to configure the K4 Edge.

2.1.3 Logout

To logout from the wizard, click the vertical ellipsis and then click **Logout**, see *Figure 3-2*.

Perform **Audit WAN Links**.

2.2 Audit WAN Links

The K4 OneDome should have 3x LTE links and 1x Wi-Fi Link available. The configuration and setup of the LTE links are completed by default and do not require change. The marina Wi-Fi WAN link will be available in a future release.

To view details about the WAN links, perform the following steps.

1. Click on the **Start** page or click **WAN Links**. The **WAN Links** page appears, see *Figure 2-6*.

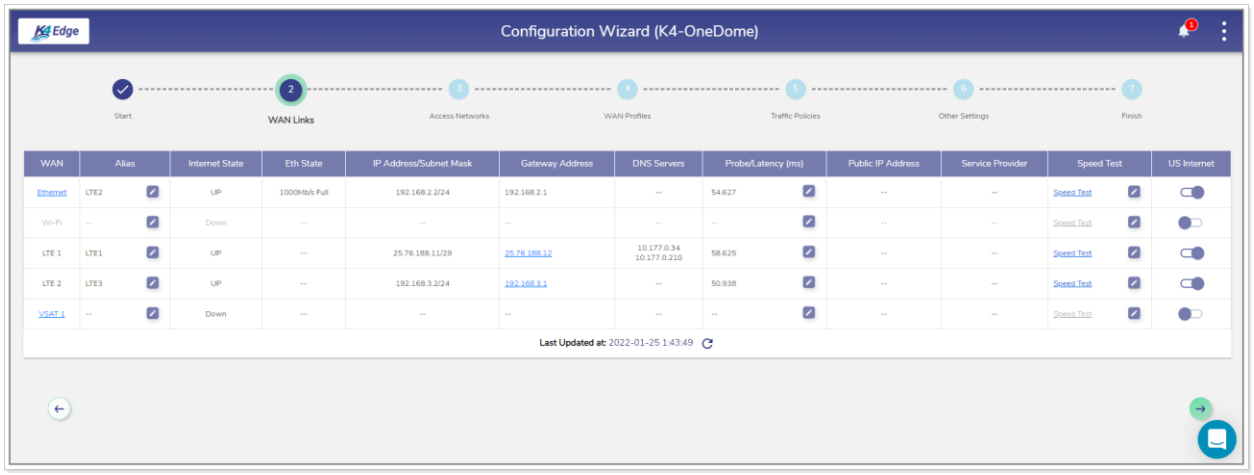

Figure 2-6 WAN Link Page

NOTE: Initially, the WAN Link page with the specified information appears. Once, the WAN links are configured, details of the WAN links become available.

Initially, on server installation, AP Mode is enabled by default and the Marina Wi-Fi is unavailable. This allows us to use the on-board Wi-Fi on EdgeOne servers to be used as a Wi-Fi access point connected to the untagged VLAN on the LAN-side (instead of a WAN-side Wi-Fi client). For more details, see *Enabling AP Mode* on page *107*.

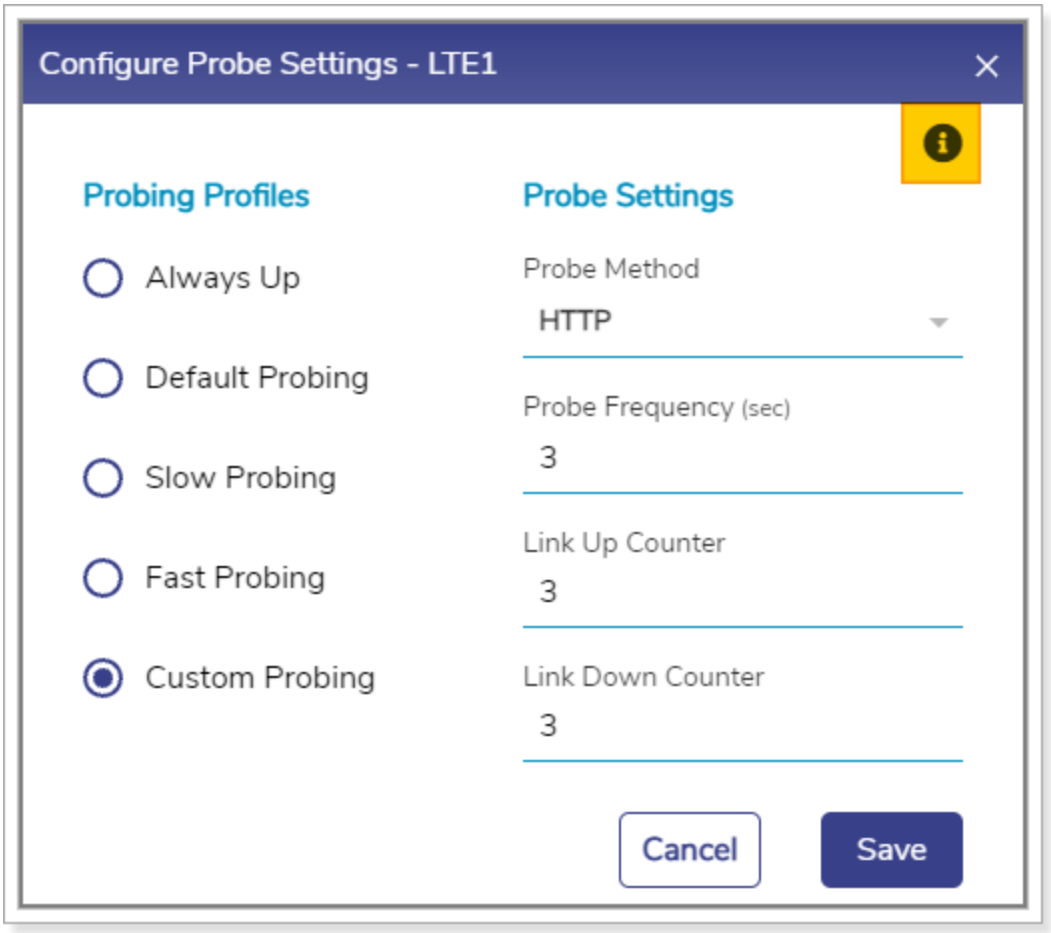

Figure 2-7 Configure Probe Settings

Return

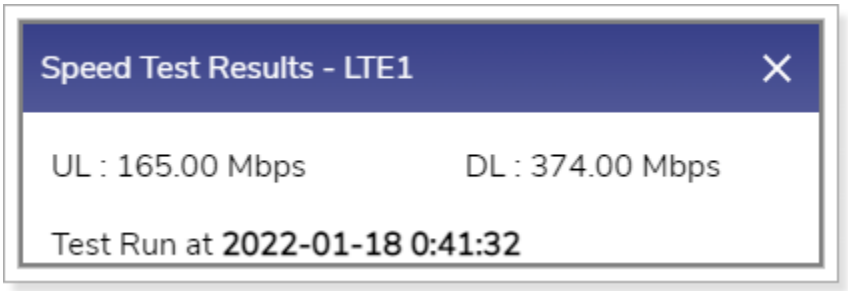

Figure 2-8 Speed Test Result

Return

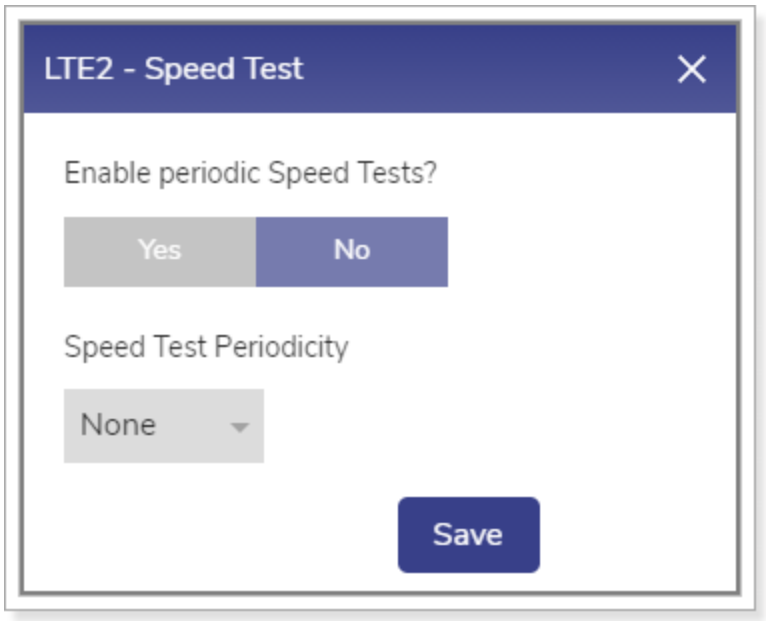

Figure 2-9 Enable Periodic Speed Test

Return

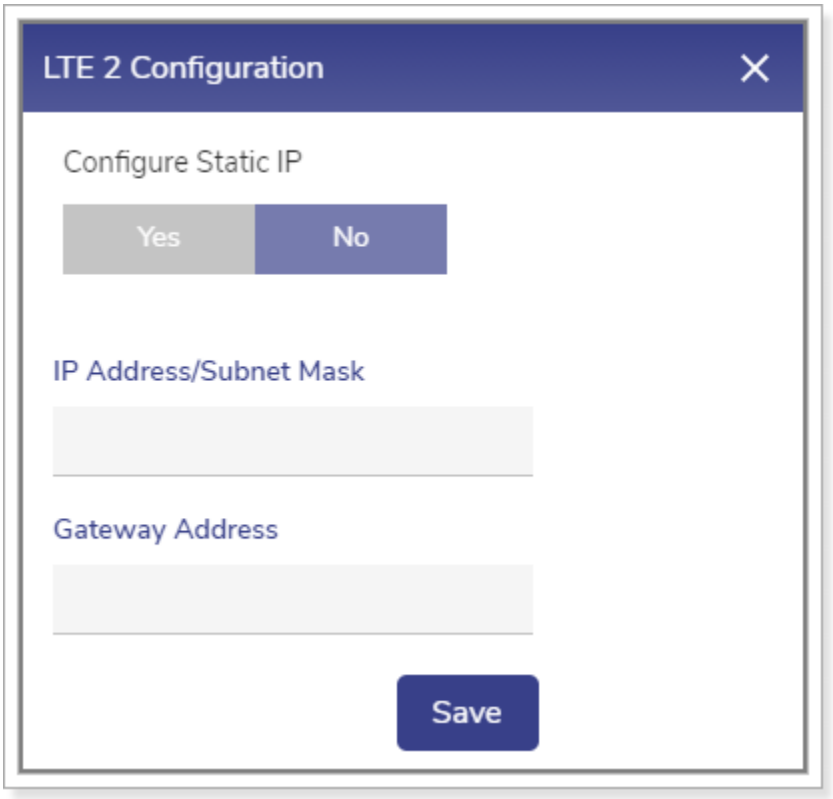

Figure 2-10 Static IP Configuration of LTE

Return

If the status of the WAN link is **Up**, then the various details such as – WAN link state of the link, IP address or Subnet Mask populate on the WAN Links page. For details, see *Table 2-2*.

Table 2-2 WAN Links Information

Fields	Description	Configuration
WAN	This indicates the WAN links that are available on the vessel. You can configure the static IP address of a WAN link as the Static IP has advantages and the following are a few advantages. • Easy to manage with DNS. • It would be easier to work remotely through a VPN or other remote services using the WAN link. • It is reliable to access the geo-location based services using the WAN link. • It is reliable for audio and video communications through VoIP using the WAN link. The K4 OneDome comes with the following pre-installed K4 EdgeOne boxes. • LTE1 is pre-configured as the parent K4 EdgeOne box of the K4 OneDome and is accessed to connect to the K4 OneDome. • LTE2 and LTE3 are pre-configured as the child K4 EdgeOne box.	**To configure the static IP of a WAN link, perform the following steps.** 1. Click a WAN Link. The WAN Configuration pop-up window appears. For LTE, see *Figure 2-10*. 2. Click **Yes** in the **Configure Static IP** field. 3. Enter the IP address and subnet mask number in the **IP Address/Subnet Mask** field. 4. Enter the gateway address in the **Gateway Address** field. 5. Click **Save**.
Alias	Alias is pre-configured for the K4 OneDome product.	**To configure the alias name, perform the following steps.**

Fields	Description	Configuration
	You can modify the alias name to the entire WAN link.	1. Click  corresponding to the WAN link. 2. Enter a unique alias name of your choice. 3. Click  . Alias name of the WAN is saved. Or, To exit without giving an alias name, click  .
		If the AP Mode is enabled, you cannot configure the alias name of the Wi-Fi. To verify whether the AP is enabled and the Marina Wi-Fi is unavailable, point the mouse to the  corresponding to the Wi-Fi. If the message **Wi-Fi is an AP mode** is displayed, then the AP is enabled and the W-Fi is unavailable.
Internet State	This indicates the current status of the WAN link. Following are the statuses of the WAN link. • Up. This indicates that internet connectivity is available on the vessel. • Down. This indicates that internet connectivity is not available on the vessel. If the LTE link of the parent K4 EdgeOne box is down and the LTE links of the child K4 EdgeOne box is up, then the K4 OneDome is accessible as the child K4 EdgeOne are up.	NA
Eth State	This indicates the maximum capacity of the respective	NA

Fields	Description	Configuration
	Ethernet cable connected to the server. The maximum capacity should be 1000Mb/s FD.	
IP Address/Subnet Mask	This indicates the address of the network, host or device address, and subnet number.	NA
Gateway Address	This indicates that the internet modems and switches on the VLANs can be reached through the gateway address. The hardware is provided by the respective companies or vendors. The K4 boxes connect to the network of the companies or vendors to establish internet connectivity on the vessel.	Click the IP address link. You will be routed to the URL of the company to procure details and services (data consumed by the WAN link and signal strength etc.) offered by the respective company or vendor. To procure details and services (data consumed by the WAN link and signal strength etc.) offered by the respective company or vendor, click  . The pop-up window appears. Enter the required details in the respective fields and click **Save**. You will be routed to the URL of the company.
DNS Server	This indicates the initial DNS used by the device to convert the name of the host to an IP address. However, a maximum of three DNSs' can be configured.	NA
Probe/Latency (ms)	Latency indicates the delay between the action and response in milliseconds. **NOTE:** Latency is available for the WAN link whose status is **Up**.	**To configure the probe settings, perform the following steps.** 1. Click  corresponding to the WAN link. The **Configure Probe Settings** pop-up window appears, see *Figure 2-7*. 2. Click a probing profile in the **Probing Profiles** field.

Fields	Description	Configuration

	You can configure the probe settings for the WAN link.	To procure details about the probing profile, point the mouse to . Details about the probe profiles become available.
		To disable the probe, select the **Always Up** profile of the profile.
		Disabling the WAN link probe will expose the following threats.
		• Reduce the probe rate to a few times an hour
		• The speed test will be disabled
		• It will also impact the WAN link usage and reliability.
		Therefore, it is highly recommended that don't disable the probe. However, the WAN link can be disabled for high costs low priority links.
		3. Configure the following probe settings in the **Probe Settings** field.
		• Probing Method. Click one of the following probing methods.
		  • ICMP. This engages lesser bandwidth to do a probe. However, many WAN access networks may block ICMP to evade the potential security threat.
		  • HTTP.
		• Probe Frequency (sec). Enter the probe frequency at which the probe is to be performed.
		If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down values will become available.
		To define the probe frequency, you must select the **Custom Probing** profile of the probe and enter the

Fields	Description	Configuration
		probe frequency within the range of 1 to 3600. • Link Up Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the WAN link is up. If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down values will become available. To define the link up counter, you must select the **Custom Probing** profile of the probe and enter the link up counts within the range of 1 to 100. • Link Down Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the WAN link is down. If you select the **Default Probing**, **Slow Probing**, and **Fast Probing** profile of the probe, then the probe frequency and link up and down values will become available. To define the probe frequency, you must select the **Custom Probing** profile of the probe and enter the link down counts within the range of 1 to 100. 4. Click **Save**.
Public IP Address	This indicates the public or global IP address used to access the internet. The public or global IP address is assigned by the internet service provider (ISP).	NA
Service Provider	This indicates the name of ISP.	NA

Fields	Description	Configuration
Speed Test	You can measure the performance of a specific WAN link in real-time.	Click **Speed Test**. The **Speed Test Results** pop-up window appears, see *Figure 2-8*. The speed test result will include the upload and download speed in Mbps and time stamp i.e. date and time when the speed test was performed. The speed test can be performed for the WAN link whose state is Up. **To enable the periodic speed test, perform the following steps.** 1. Click corresponding to the WAN link. The **Speed Test** pop-up window appears, see *Figure 2-9*. 2. Click **Yes** in the Enable periodic Speed Tests? field. The Speed Test Periodicity field becomes available. 3. Click the interval or periodicity when the speed tests are to be performed. 4. Click **Save**.
US Internet	To allow access to the US internet.	Switch on the US Internet.

To update the page, click (Refresh).

Perform **Audit Access Networks**.

2.3 Audit Access Networks

You can configure the following three types of access networks supported by the K4 OneDome.

16. Connected Networks
17. Managed Connected Networks (Traditional VLAN-s)
18. Managed Routed Networks

However, a single native (non-VLAN) network is configured as 192.168.231.0/24. The typical K4 OneDome deployments will have the K4 OneDome connected back to an EdgeServer/One or SDWAN system that provides LAN services. However, the K4 OneDome can provide this functionality as well and is kept for completeness.

To configure the connected network, perform the following steps.

1. Click  on the **WAN Links** page or click **Access Networks**. The **Access Networks** page appears, see *Figure 2-11*.

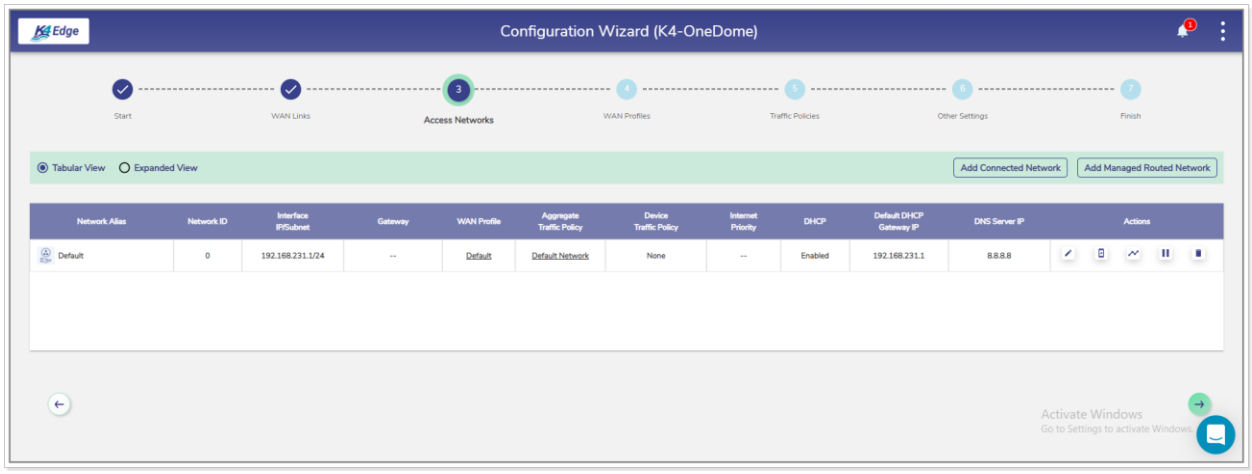

Figure 2-11 Access Networks

NOTE: Initially, the **Default** network is available. You can configure multiple networks. Once, the networks are configured, the networks become available on the **Access Networks** page. See *Figure 2-12*.

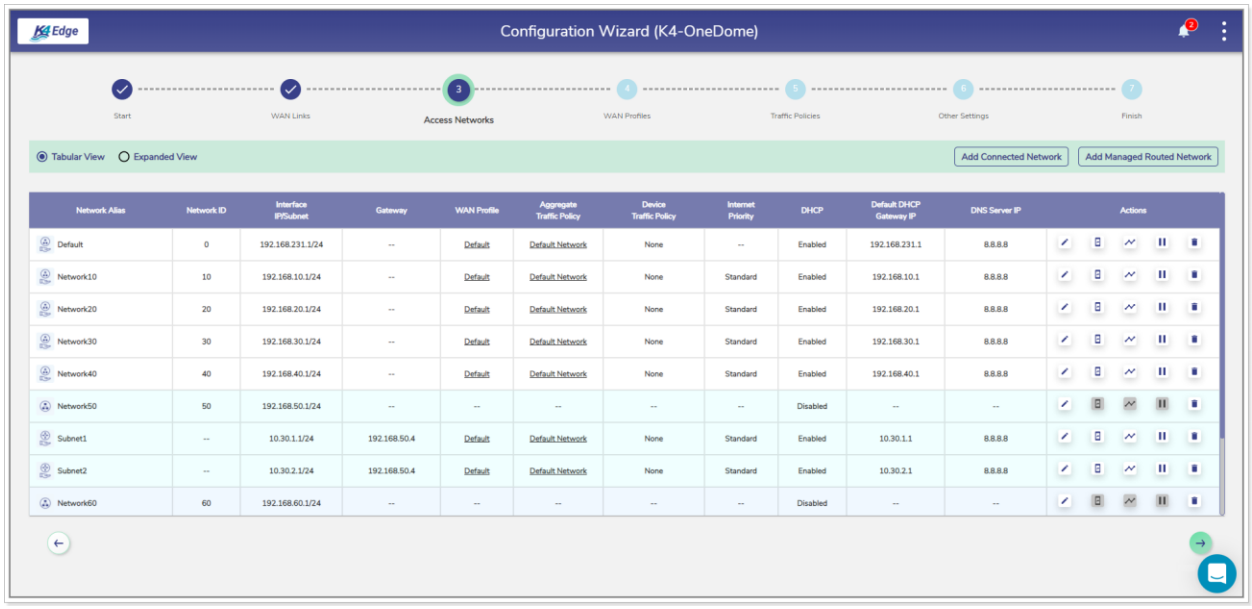

Figure 2-12 Configured Access Networks

Return

1. Click **Tabular View**. By default, details about the network are available in the Tabular form, see *Figure 2-12*.

   Or,

   Click **Expanded View**. The details about the network are available in the expanded form, see *Figure 2-13*.

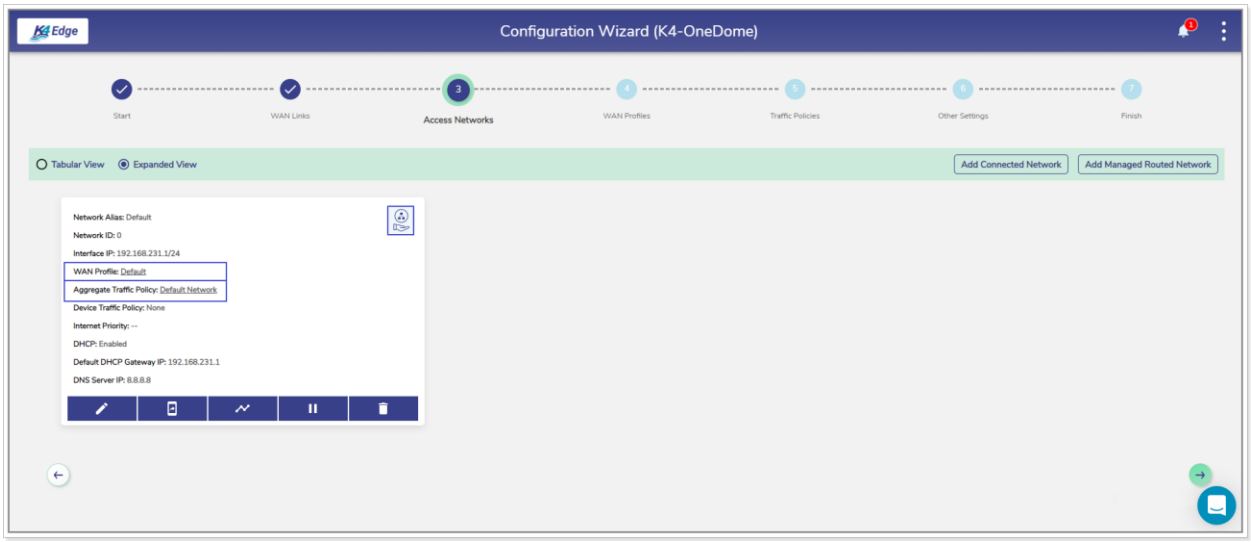

Figure 2-13 Expanded View

The connected networks are displayed with a color background.

To view the network type, point the mouse at the upper right corner of the network, see *Figure 2-13*.

To modify details of the WAN profile of the network, click the WAN profile link, see *Figure 2-13*. The **WAN Profiles** page appears. For details, see *Audit WAN Profiles* on page *66*.

To modify details of the aggregate traffic policy, click the aggregate traffic policy link, see *Figure 2-13*. The **Traffic Profiles** page appears. For details, see *Audit Traffic Policies* on page *71*.

2. Click **Add Connected Network**. The **Add Connected Network** page appears, see *Figure 2-14*.

NOTE: This indicates that configuring multiple local networks to be used by the users' basis on the hierarchy. This is an example.

You can configure the local network for the crew of the vessel, a local network for the captain of the vessel, and a local network for the owner of the vessel distinctly.

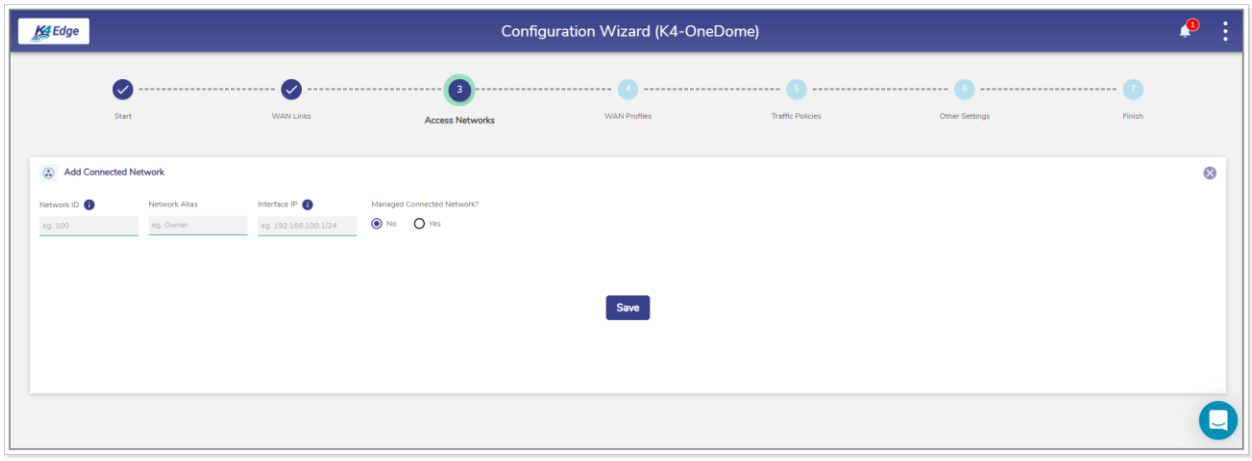

Figure 2-14 Add Connected Network

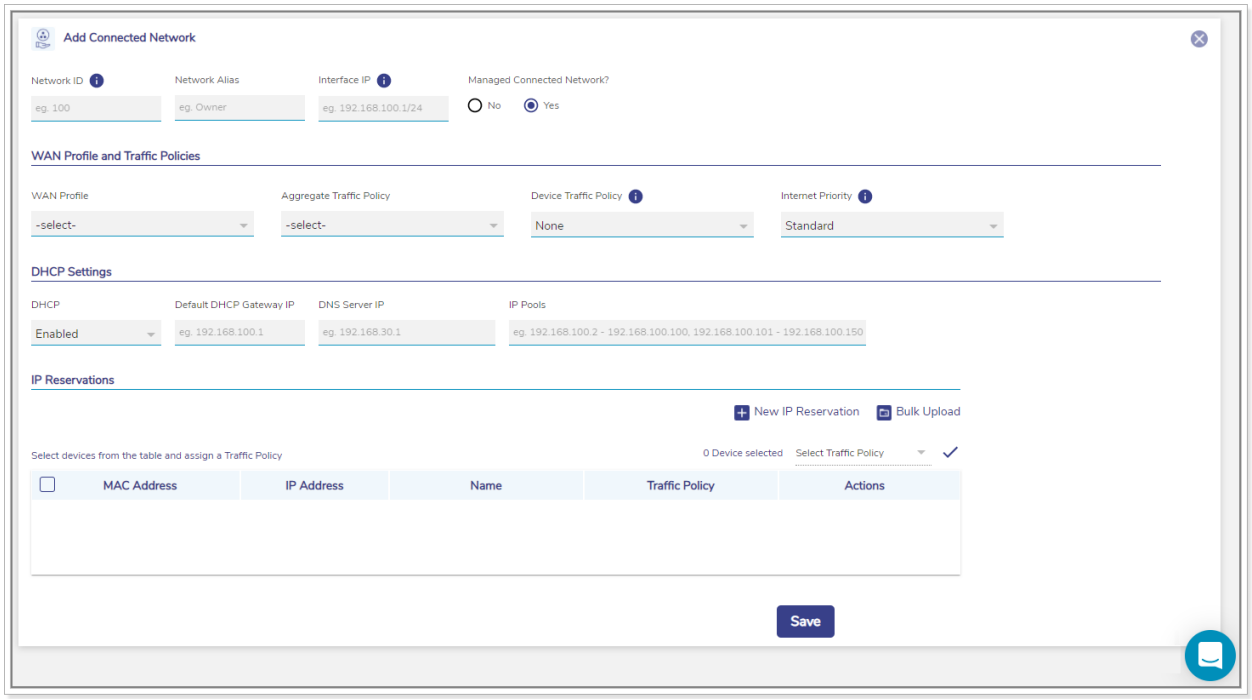

Figure 2-15 Configure Manage Connected Network

Return

Figure 2-16 Bulk Upload IP Reservations

Return

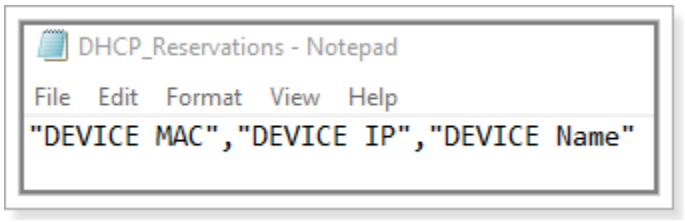

Figure 2-17 IP Reservations Template in CSV Format

Return

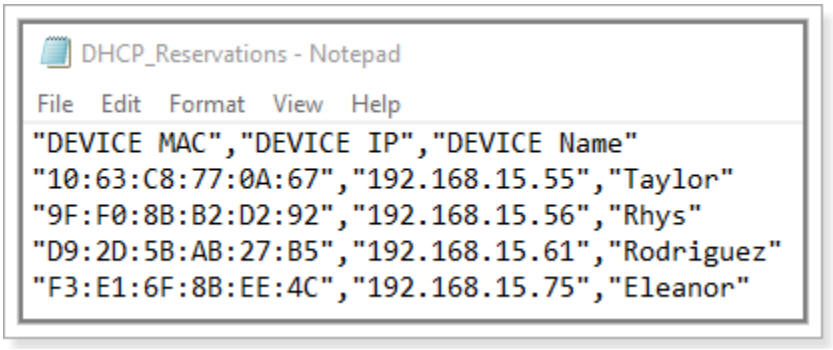

Figure 2-18 Example of IP Reservations Template in CSV Format

Return

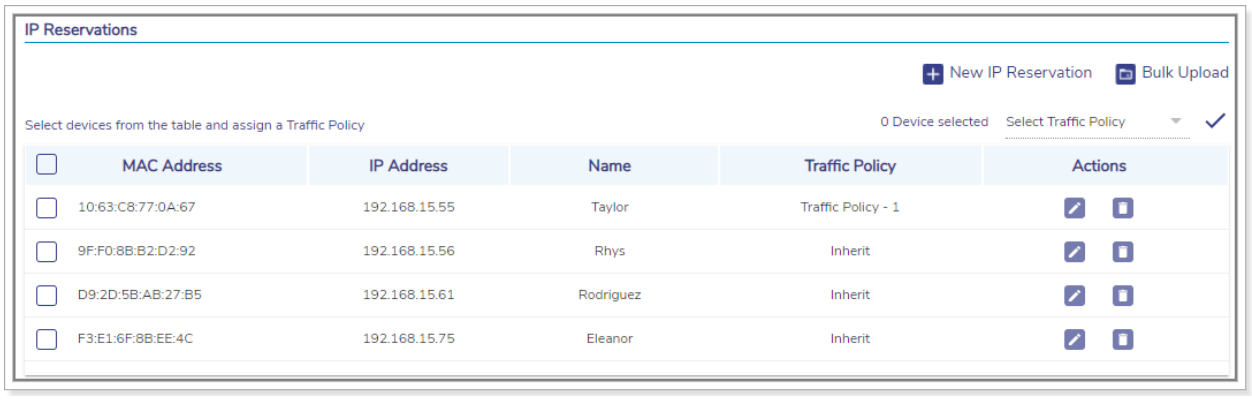

Figure 2-19 IP Reservations Details

Return

Table 2-3 Connected Network Information

Fields	Description
Network ID	Enter a unique numeric ID from 2 to 4090. For details about the network ID, click  next to the Network ID. **NOTE:** Network ID is known as a VLAN ID. Once the network ID is configured, you cannot modify or update the VLAN ID or network ID in the future.
Network Alias	Enter a unique alias of the network.
Interface IP	Enter an interface IP address and subnet mask.
Managed Connected Network	Click one of the following options. • No. This indicates that by default, you will configure the unmanaged connected network is configured. • Yes. To manage and configure the connected network, click **Yes**. The network configuration section becomes available, see *Figure 2-15*. **NOTE:** The Managed Connected Network is the Traditional VLAN-s.
WAN Profile and Traffic Policies	
WAN Profile	Click a WAN profile. **NOTE:** If you are assigning the WAN profile initially after the K4 server installation, then only the default WAN profile will become available. However, you can configure the distinct WAN profiles. Therefore, the entire WAN profiles will become available. For details about configuring the WAN profiles, see *Audit WAN Profiles* on page 66.
Aggregate Traffic Policy	Click a network traffic policy. **NOTE:** If you are assigning the network traffic policy initially after the K4 server installation, then only the default network traffic policy will become available. However, you can configure the distinct network traffic policies. Therefore, the entire network traffic policies will become available. For details about configuring the network traffic policies, see *Audit Traffic Policies* on page 71. The **Aggregate Traffic Policy** will apply to VLAN.

Fields	Description
Device Traffic Policy	Click a device traffic policy. **NOTE:** If you are assigning the device traffic policy initially after the K4 server installation, then only the default device traffic policy will become available. However, you can configure the distinct device traffic policies. Therefore, the entire device traffic policies will become available. For details about configuring the device traffic policies, see *Audit Traffic Policies* on page *71*. You can assign the traffic policy to a device from also **Step 6: Other Settings**. For details, see *Audit Other Settings* on page *83*. However, the traffic policy last assigned to a device from any step will override the traffic policy of that device. Following is an example. Previously, the traffic policy was assigned to a device from **Step 3: Access Networks**. A new traffic policy is assigned to a device from **Step 6: Other Settings**. Therefore, the traffic policy assigned to a device from **Step 6: Other Settings** will override the existing traffic policy of that device.
Internet Priority	Click an internet priority. For details, click ⓘ next to the Internet Priority. **NOTE:** Real-time priority works best for only voice/video call applications.
DHCP Settings	
DHCP	To enable DHCP so that a DHCP can automatically assign the IP address and the other allied configuration details to a host on a network to communicate with the endpoints, click **Enable**.
Default DHCP Gateway IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address.
DNS Server IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address. **NOTE:** You can assign a maximum of three DNS IP addresses.
IP Pools	The default sequential range of the IP addresses becomes available.

<table>
<tr><th>Fields</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">You can assign a new range of the sequential IP address. For this, click and delete the IP address range and then assign a new sequential range of the IP address.
You can assign multiple sequential IP address range excluding the specific IP addresses of that range. This is an example.
192.168.10.2-192.168.10.100, 192.168.10.151-192.168.10.200, 192.168.10.220-192.168.10.254
The following IP addresses will not be assigned to the device in the network.
• 192.168.10.101-192.168.10.150
• 192.168.10.2-201.168.10.219
DHCP will assign the IP address to a device in the specified network basis on the IP address range.</td></tr>
<tr><th colspan="3">IP Reservations</th></tr>
<tr><td rowspan="5">New IP Reservation</td><td colspan="2">To reserve an IP address for a device, perform the following steps.
1. Click New IP Reservation.
2. Configure the MAC Address, IP Address, Name, Traffic Policy, and Actions fields.</td></tr>
<tr><td>MAC Address</td><td>To reserve an IP address for a device, click New IP Reservation, and then enter the MAC address of a device.</td></tr>
<tr><td>IP Address</td><td>Enter IP address from the sequential IP address range specified in the IP Pools field.</td></tr>
<tr><td>Name</td><td>Enter a name for the device.</td></tr>
<tr><td>Traffic Policy</td><td>Click a traffic policy is to be assigned to the device.
NOTE: Inherit indicates that the device will inherit the device policy of the network.</td></tr>
<tr><td>Actions</td><td>To save the IP reservations, click  .
Or,
To cancel the IP reservations, click  .</td></tr>
<tr><td>Bulk Upload</td><td colspan="2">To upload details about the IP reservation, perform the following steps.
1. Click Bulk Upload. The Bulk upload IP Reservations pop-up window appears, see Figure 2-16.</td></tr>
</table>

Fields	Description
	2. To download the bulk IP reservation template, click **Download Reservations**. The IP reservation template downloads in CSV format, see *Figure 2-17*. 3. Fill in the required details in the file. For an example, see *Figure 2-18*. **NOTE:** The first row is referred to as the header row. 4. Save the file. 5. Click **Upload Reservations** and browse the IP reservations CSV file. 6. Click **Open**. The IP reservations are displayed under the **IP Reservations** section, see *Figure 2-19*. 7. Click **Save**.
	You can modify the details of the IP reservation. **To modify the details of the IP reservation, perform the following steps.** 1. Click  . 2. Modify the IP address of the device in the IP Address field, the name of the device in the Device field, and the traffic policy in the Traffic Policy field. **NOTE:** The MAC Address field is read-only. 3. Click  . Or, To cancel the IP reservation, click  . 4. Click **Save**. Details of the IP reservation are modified.
	To delete the IP reservation, perform the following steps. 1. Click  . The IP reservation details are deleted. 2. Click **Save**.

3. Click **Save**.
4. Click **Add Managed Routed Network**. The **Add Managed Routed Network** page appears, see *Figure 2-20*. To enter data in the respective fields, see *Table 2-4*.

NOTE: Managed Routed Networks linked to the Unmanaged Connected Network are available in a group with a color background.

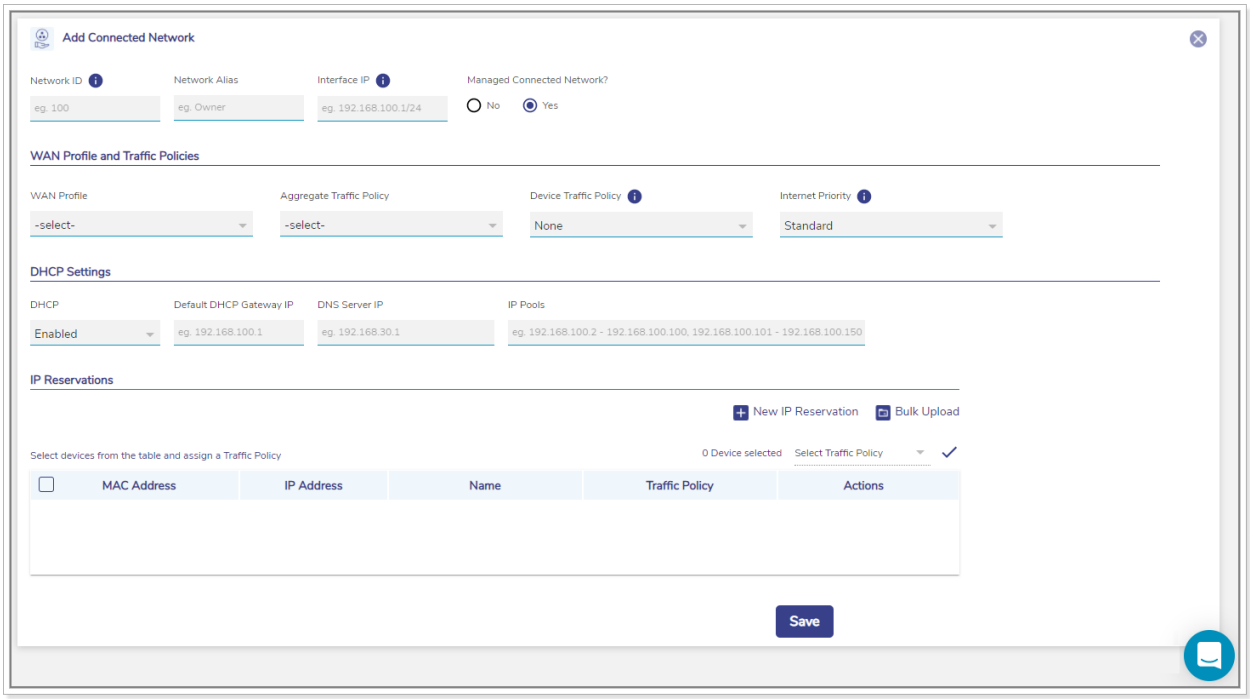

Figure 2-20 Add Managed Routed Network

Table 2-4 Managed Routed Network Information

Fields	Description
Network Alias	Enter a unique alias of the network.
Subnet	Enter the subnet basis on the interface IP address and mask that was configured while configuring the connected network.
Gateway	Enter the IP address of the device managing the communication with the external network. **NOTE:** You must assign the IP address basis on the interface IP address that was configured while configuring the connected network.
WAN Profile and Traffic Policies	
WAN Profile	Click a WAN profile. **NOTE:** If you are assigning the WAN profile initially after the K4 server installation, then only the default WAN profile will become available. However, you can configure the distinct WAN profiles. Therefore, the entire WAN profiles will become available. For details about configuring the WAN profiles, see *Audit WAN Profiles* on page 66.

Fields	Description
Aggregate Traffic Policy	Click a network traffic policy. **NOTE:** If you are assigning the network traffic policy initially after the K4 server installation, then only the default network traffic policy will become available. However, you can configure the distinct network traffic policies. Therefore, the entire network traffic policies will become available. For details about configuring the network traffic policies, see *Audit Traffic Policies* on page *71*.
Device Traffic Policy	Click a device traffic policy. **NOTE:** If you are assigning the device traffic policy initially after the K4 server installation, then only the default device traffic policy will become available. However, you can configure the distinct device traffic policies. Therefore, the entire device traffic policies will become available. For details about configuring the network traffic policies, see *Audit Traffic Policies* on page *71*.
Internet Priority	Click an internet priority. For details, click  next to the Internet Priority. **NOTE:** Real-time priority works best for only voice/video call applications.
DHCP Settings	
DHCP	To enable DHCP so that a DHCP can automatically assign the IP address and the other allied configuration details to a host on a network to communicate with the endpoints, click **Enable**.
Default DHCP Gateway IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address.
DNS Server IP	The default IP address becomes available. You can assign a new IP address. For this, click and delete the IP address and then assign a new IP address. **NOTE:** You can assign a maximum of three DNS IP addresses.
IP Pools	The default sequential range of the IP addresses becomes available. You can assign a new range of the sequential IP address. For this, click and delete the IP address range and then assign a new sequential range of the IP address.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>You can assign multiple sequential IP address range excluding the specific IP addresses of that range. This is an example.
192.168.10.2-192.168.10.100, 192.168.10.151-192.168.10.200, 192.168.10.220-192.168.10.254
The following IP addresses will not be assigned to the device in the network.
• 192.168.10.101-192.168.10.150
• 192.168.10.2-201.168.10.219
DHCP will assign the IP address to a device on the specified network basis on the IP address range.</td></tr>
<tr><th colspan="2">IP Reservations</th></tr>
<tr><td rowspan="6">New IP Reservation</td><td colspan="2">To reserve an IP address for a device, perform the following steps.
1. Click New IP Reservation.
2. Configure the MAC Address, IP Address, Name, Traffic Policy, and Actions fields.</td></tr>
<tr><td>MAC Address</td><td>To reserve an IP address for a device, click New IP Reservation, and then enter the MAC address of a device.</td></tr>
<tr><td>IP Address</td><td>Enter IP address from the sequential IP address range specified in the IP Pools field.</td></tr>
<tr><td>Name</td><td>Enter a name for the device.</td></tr>
<tr><td>Traffic Policy</td><td>Click a traffic policy to be assigned to the device.
NOTE: Inherit indicates that the device will inherit the device policy of the network.</td></tr>
<tr><td>Actions</td><td>To save the IP reservations, click  .
Or,
To cancel the IP reservations, click  .</td></tr>
<tr><td>Bulk Upload</td><td colspan="2">To upload details of the IP reservation, perform the following steps.
1. Click Bulk Upload. The Bulk upload IP Reservations pop-up window appears, see Figure 2-16.
2. To download the bulk IP reservation template, click Download Reservations. The IP reservation template downloads in the CSV format, see Figure 2-17.</td></tr>
</table>

Fields	Description
	3. Fill in the required details in the file. For an example, see *Figure 2-18*. **NOTE:** The first row is referred to as the header row. 4. Save the file. 5. Click **Upload Reservations** and browse the IP reservations CSV file. 6. Click **Open**. The IP reservations are displayed under the **IP Reservations** section, see *Figure 2-19*. 7. Click **Save**.
	You can modify the details of the IP reservation. **To modify the details of the IP reservation, perform the following steps.** 1. Click  . 2. Modify the IP address of the device in the IP Address field, the name of the device in the Device field, and the traffic policy in the Traffic Policy field. **NOTE:** The MAC Address field is read-only. 3. Click  . Or, To cancel the IP reservation, click  . 4. Click **Save**. Details of the IP reservation are modified.
	To delete the details of the IP reservation, perform the following steps. 1. Click  . The IP reservation details are deleted. 2. Click **Save**.

To configure the WAN profile through the **Access Networks** page, click the WAN profile link. The **WAN Profiles** page appears. For details, see *Audit WAN Profiles* on page 66.

To configure the aggregate traffic policy and device traffic policy through the **Access Networks** page, click the aggregate traffic policy or device traffic policy link. The **Traffic Profiles** page appears. For details, see *Audit Traffic Policies* on page 71.

2.3.1 Modifying Network

To modify details about the network, perform the following steps.

1. Click corresponding to the network under the **Action** section on the **Access Networks** page. The **Updated Connected Network** page appears, see *Figure 2-21*. To enter data in the respective fields, see *Table 2-3*.

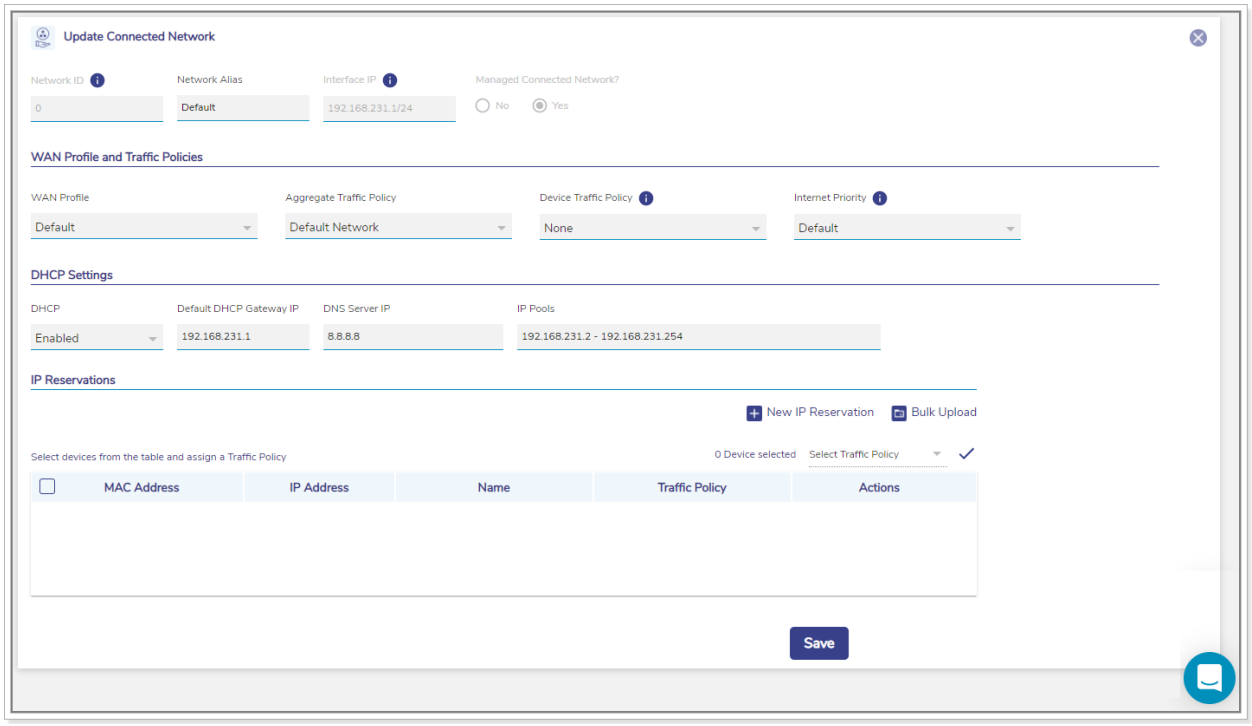

Figure 2-21 Update Connected Network

2. Click **Save**.

2.3.2 Modifying Device Profile

To modify the device profile, perform the following steps.

1. Click corresponding to the network under the **Action** section on the **Access Networks** page. The **Device Profile** page appears, see *Figure 2-22*. To enter data in the respective fields, see *Table 2-3*.

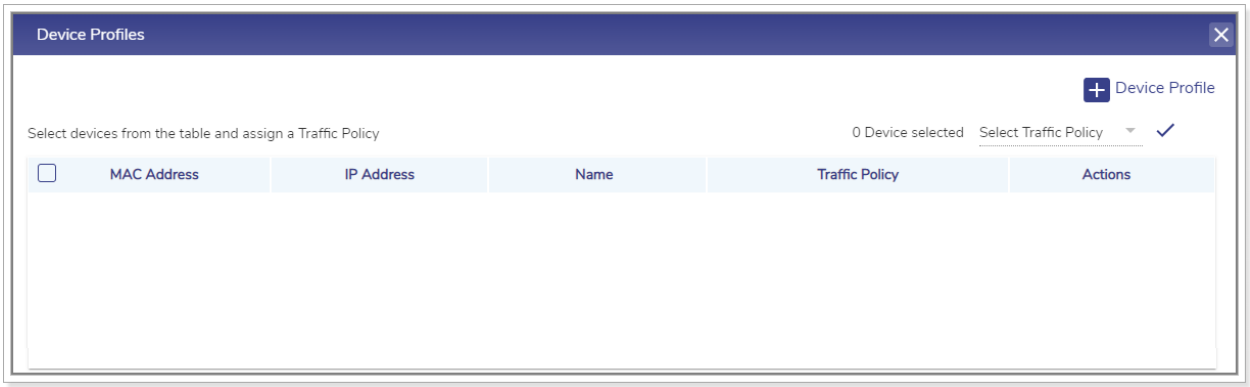

Figure 2-22 Update Device Profile

2. Click **Save**.

You can add a new device profile. For this, click **Device Profile**. To enter data in the respective fields, see *Table 2-3*.

You cannot modify the device profiles of the connected network.

2.3.3 Viewing Network Usage Data

To view network usage data, perform the following steps.

1. Click  corresponding to the network under the **Action** section on the **Access Networks** page. The **Network Usage** page appears, see *Figure 2-23*. For details about the fields, see *Table 2-5*.

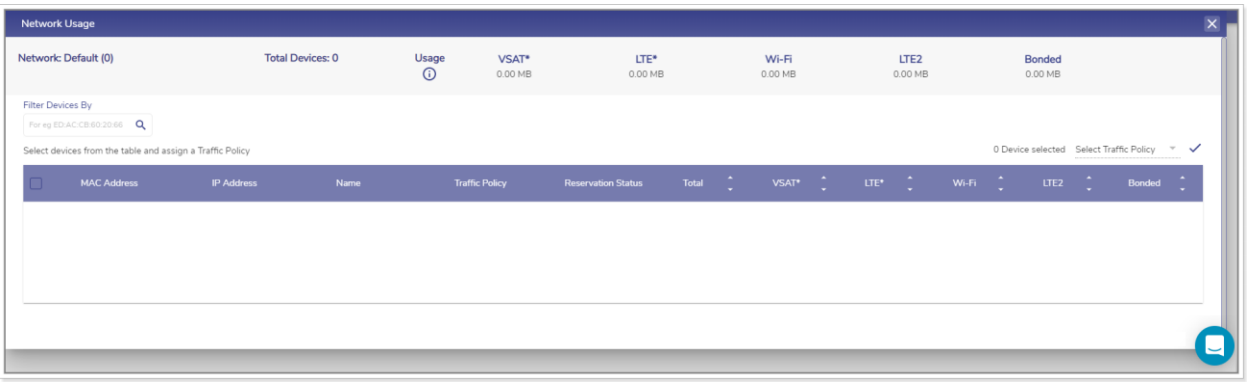

Figure 2-23 Network Usage

Remaining	VSAT	LTE	Wi-Fi	LTE2	Bonded
UL Quota	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
DL Quota	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

Figure 2-24 Quota Details

Return

Figure 2-25 Pause Device Profile Confirmation Message

Return

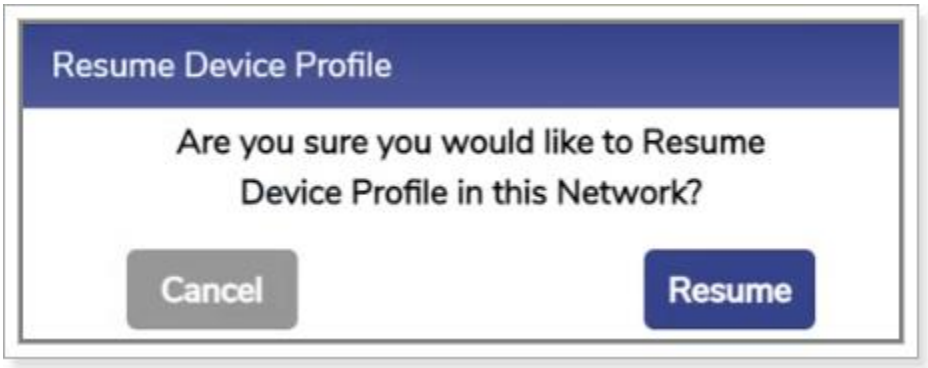

Figure 2-26 Resume Device Profile Confirmation Message

Return

Table 2-5: Network Usage Information

Fields	Description
Network	This indicates the name of the network
Total Devices	This indicates the count of the devices connected to the network.
Usage	This indicates details about the quota of the network. To view the quota details, click ⓘ. Details about the quota are displayed, see *Figure 2-24*.
VSAT	This indicates the total data consumed by the VSAT.
LTE	This indicates the total data consumed by the LTE.
Wi-Fi	This indicates the total data consumed by the Wi-Fi.
LTE2	This indicates the total data consumed by the LTE2.
Bonded	This indicates the total data consumed by the Bonded.

Fields	Description
Filter Devices By	Enter the MAC address of the specific device. Details about the device become available.
MAC Address	This indicates the MAC address of the device connected to the network. 1. To pause the device, click . The **Pause Device Profile** confirmation message pop-up window appears, see *Figure 2-25*. 2. Click **Pause**. The (resume button) becomes available and the row of the device is highlighted by a color. Or, 1. To resume the device, click . The **Resume Device Profile** confirmation message pop-up window appears, see *Figure 2-26*. 2. Click **Resume**.
IP Address	This indicates the IP address assigned to the device.
Name	This indicates the alias name of the device. To modify the alias name, click and modify the alias name.
Traffic Policy	This indicates the traffic policy assigned to the device. To modify the traffic policy, click and modify the traffic policy. For details, see *Audit Traffic Policies* on page *71*. **To assign the traffic policy to multiple devices, perform the following steps.** 1. Select the check box corresponding to the device. The count of the devices selected is displayed in the **Devices Selected** field. 2. Click **Select Traffic Policy**. 3. Click the traffic policy to be assigned the devices selected. Or, **To assign the traffic policy to the devices in bulk, perform the following steps** 1. Select the check box corresponding to the **MAC Address** field. The count of the devices selected is displayed in the **Devices Selected** field. 2. Click **Select Traffic Policy**. 3. Click the traffic policy to be assigned the devices selected.

Fields	Description
Reserved Status	This indicates that, whether the IP address assigned to the device is reserved. To reserve the IP address of the device, click the corresponding check box. Or, To un-reserve, the IP address of the device, clear the check box.
Total	This indicates the sum of the data consumed by the device on the following WAN links. • VSAT • LTE • Wi-Fi • LTE2 • Bonded
VSAT	This indicates the quantum of the data consumed by the device on the VSAT. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, LTE2 and Bonded links is displayed in the **Total** field.
LTE	This indicates the quantum of the data consumed by the device on the LTE. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, LTE2 and Bonded links is displayed in the **Total** field.
Wi-Fi	This indicates the quantum of the data consumed by the device on the Wi-Fi. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, LTE2 and Bonded links is displayed in the **Total** field.
LTE2	This indicates the quantum of the data consumed by the device on the LTE2. **NOTE:** The sum of the VSAT, LTE, Wi-Fi, LTE2 and Bonded links is displayed in the **Total** field.
Bonded	This indicates the quantum of the data consumed by the device on the Bonded.

Fields	Description
	NOTE: The sum of the VSAT, LTE, Wi-Fi, LTE2 and Bonded links is displayed in the **Total** field.

2.3.4 Pausing or Resuming Network Traffic

To pause the network traffic, perform the following steps.

1. Click corresponding to the network under the **Action** section on the **Access Networks** page. The **Pause Network Traffic** confirmation message pop-up window appears, see *Figure 2-27*.

Figure 2-27 Pause Network Traffic Confirmation Message

2. Click **Pause**. The Resume Network Traffic button becomes available and the row of the network is highlighted by a color.

You cannot pause the network traffic of the connected network.

To resume the network traffic, perform the following steps.

1. Click corresponding to the network under the **Action** section on the **Access Networks** page. The **Resume Network Traffic** confirmation message pop-up window appears, see *Figure 2-28*.

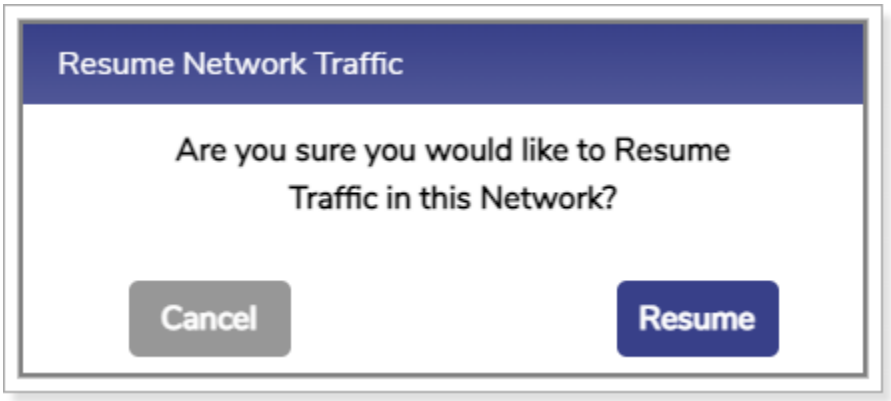

Figure 2-28 Resume Network Traffic Confirmation Message

2. Click **Resume**.

The network traffic on the network resumes.

2.3.5 Deleting Network

To delete the network, perform the following steps.

1. Click corresponding to the network under the **Action** section on the **Access Networks** page. The **Delete Network** confirmation message pop-up window appears, see *Figure 2-29*.

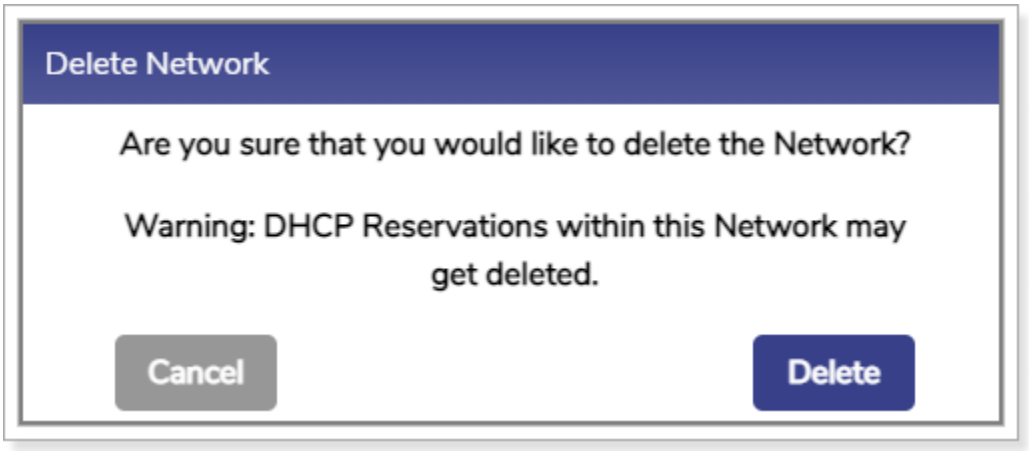

Figure 2-29 Delete Network Confirmation Message

2. Click **Delete**.

The network is successfully deleted. It will impact the DHCP reservations. Therefore, it is highly recommended to verify the network details before deleting the network.

Perform **Audit WAN Profiles**.

2.4 Audit WAN Profiles

The K4 OneDome is installed on the vessel, by default, the K4 OneDome has configured to **Advance Bond** the three LTE links. With this, the K4 OneDome LTE links will appear as a single link to the SDWAN service. **It is not recommended to modify the default configuration**. However, based on the need, you can set the access network, application priority on the K4 OneDome to improve overall service behavior.

To create a WAN profile, perform the following steps.

1. Click on the **Access Networks** page or click **WAN Profiles**. The **WAN Profiles** page appears, see *Figure 2-30*.

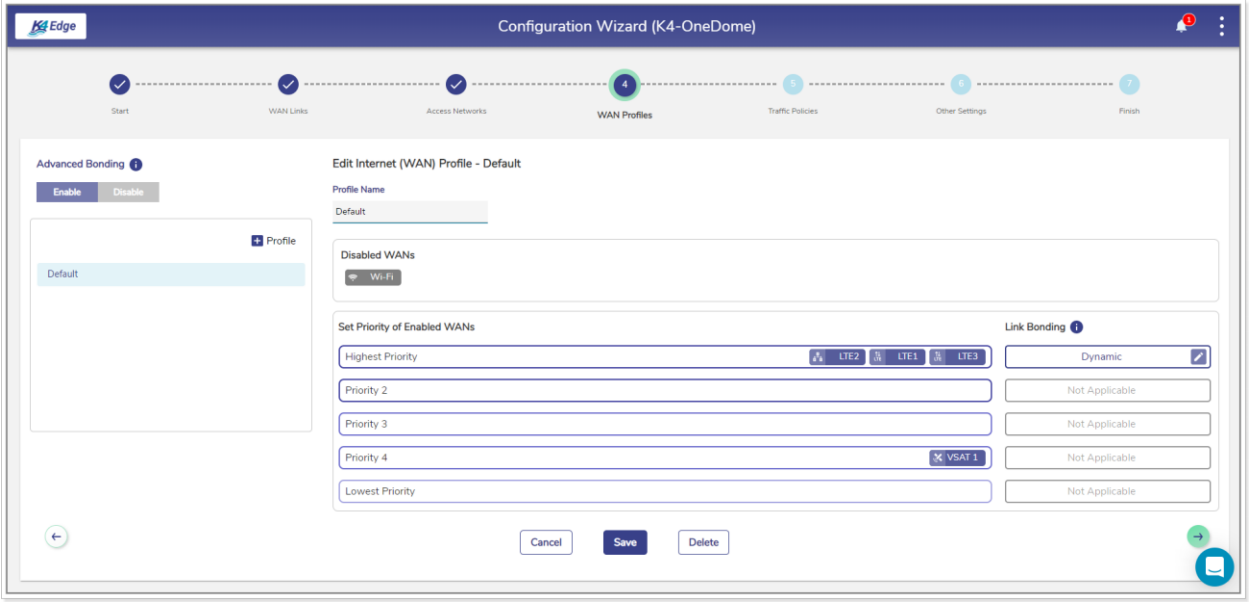

Figure 2-30 Create WAN Profile

NOTE: Initially, the **Default** WAN profile is available. You can create multiple profiles. Once, the profiles are configured, the profiles become available on the **WAN Profiles** page. You can associate the WAN profile with VLAN.

NOTE: Initially, the Wi-Fi is unavailable as AP Mode is enabled. Therefore, Wi-Fi WAN is disabled in the Default WAN Profile. Once Marina Wi-Fi is enabled (AP Mode is disabled), the Wi-Fi WAN is set to Priority 2 in the Default WAN Profile. Hence, if the Wi-Fi is unavailable, then you cannot define the priority of the Wi-Fi. Therefore, before defining the priority of the Wi-Fi, you must ensure that the Wi-Fi is available.

2. Click **+ Profile**. The Profile Name field becomes available under the **Edit Internet (WAN) Profile** section. To enter data in the respective fields, see *Table 2-6*.

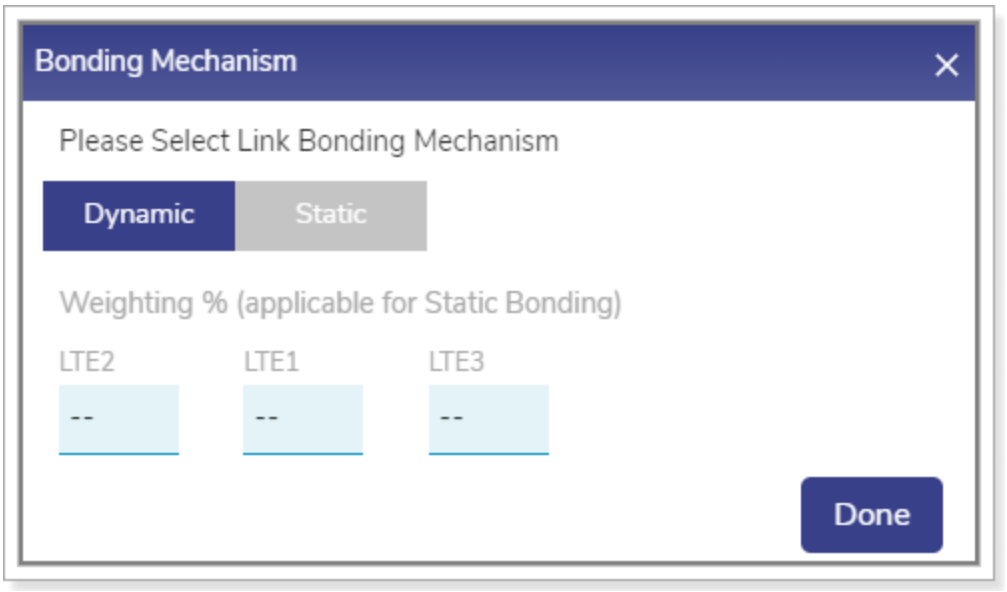

Figure 2-31 Dynamic Bonding Mechanism for WANs

Return

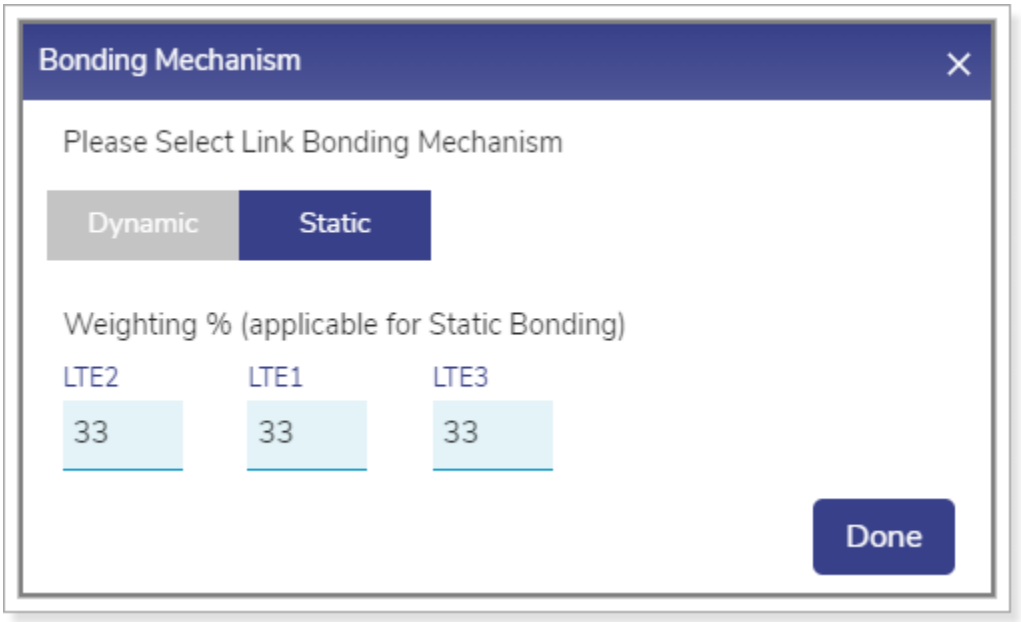

Figure 2-32 Static Bonding Mechanism for WANs

Return

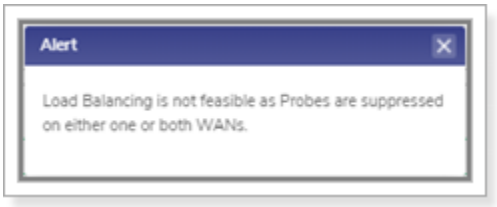

Figure 2-33 Error Message

Return

Table 2-6: Profile Information

Fields	Description
Profile Name	Enter the name of the profile.
Disabled WANs	Disabled WAN sources are displayed.
Set Priority of Enabled WANs	
Highest Priority	**To assign the like WAN links to a priority level, perform the following steps.** Drag and drop the like WAN links available under the **Disabled WANs** section. By default, only the like WAN bonding can be assigned to the priority levels. You can assign also the unlike WANs to the priority levels, by enabling the **Advanced Bonding**. However, **Advanced Bonding** is a licensed feature of the K4 Mobility and is available with only US Internet features. Therefore, you must ensure that the license of the Advanced Bonding is available for your vessel. It is highly prohibited to modify the **Default** WAN profile. However, you can configure the new WAN profile. **To assign the unlike WAN to the priority levels, perform the following steps** 1. Click **Enable** under the **Advanced Bonding** section. For details of the advanced bonding, point the mouse to ⓘ next to the **Advanced Bonding**. By default, the advanced bonding is disabled. 2. Drag and drop the unlike WAN link available under the **Disabled WANs** section. **NOTE:** You can configure only single Advanced Bonding in a profile. By default, the link bonding **Dynamic** with pre-configured weighting % is configured for both like and unlike WAN links. For details about the types of link bonding, point the mouse to ⓘ next to the **Link Bonding**. You can configure the weighting % of the WAN link. **To configure the weighting %, perform the following steps.** 1. Click **Dynamic** under the link bonding section. The **Bonding Mechanism** pop-up window appears, see *Figure 2-31*. 2. Click **Static**. The **Weighting % (applicable for Static Bonding)** section becomes available, see *Figure 2-32*.

Fields	Description
	3. Enter the weighting % for the WAN links. You must ensure that the sum of the weighting % for both like and unlike WAN links must be 100%. This is an example of the like WAN link. You can configure 40 the weighting % for the LTE1 and 60 the weighting % for the LTE2. As, sum of both weighting % (40 + 60) = 100. This is an example of the unlike WAN link. You can configure 40 the weighting % for the LTE1, 30 the weighting % for the LTE2, and 30 the weighting % for the LTE3. As, sum of the weighting % (40 + 30 + 30) = 100. 4. Click **Done**. The **Create Internet** (**WAN) Profiles** page appears, see *Figure 2-30*. If an error occurred due to a probe of the WAN, then an error message is displayed, see *Figure 2-33*. **NOTE:** The Link Bonding will not be available for a single WAN link. Therefore, weighting % cannot be configured.
Priority 2	Refer to Highest Priority.
Priority 3	Refer to Highest Priority.
Priority 4	Refer to Highest Priority.
Lowest Priority	Refer to Highest Priority.

Once the WAN link is assigned to the priority levels, the server will verify the network basis on the priority levels. This is an example.

You set the following priority levels of enabled WANs.

Priority 1 – LTE 1 and LTE 2.

Priority 2 – LTE 3.

Initially, the server will verify whether the LTE1 and LTE 2 network is available as the LTE 1 and LTE 2 are assigned priority level 1. If the LTE network is available, then the internet connection will be established through the LTE network. Otherwise, the server will verify whether the Ethernet network is available as the Ethernet is assigned the priority 2 level. The process will continue up to the priority level configured.

The server will distribute the traffic basis on the weighting % configured for the WAN links.

3. Click **Save**.

WAN profile configured successfully. The WAN profile will become available while configuring the networks. For details, see *Audit Access Networks* on page *44*.

Perform **Audit Traffic Policies**.

2.5 Audit Traffic Policies

When the K4 OneDome is installed on the vessel, by default, the network level, and device level traffic policies are not configured. The network level policy will be applicable under the Aggregate Traffic Policy and the device level policy will be applicable under the Device Traffic Policy.

1. Click on the **WAN Profiles** or click **Traffic Policies**. The **Traffic Profiles** page appears, see *Figure 2-34*.

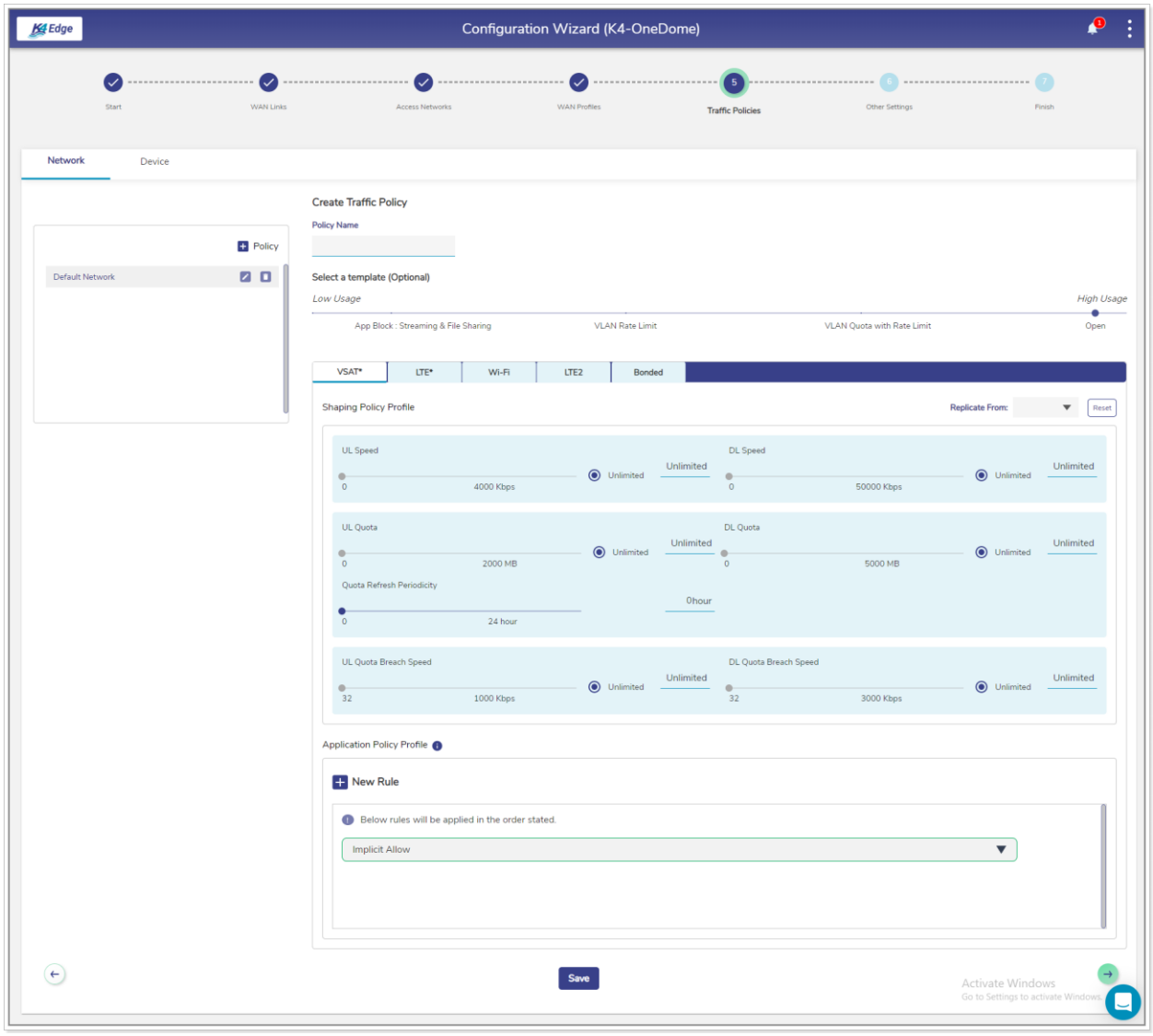

Figure 2-34 Traffic Policies

NOTE: Initially, the **Default Network** is available. You can configure multiple traffic policies. Once, the traffic policies are configured, the traffic policies become available on the **Traffic Policies** page.

2. Click **Network**.

   By default, the **Network** is selected.

3. Click **+ Policy**. The **Policy Name** field becomes available under the **Create Traffic Policy** section. To enter data in the respective fields, see *Table 2-7*.

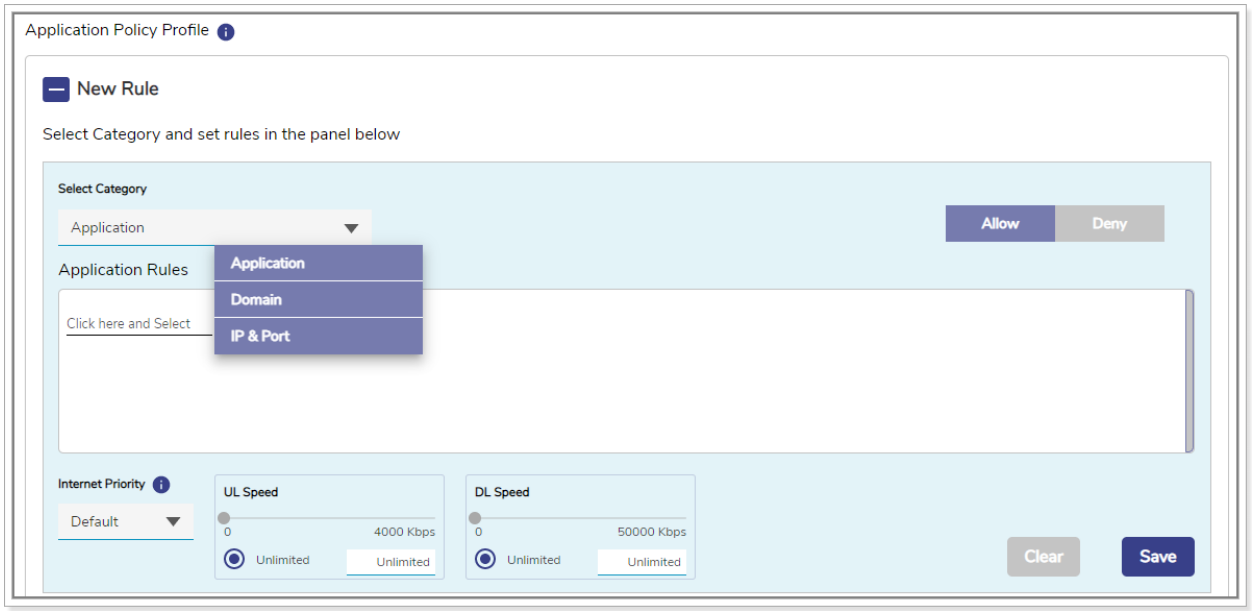

Figure 2-35 Category List

Return

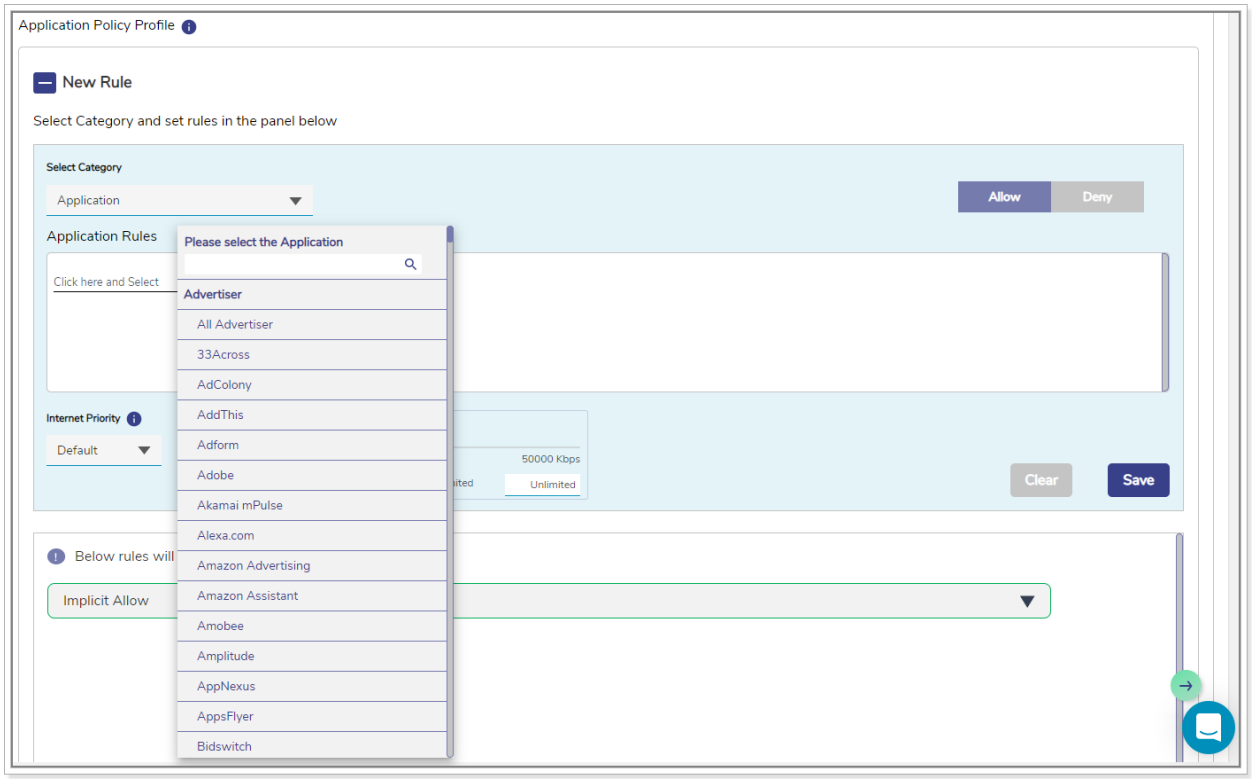

Figure 2-36 Application Rule

Return

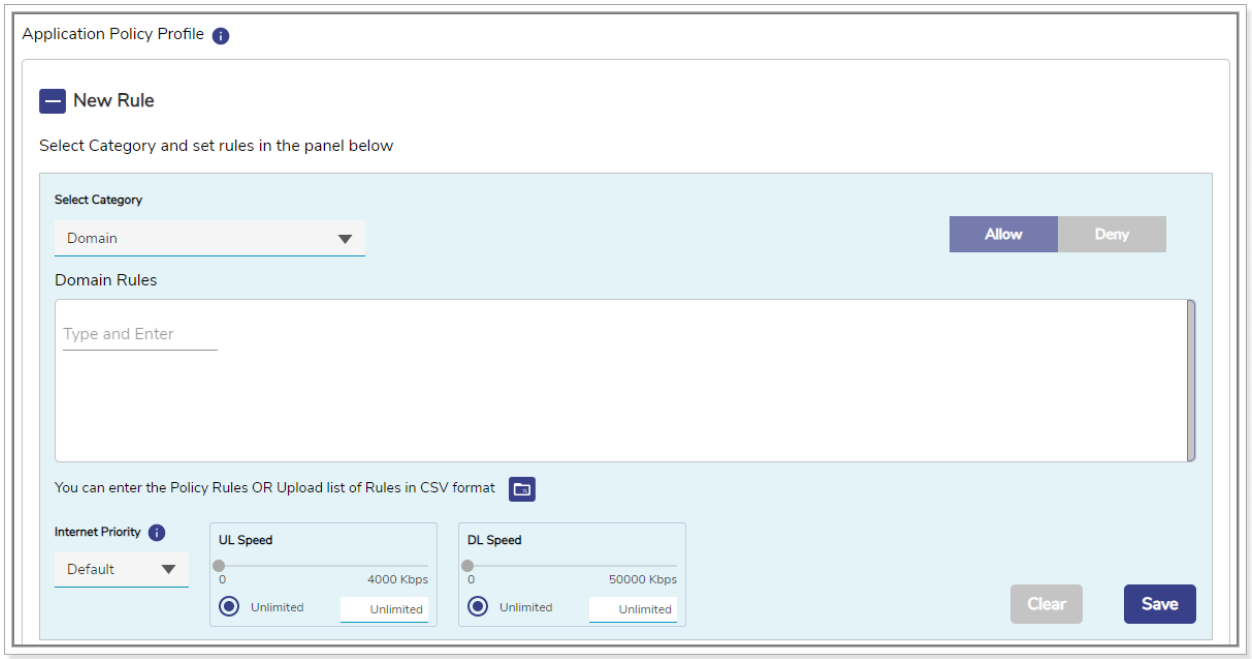

Figure 2-37 Domain Rule

Return

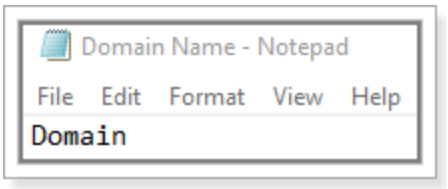

Figure 2-38 Domain Rule Template in CSV Format

Return

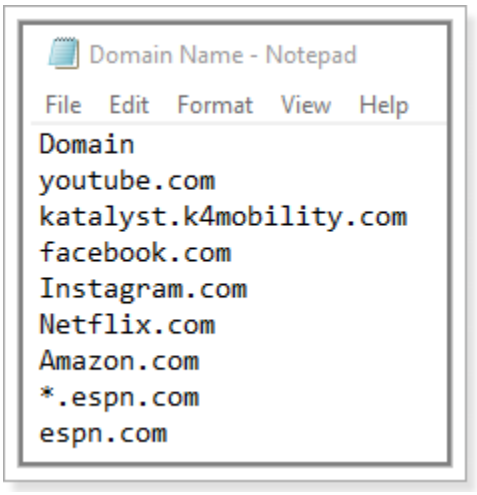

Figure 2-39 Example of Domain Rule Template in CSV Format

Return

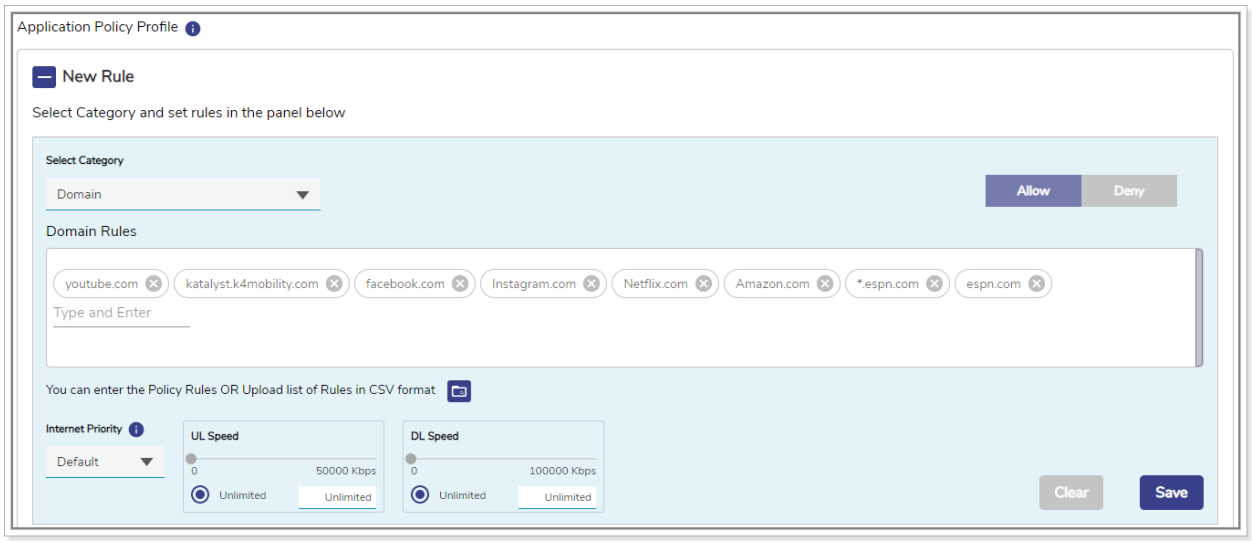

Figure 2-40 Valid Domains

Return

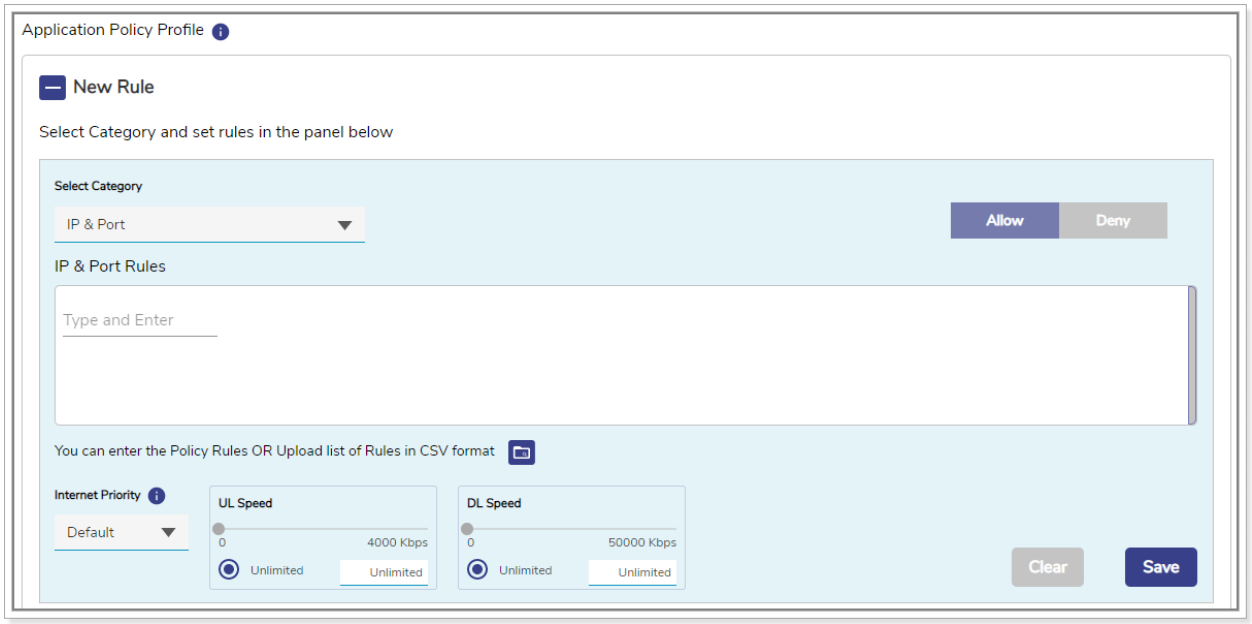

Figure 2-41 IP & Port Rule

Return

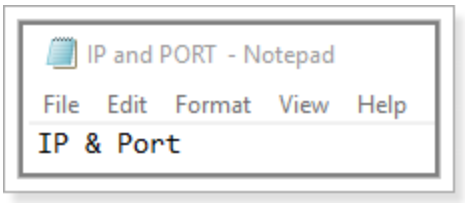

Figure 2-42 IP & Ports Template in CSV Format

Return

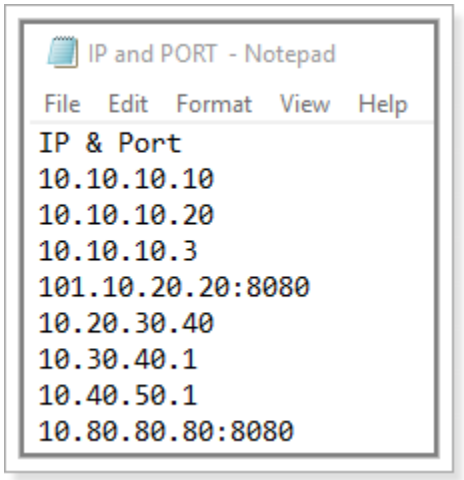

Figure 2-43 Example of IP & Ports Template in CSV Format

Return

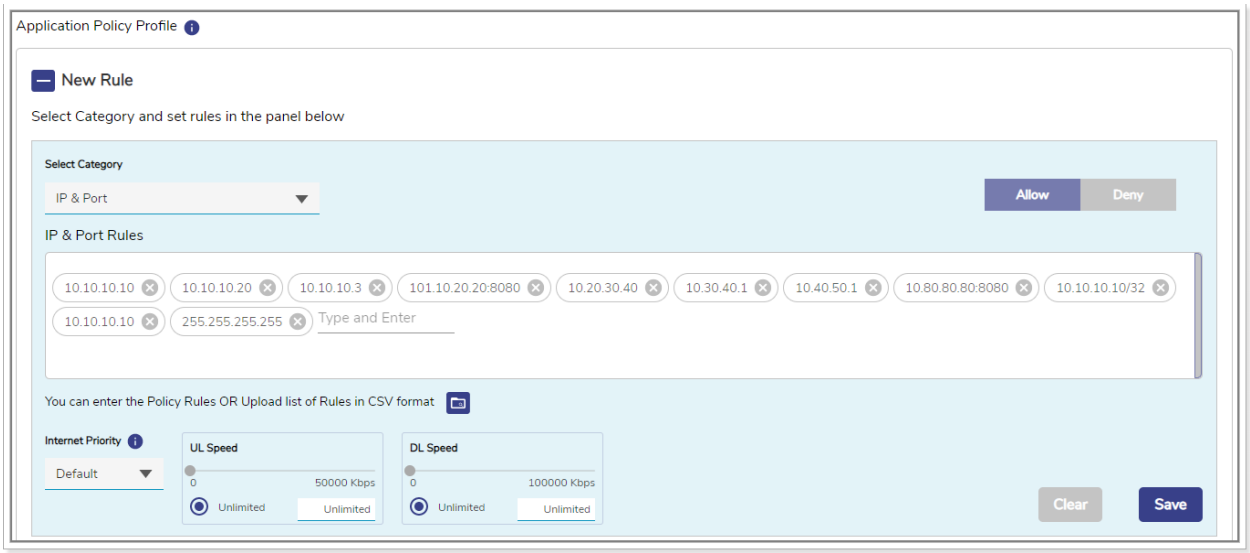

Figure 2-44 Valid IP & Ports

Return

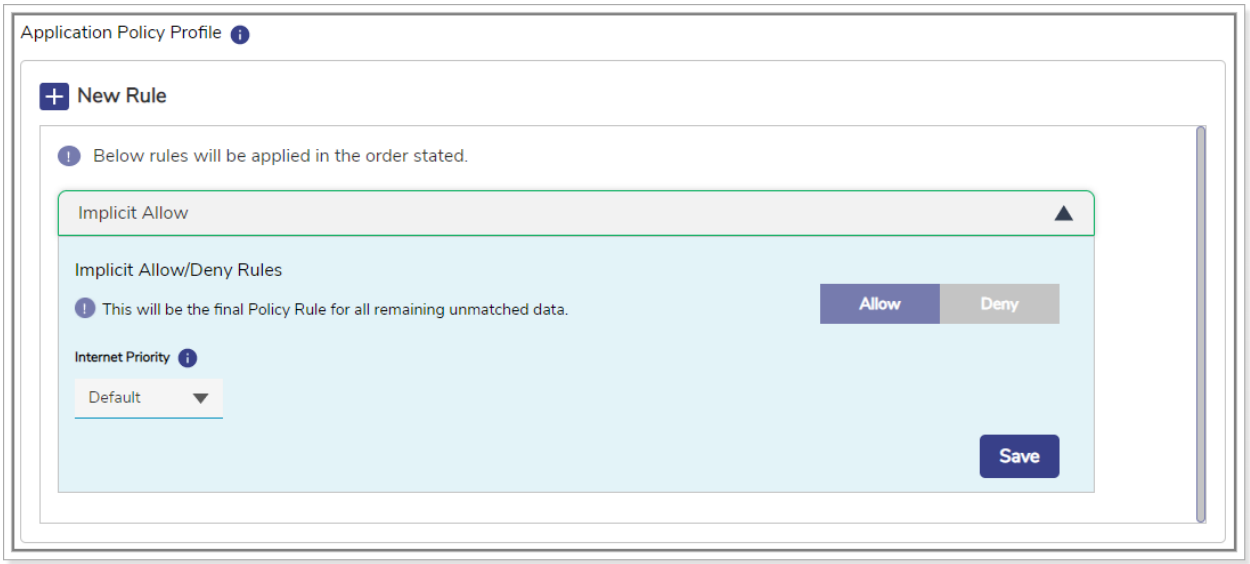

Figure 2-45 Application Allow or Deny

Return

Table 2-7: Traffic Policy Information

Fields	Description
Policy Name	Enter the name of the policy.
Select a template (Optional)	Click a template that is to be assigned to a WAN and then click one of the following WAN tabs. • VSAT • LTE

Fields	Description
	• Wi-Fi • LTE 2 • Bonded A template will include pre-configured UL Speed, DL Speed, UL Quota, DL Quota, Quota Refresh Periodicity, UL Quota Breach Speed, and DL Quota Breach Speed. However, you can modify the template. You can assign a template with the pre-configured traffic policy, or re-configure the traffic policy of a template, or configure the traffic policy based on your requirement through the **Open** template. By default, the **Open** template is selected.
Shaping Policy Profile	
UL Speed	By default, **Unlimited** is selected. This indicates that the unlimited upload speed is configured and the **Unlimited** speed is displayed corresponding to the **UL Speed**. To configure the upload speed, move the slider to the right or click the speed. The **Unlimited** is cleared and the upload speed configured is displayed corresponding to the **UL Speed**.
DL Speed	By default, **Unlimited** is selected. This indicates that the unlimited download speed is configured and the **Unlimited** speed is displayed corresponding to the **DL Speed**. To configure the download speed, move the slider to the right or click the speed. The **Unlimited** is cleared and the download speed configured is displayed corresponding to the **DL Speed**.
UL Quota	This indicates the permissible quota up to which the user can upload the data.
	By default, **Unlimited** is selected. This indicates that the unlimited upload quota is configured and the **Unlimited** quota is displayed corresponding to the **UL Quota**. To configure the upload quota, move the slider to the right or click the quota. The **Unlimited** is cleared and the upload quota configured is displayed corresponding to the **UL Quota**.
DL Quota	This indicates the permissible quota up to which the user can download the data.

Fields	Description
	By default, **Unlimited** is selected. This indicates that the unlimited download quota is configured and the **Unlimited** quota is displayed corresponding to the **DL Quota**. To configure the download quota, move the slider to the right or click the quota. The **Unlimited** is cleared and the download quota configured is displayed corresponding to the **DL Quota**.
Quota Refresh Periodicity	This indicates the expiry of hours after which the upload quota and download quota will be refilled or reset to the pre-configured upload quota and download quota respectively.
	To configure the quota refresh periodicity, move the slider to the right or click the refresh periodicity. The refresh periodicity configured is displayed corresponding to the **Quota Refresh Periodici**ty.
UL Quota Breach Speed	This indicates the upload speed that will be applicable after the UL quota is exhausted.
	By default, **Unlimited** is selected and the **Unlimited** UL quota breach speed is displayed corresponding to the **UL Quota Breach Speed**. This indicates that the UL quota breach speed will continue until the UL quota is refilled based on the quota refresh periodicity. To configure the UL quota breach speed, move the slider to the right or click the breach speed. The UL quota breach speed configured is displayed corresponding to the **UL Quota Breach Speed**.
DL Quota Breach Speed	This indicates the download speed that will be applicable after the DL quota is exhausted.
	By default, the **Unlimited** is selected and the **Unlimited** DL quota breach speed is displayed corresponding to the **DL Quota Breach Speed**. This indicates that the DL quota breach speed will continue until the DL quota is refilled based on the quota refresh periodicity. To configure the DL quota breach speed, move the slider to the right or click the breach speed. The DL quota breach speed configured is displayed corresponding to the **DL Quota Breach Speed**.

Fields	Description
Replicate From	**To replicate the traffic policy of a WAN, perform the following steps.** 1. Click **Replicate From**. 2. Click a WAN whose traffic policy is to be applied to the WAN. You can re-configure the replicated traffic policy.
Application Policy Profile	
New Rule	To create a new rule, click **New Rule**. The Category and Application Rules fields become available.
Select Category	Click a category, see *Figure 2-35*. **NOTE:** By default, the **Application** category is selected. Therefore, the Application Rules field becomes available, see *Figure 2-36*. Or, If you select the **Domain** category, then the Domain Rules field becomes available, see *Figure 2-37*. Or, If you select the **IP & Port** category, then the IP & Port field becomes available, see *Figure 2-41*. In addition to this, the entire categories are by default **Allowed**. Therefore, by default **Implicit Allow** rule becomes available under the **Application Policy Profile** section. You cannot modify the **Implicit Allow** rule.
Application Rules	**To apply or deny application rules, perform the following steps.** 1. Click under the **Application Rules** section. The list becomes available, see *Figure 2-36*. 2. Click **Category** or **Subcategory**. List based on the selected **Category** or **Subcategory** becomes available. 3. Click a category or subcategory. 4. To allow the application, click **Allow**. Or, To block the application, click **Deny**. **NOTE:** By default, **Allow** is selected. 5. Click **Save**. The allowed and blocked application becomes available, see *Figure 2-45*.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>NOTE: There can be a single deny and single allow rule per category or an implicit allow or an implicit deny rule.
If you select the Application Rule in the Select Category field, then the Application Rules field becomes available.</td></tr>
<tr><td rowspan="2">Domain Rules</td><td>To apply or deny domain rules, perform the following steps.
1. Click under the Domain Rules section.
2. Enter the name of the domain in one of the following formats.
• domain.com
• domain1.domain2.com
• *.domain.com,
Where,
* can be any value.
NOTE: You can enter multiple domain names.
3. To allow the domain, click Allow.
Or,
To block the domain, click Deny.
NOTE: By default, Allow is selected.
4. Click Save.
The allowed and blocked domain becomes available, see Figure 2-45.
NOTE: If you select the Domain Rule in the Select Category field, then the Domain Rules field becomes available.</td></tr>
<tr><td>You can also upload the rule list in CSV format.
To upload the rule list in CSV format, perform the following steps.
1. Open the Notepad.
NOTE: You can create the CSV file in various text editors such as - Notepad, Microsoft Excel, and Google Docs.
2. Enter the Domain in the first row, see Figure 2-38.
NOTE: The first row is referred to as the header row.
3. Enter the name of the domain in the subsequent rows, see Figure 2-39.
4. Save the file with the .csv extension.</td></tr>
</table>

Fields	Description
	5. Click  and browse the CSV file of the domain rule list. 6. Click **Open**. The domain rules are displayed under the **Domain Rules** section, see *Figure 2-40*. 7. Click **Save**. **NOTE:** If you select the **Domain Rule** in the Select Category field, then the Domain Rules field becomes available.
IP & Port	**To apply or deny IP and port rules, perform the following steps.** 1. Click under the IP & Port section. 2. Enter IP and port in one of the following formats. • a.b.c.d • a.b.c.d/x • a.b.c.d:/x:y • a.b.c.d/x:y-z • a.b.c.d:y-z • a.b.c.d:y Where, x is a subnet and its value can be from 0 (zero) to 32. y and z are port numbers and its value can be from 0 (zero) to 65535. a/b/c/d are IP and its value can be from 0 (zero) to 255. **NOTE:** You can enter IP and ports. 3. To allow the IP, click **Allow**. Or, To block the IP, click **Deny**. **NOTE:** By default, **Allow** is selected. 4. Click **Save**. The allowed and blocked IP and the port become available. **NOTE:** If you select **IP & Port** in the Select Category field, then the IP & Port field becomes available.
	You can also upload the rule list in CSV format. **To upload the rule list in CSV format, perform the following steps.** 1. Open the Notepad.

Fields	Description
	NOTE: You can create the CSV file in various text editors such as - Notepad, Microsoft Excel, and Google Docs. 2. Enter the **IP & Port** in the first row, see *Figure 2-42*. **NOTE:** The first row is referred to as the header row. 3. Enter the IP and port in the subsequent rows, see *Figure 2-43*. 4. Save the file with the **.csv** extension. 5. Click and browse the CSV file of the IP & Port rule list. 6. Click **Open**. Only the valid IP & Port rules are displayed under the **IP & Port Rules** section, see *Figure 2-44*. If an invalid IP & Ports are available, then an error is displayed. 7. Click **Save**. **NOTE:** If you select **IP & Port** in the Select Category field, then the IP & Port field becomes available.
Internet Priority	To view the details of the internet priority, point the mouse to . And, In the **Internet Priority** list, click the internet priority.
UL Speed	By default, **Unlimited** is selected. This indicates that the unlimited upload speed is configured and the **Unlimited** speed is displayed corresponding to the **UL Speed**. To configure the upload speed, move the slider to the right or click the speed. The **Unlimited** is cleared and the upload speed configured is displayed corresponding to the **UL Speed**.
DL Speed	By default, **Unlimited** is selected. This indicates that the unlimited download speed is configured and the **Unlimited** speed is displayed corresponding to the **DL Speed**. To configure the download speed, move the slider to the right or click the speed. The **Unlimited** is cleared and the download speed configured is displayed corresponding to the **DL Speed**.
	After configuring the new rule, click **Save**.
Implicit Allow/Deny Rules	To implicitly allow the final policy, click and then click **Implicit Allow/Deny Rules**, and then click **Allow**. Or,

Fields	Description	
	To implicitly allow the final policy, click ▼ and then click **Implicit Allow/Deny Rules**, and then click **Deny**.	
	Internet Priority	To view the details of the internet priority, point the mouse to ⓘ. And, In the **Internet Priority** list, click the internet priority.
	After configuring the implicit allow or deny rule, click **Save**.	

4. Click **Save**.
5. Click **Device** and then continue from step 3 on page 72.

NOTE: Initially, the default traffic policy is unavailable for the Device.

Network traffic policy and device traffic policy configured successfully. The network traffic policy will become available to assign to the aggregate traffic policy, and the device traffic policy will become available to assign to the device traffic policy while configuring the **Managed Connected Network**. For details, see *Audit Access Networks* on page 44.

In addition to this, the device traffic policy will become available to assign to the specific MAC address while configuring the **Other Settings**.

Perform **Audit Other Settings**.

2.6 Audit Other Settings

You can configure the global device traffic policy, static route, US internet and firewall, and DNS proxy. The global settings will override the network (VLAN) policy. It is not recommended to modify the configurations for the K4 OneDome.

1. Click → on the **Traffic Profiles** page or click **Other Settings**. The **Other Settings** page appears, see *Figure 2-46*.

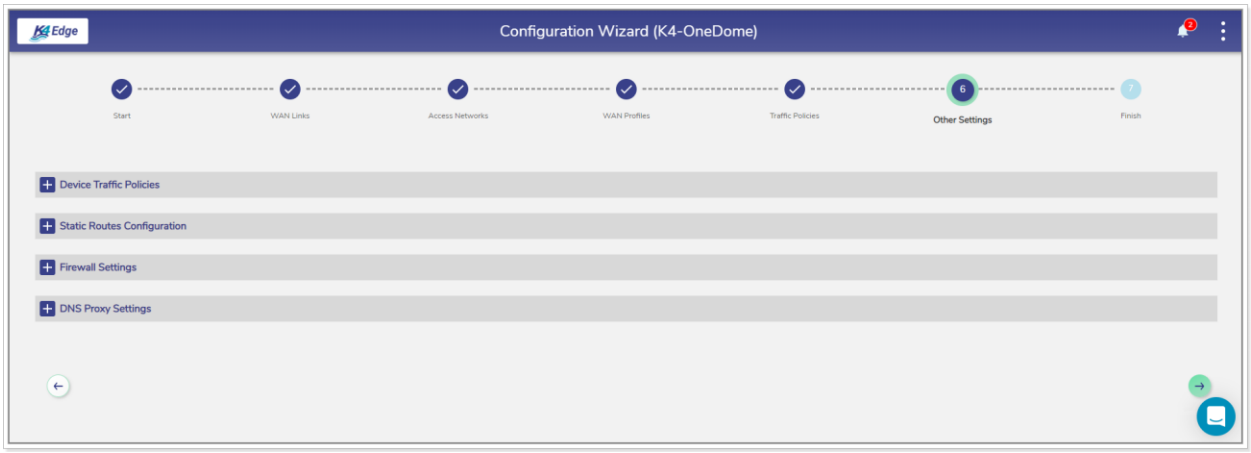

Figure 2-46 Other Settings

2. Click **Device Traffic Policies**. The **Add Device** and **Device Traffic Policies** section becomes available, see *Figure 2-47*. To enter data in the respective fields, see *Table 2-8*.

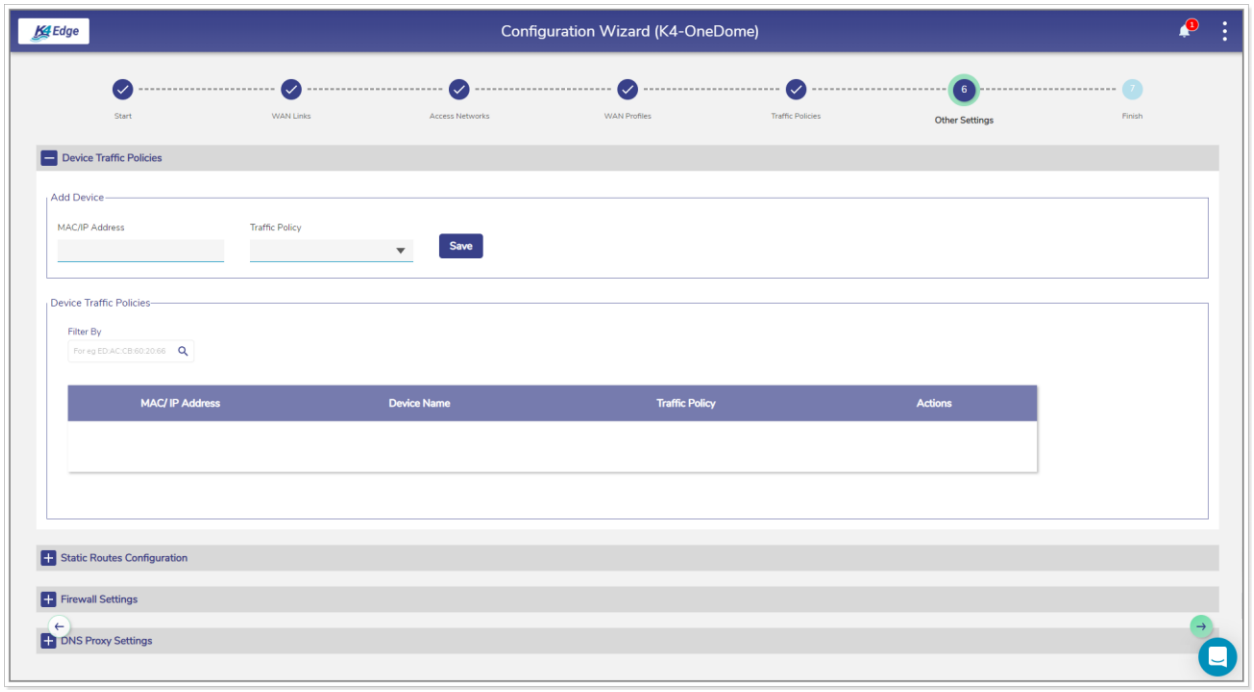

Figure 2-47 Device Traffic Policy

NOTE: Initially, the **Default Network** is available. You can configure multiple traffic policies. Once, the traffic policies are configured, the traffic policies become available on the **Traffic Policies** page.

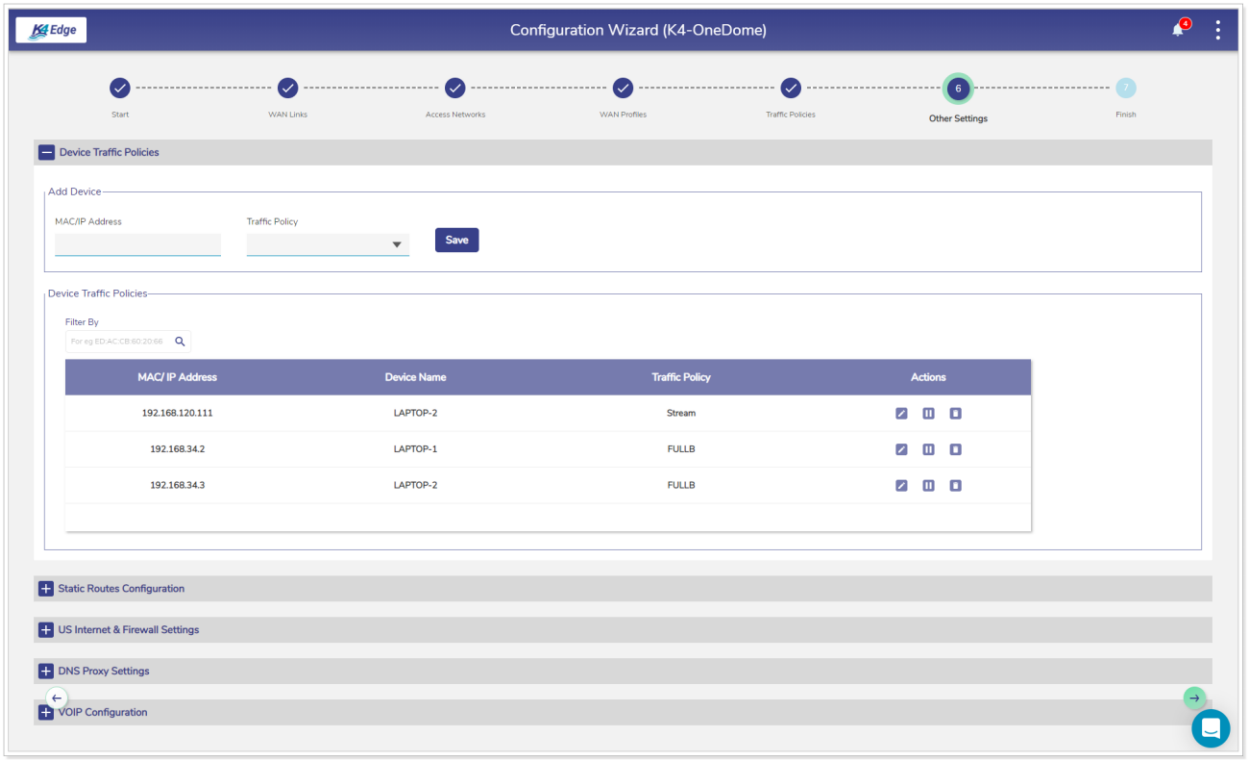

Figure 2-48 Devices and Assigned Device Traffic Policy

Table 2-8 Device Traffic Policies Information

Fields	Description	
Add Device	MAC/IP Address	Enter the MAC or IP address of a device. Or, Click the box and select a MAC or IP address. **NOTE:** The devices connected to the entire network become available.
	Traffic Policy	In the **Traffic Policy** list, click a traffic policy to be assigned to the MAC or IP address specified in the MAC/IP Address field and then click **Save**. **NOTE:** The device traffic policy created while configuring the traffic policies will become available. For details about the traffic policy, see *Audit Traffic Policies* on page *71*. You can assign the traffic policy to a device from also **Step 3: Access Networks**. For details, see *Audit Access Networks* on page *44*. However, the traffic policy last assigned to a device from any step will override the traffic policy of that device. Following is an example. Previously, the traffic policy was assigned to a device from **Step 3: Access Networks**. A new traffic policy is assigned to a device from **Step 6: Other Settings**. Therefore, the traffic policy assigned to a device from **Step 6: Other Settings** will override the existing traffic policy of that device.
Device Traffic Policies or Filter By		Details about the MAC or IP address become available under the **Device Traffic Policies** or **Filter By** section. **To assign a new traffic policy to a MAC or IP address, perform the following steps.** 1. Click  corresponding to the MAC/IP address. The box becomes available corresponding to the MAC/IP address. 2. Click and select a new traffic policy is to be assigned to the MAC/IP address. Or, To stop the traffic policy of a MAC/IP address, click  corresponding to the MAC/IP address.

Fields	Description
	The device basis on the MAC/IP address in the network will stop. To resume the traffic policy, click **Resume**. Or, **To delete the traffic policy of a MAC/IP address, perform the following steps.** 1. Click corresponding to the MAC/IP address. The confirmation message box appears. 2. Click **OK**.

3. Click **Static Route Configuration**. The **Add Static Routes** section becomes available, see *Figure 2-49*.

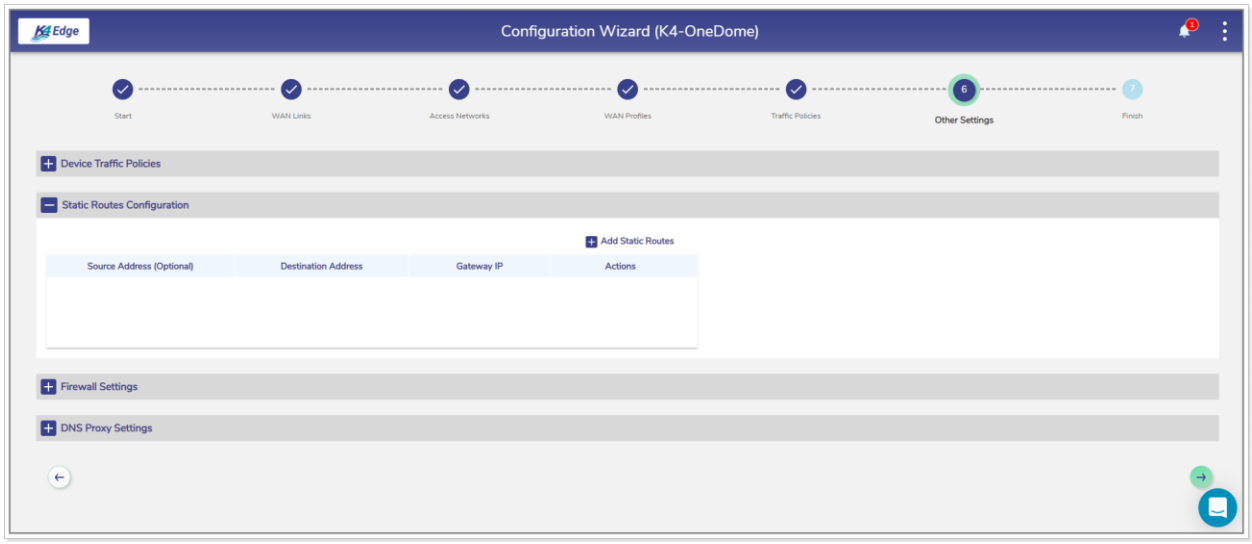

Figure 2-49 Add Static Route

4. Click **Add Static Routes**. The route section becomes available, see *Figure 2-50*. To enter data in the respective fields, see *Table 2-9*.

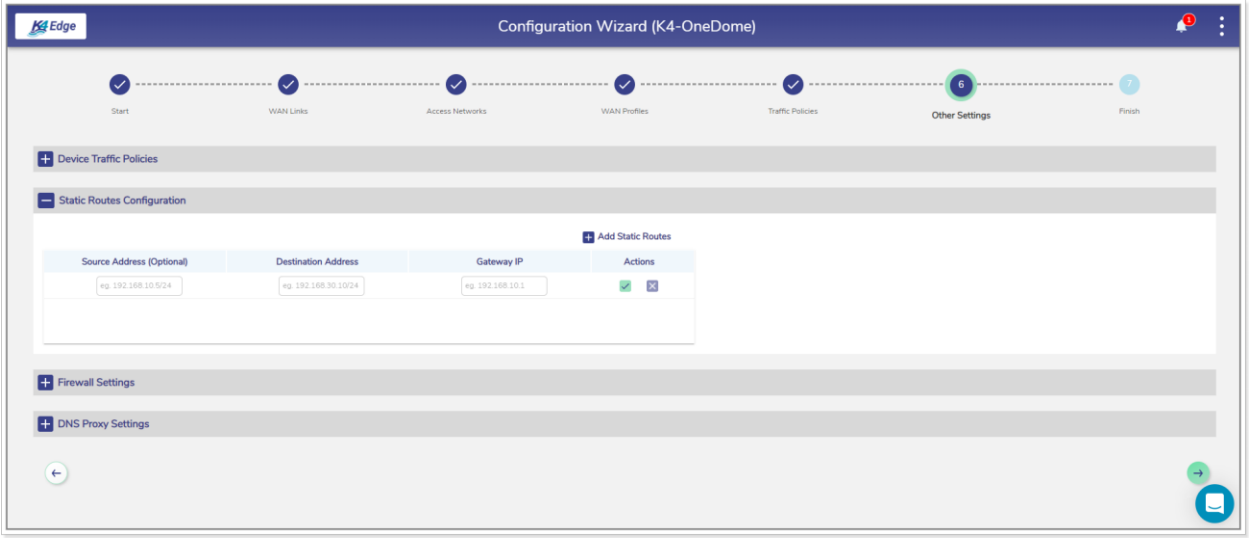

Figure 2-50 Add Static Route

Table 2-9: Static Route Information

Fields	Description
Source Address (Optional)	Enter the source IP address and subnet mask.
Destination Address	Enter the destination IP address and subnet mask that is to be routed to a specific router.
Gateway IP	Enter the IP address of the router to which the traffic is to be routed. This indicates that the traffic with a source IP address and a destination IP will be routed to the router with an IP address specified in the Gateway IP field. This is an example. Source Address (Optional) 92.168.10.5/24 Destination Address 192.168.10.5/24 Gateway IP 192.168.10.1 The traffic with a source IP address/subnet mask 92.168.10.5/24 and a destination IP address/subnet mask 192.168.10.5/24 will be routed to a router with an IP address 192.168.10.1.
Action	Click .

5. Click **Firewall Settings**. The **Firewall Settings** section becomes available, see *Figure 2-51*.

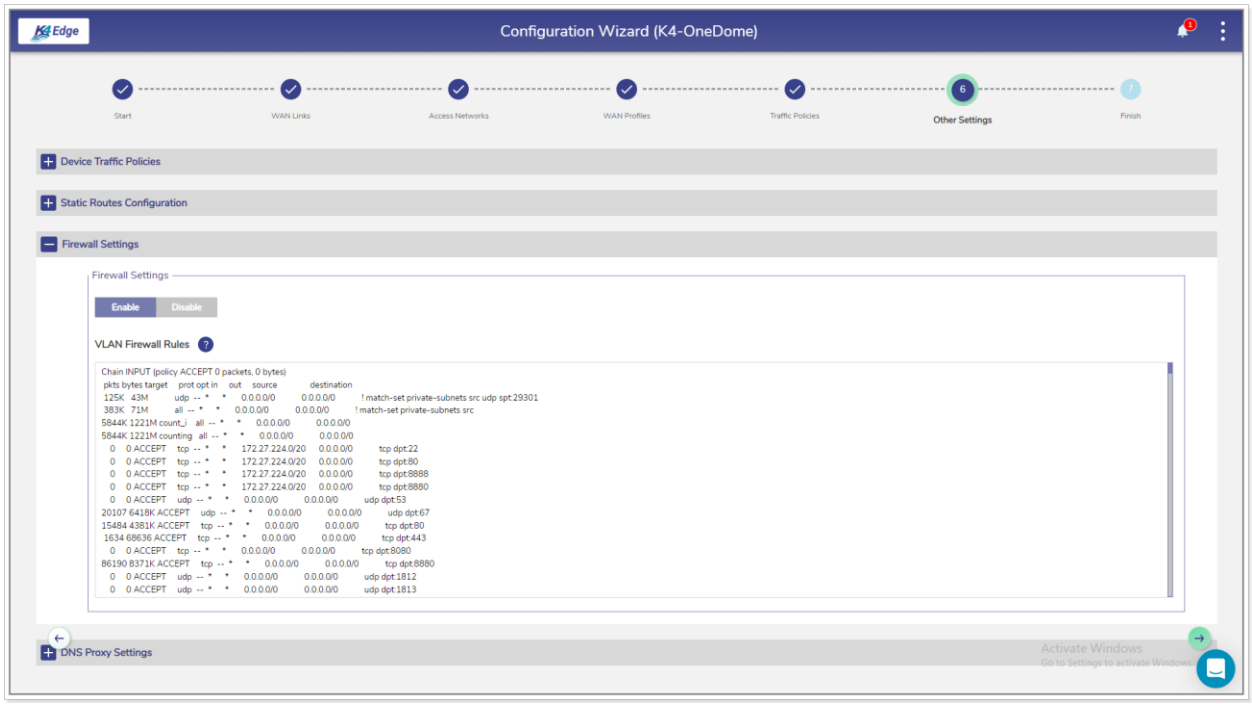

Figure 2-51 US Internet & Firewall Settings

6. To enable the firewall settings, click **Enable**.

   Or,

   To disable the firewall settings, click **Disable**.

   For details about the firewall settings, click ? next to the **VLAN Firewall Rules**.

7. Click **DNS Proxy Settings**. The **Domain/Host Mapping**, **DNS Forwarder**, and **DNS Cache** sections become available, see *Figure 2-52*. To enter data in the respective fields, see *Table 2-10*.

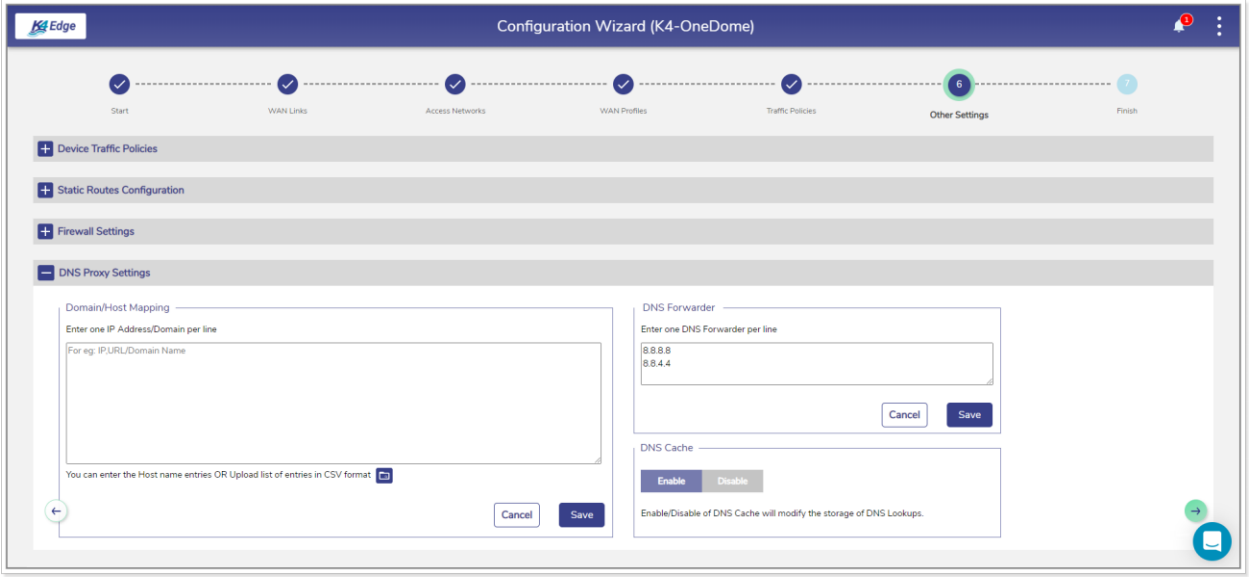

Figure 2-52 Configure DNS Proxy

Table 2-10: DNS Proxy Information

Fields	Description
Domain/Host Mapping	1. Enter an IP address and suffix domain on a single line. 2. Click **Save**. Or, 1. To configure multiple domains and host mapping, enter the IP address and suffix domain on a distinct line, and perform this step on every line. Or, You can upload the list of the domain/host mapping also in the Comma Separated Value (CSV) format. For this, click and upload the CSV file. 2. Click **Save**.
DNS Forwarder	1. Enter only one DNS forwarder on every line. 2. Click **Save**.
DNS Cache	To enhance the DNS lookups, click **Enable**.

The other settings are successfully configured.

Perform **Step 7: Finish**.

2.7 Step 7: Finish

Click  on the **Other Settings** page or click **Finish**. The **Finish** page appears, see *Figure 2-53*.

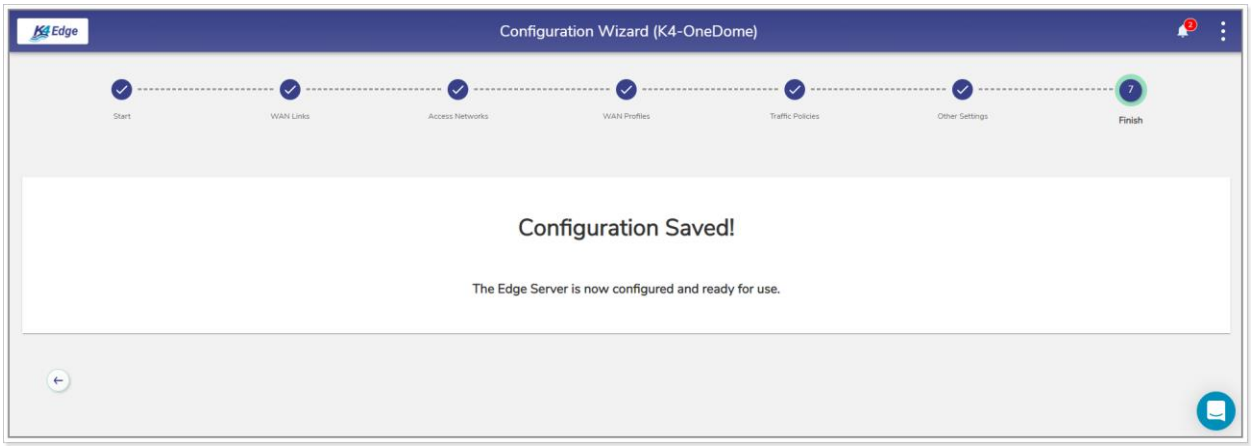

Figure 2-53 Finish

The K4 OneDome is configured successfully.

3 Monitoring

You can monitor the LTE 1, LTE 3, and LTE 2, the performance of the WANs, and track the usage of the WANs.

3.1 Monitoring Alerts

System alerts are raised based on the following scenarios.

19. When VLAN/Device/Enterprise User consumptions exceed thresholds.
20. Traffic will pause on the VLAN/Device/Enterprise User.
21. Active Internet Sources is unavailable.

Following are the severity levels of the system alerts.

22. Critical
23. Major
24. Minor
25. Info
26. Warning

To view the alerts, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click the bell icon, see *Figure 2-5*. The **Notifications** pop-up window appears, see *Figure 3-1*.

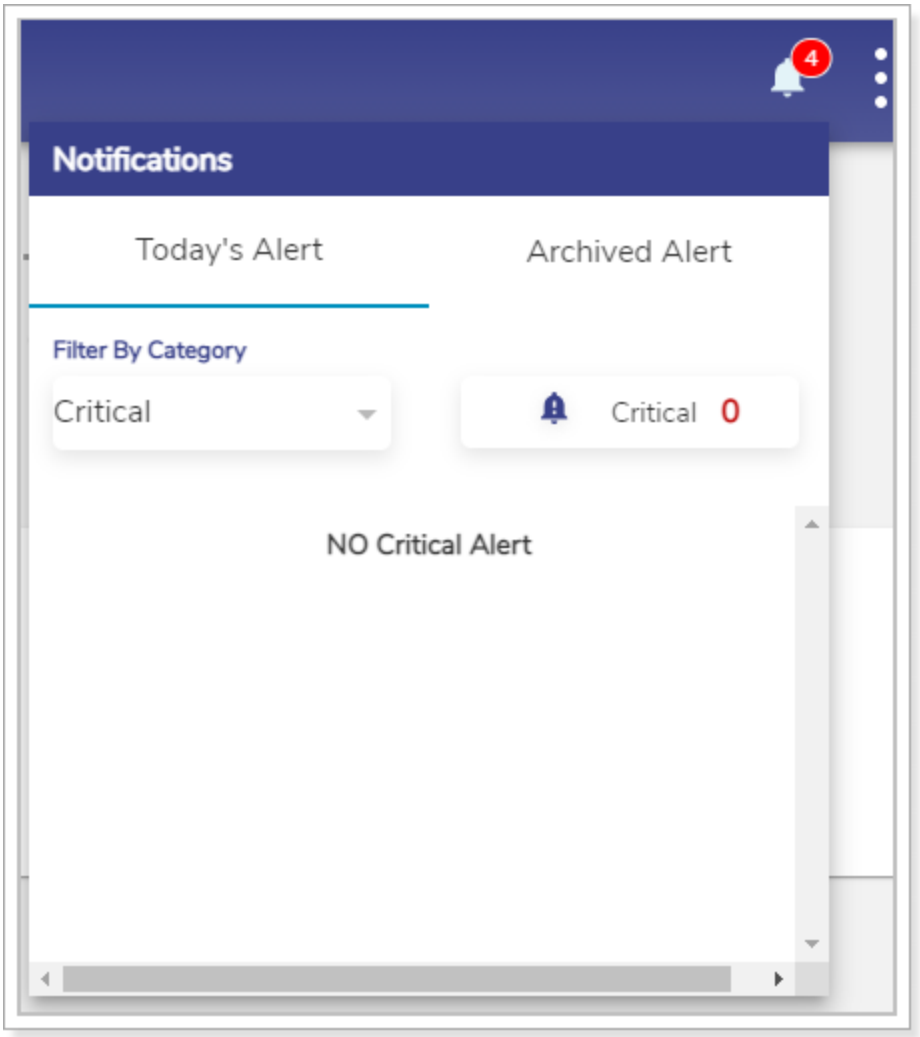

Figure 3-1 Alerts and Notifications

The count of the alerts is displayed over the bell icon, see *Figure 3-1*.

3. Click **Today's Alert**. The current day alerts will become available under the **Today's Alert** tab.
4. You can filter the alerts based on the severity levels. For this, click the drop-down arrow under the **Filter By Category** section. Details about the alerts are displayed. In addition to this, the count of the alerts based on the severity level is displayed.
5. Click **Archived Alert**. The entire alerts up to the previous day are automatically archived and will become under the **Archived Alert** tab.

3.2 Monitoring K4 Edge

After configuring the K4 OneDome, you can perform the following tasks.

27. View details about your account.
28. View details about the system.
29. Access the K4 Edge Configuration Wizard.
30. View the current status of the WAN links.
31. View the performance chart.
32. View the usage status.
33. View the Bonding performing with the Weighting menu.

3.2.1 My Account

To view details about the account, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.

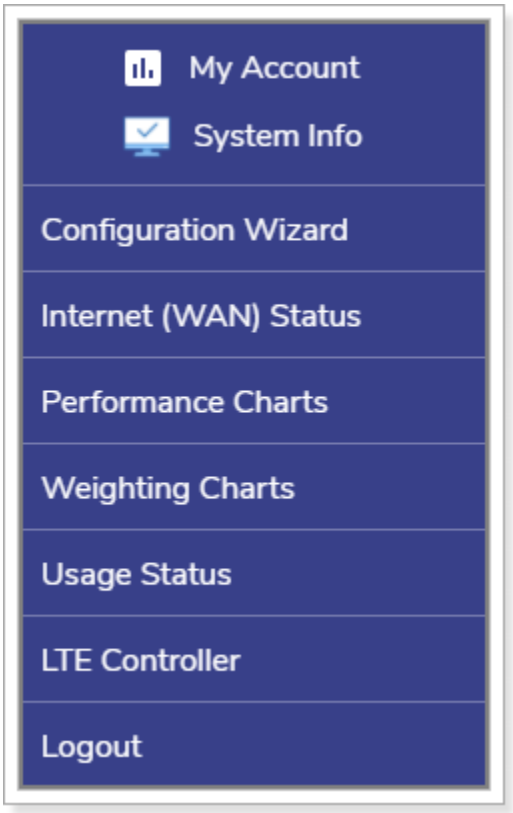

Figure 3-2 Options

3. Click **My Account**. The account details become available, see *Figure 3-3*.

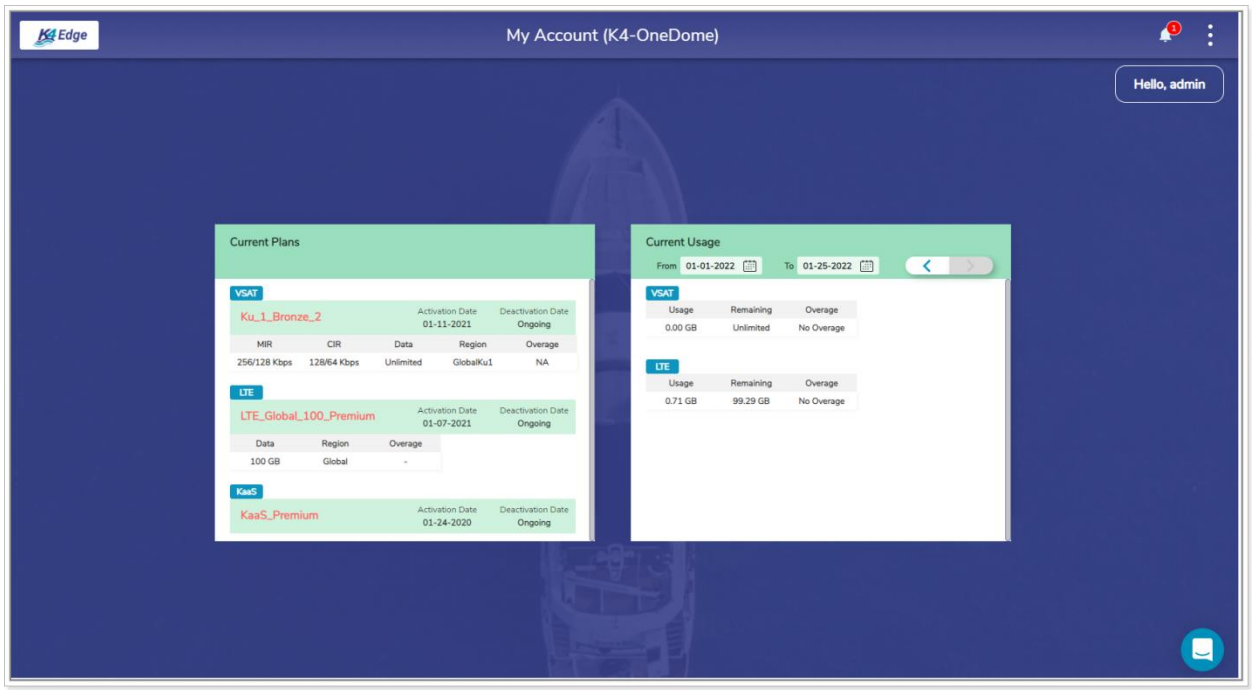

Figure 3-3 Information about Account

Following details become available.

34. **Current Plans**. This indicates the current plans of the entire WAN links available to the vessel.

35. **Current Usage**. This indicates the internet usage on the vessel based on the billing cycle of the WAN link.

3.2.2 System Information

To view details or information about the system, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **System Info**. The **System Information** pop-up window appears, see *Figure 3-4*. For details about the system information, see Table 3-1.

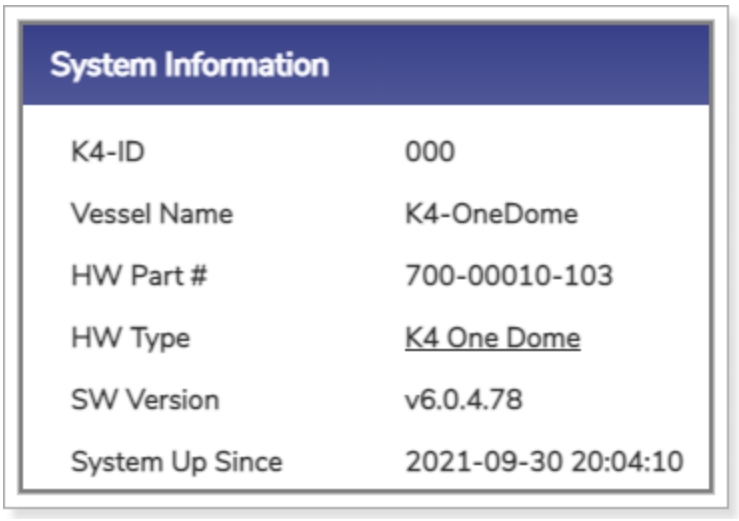

Figure 3-4 System Information

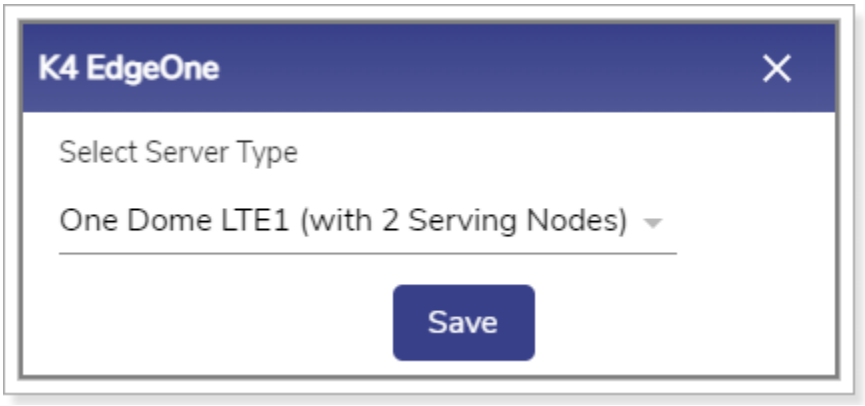

Figure 3-5 Configure Server with Serving Nodes

Return

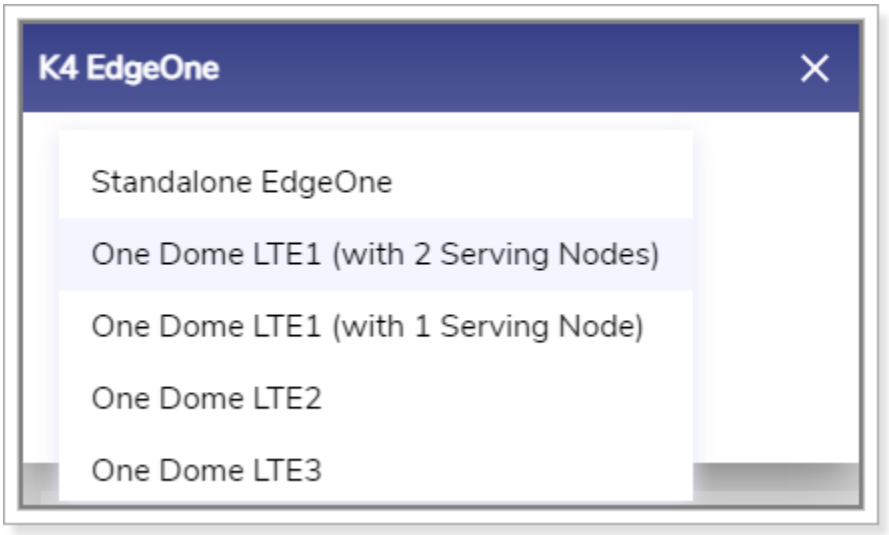

Figure 3-6 Service Nodes List

Return

Table 3-1 Details about System

Fields	Description	Configuration
K4-ID	This value is specified while registering your vessel.	NA
Vessel Name	This is the name of your vessel which is specified while installing the K4 Edge Server.	NA
HW Part #	This is a unique part number of the parent K4 EdgeOne. The five (5) numeric digits **(10-103)** from the right indicate the hardware number of the parent K4 EdgeOne.	NA
HW Type	This is the name of the parent K4 EdgeOne that you are accessing through the K4 Edge Configuration Wizard to connect to the K4 OneDome.	**To configure the OneDome server with the serving nodes, perform the following steps.** 1. Click the **K4 OneDome**. The K4 EdgeOne pop-up window appears, see *Figure 3-5*. 2. To configure the server with 2 serving nodes, click **OneDome** LTE1 **(with 2 Serving Node)** in the Select Server Type list, see *Figure 3-6*. Therefore, LTE1, LTE2, and LTE3 WAN links become available. Or, To configure the server with a single serving node, click **OneDome LTE1 (with 1 Servin**g **Node)** in the Select Server Type list, see *Figure 3-6*. Therefore, LTE1 and LTE2 WAN links become available. **NOTE:** The parent K4 EdgeOne is the K4 One Dome LTE 1. In addition to this, the K4 One Dome LTE 2 and K4 One

Fields	Description	Configuration
		Dome LTE 3 are the child K4 EdgeOne. The parent K4 EdgeOne can access the child K4 EdgeOne. 3. Click **Save**.
SW Version	This is the version of the K4 Edge Configuration Wizard used to configure the WAN profiles.	
System Up Since	This is the date and time stamp when the system is up.	

3.2.3 Configuration Wizard

To access the K4 Edge Configuration Wizard, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Configuration Wizard**. The home page appears, see *Figure 2-4*.

For details, see *Commissioning K4 OneDome* on page *31*.

3.2.4 Internet (WAN) Status

Once the K4 Edge is configured, you can monitor the status of the internet status or WAN links of the vessel.

To view internet status, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-7*.

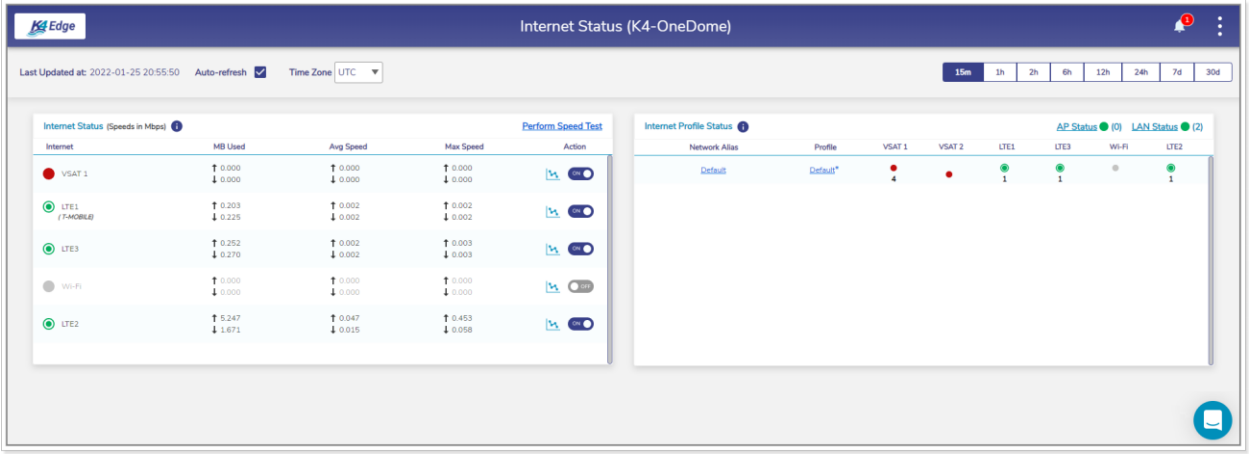

Figure 3-7 Internet Status

NOTE: Initially, the **Default** network and the **Default** profile are available. You can configure multiple networks and profiles.

Initially, the Wi-Fi is unavailable as AP Mode is enabled.

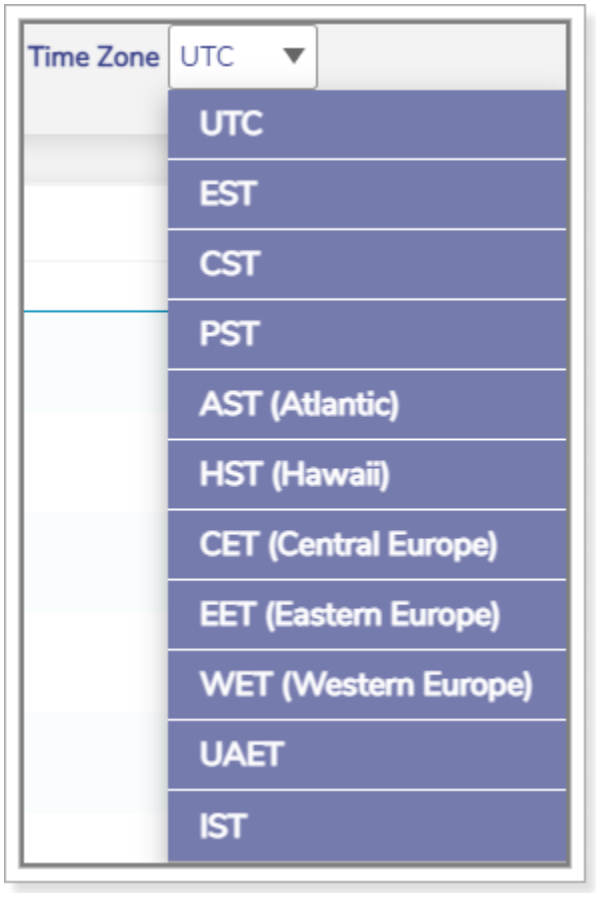

Figure 3-8 Time Zone

Return

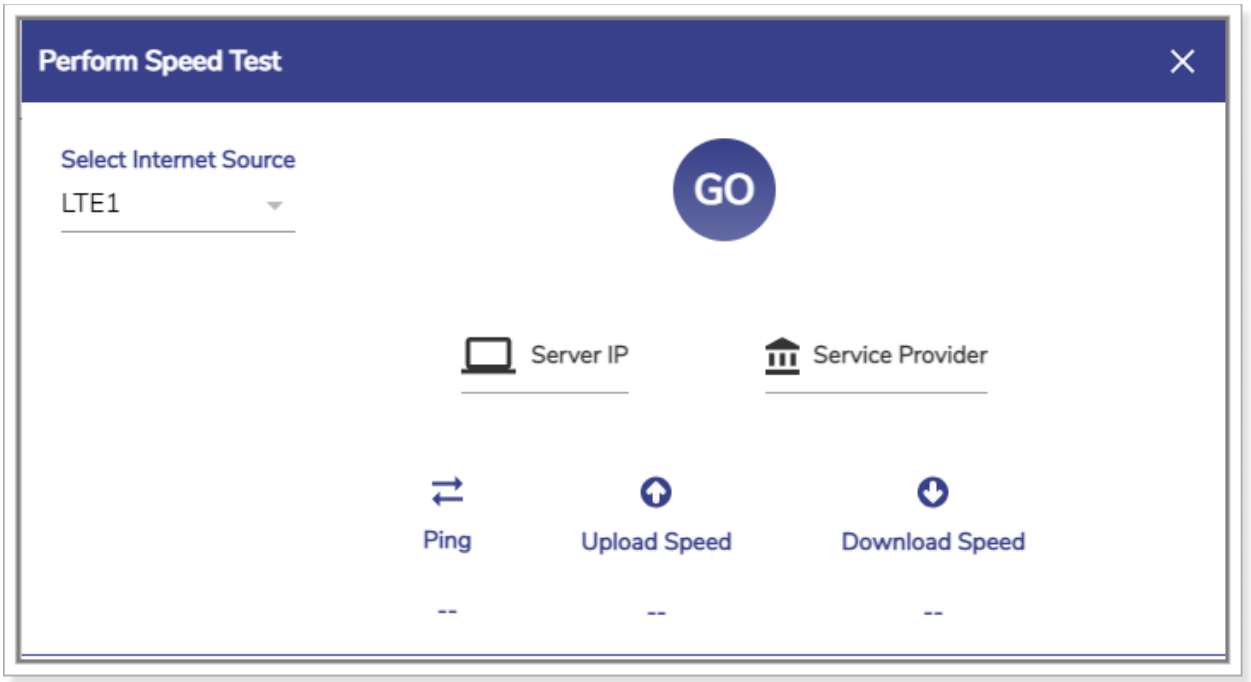

Figure 3-9 Perform Speed Test

Return

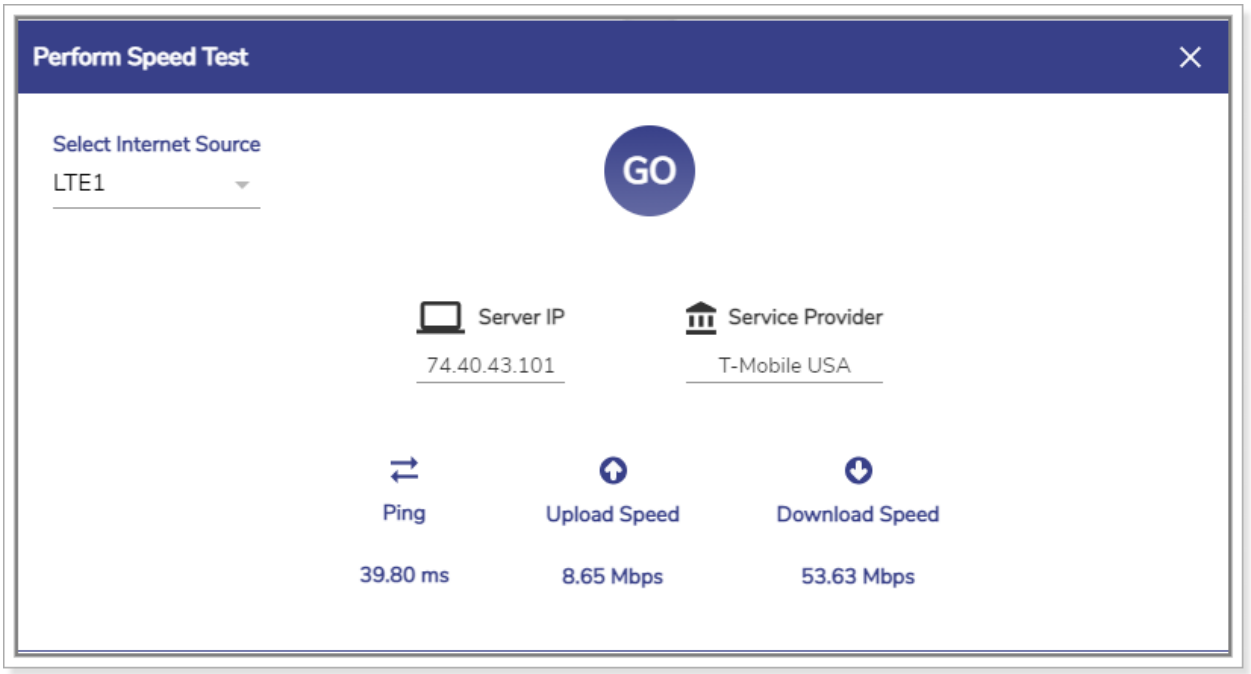

Figure 3-10 Speed Test Result

Return

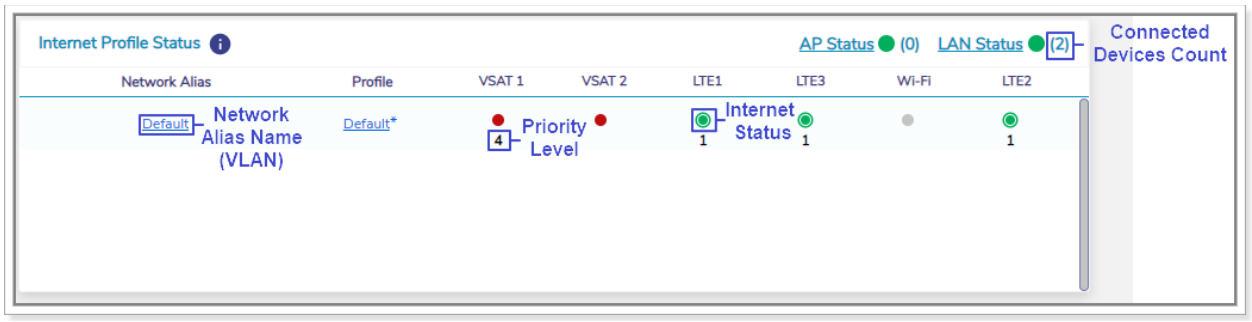

Figure 3-11 Internet Profile Status Details

Return

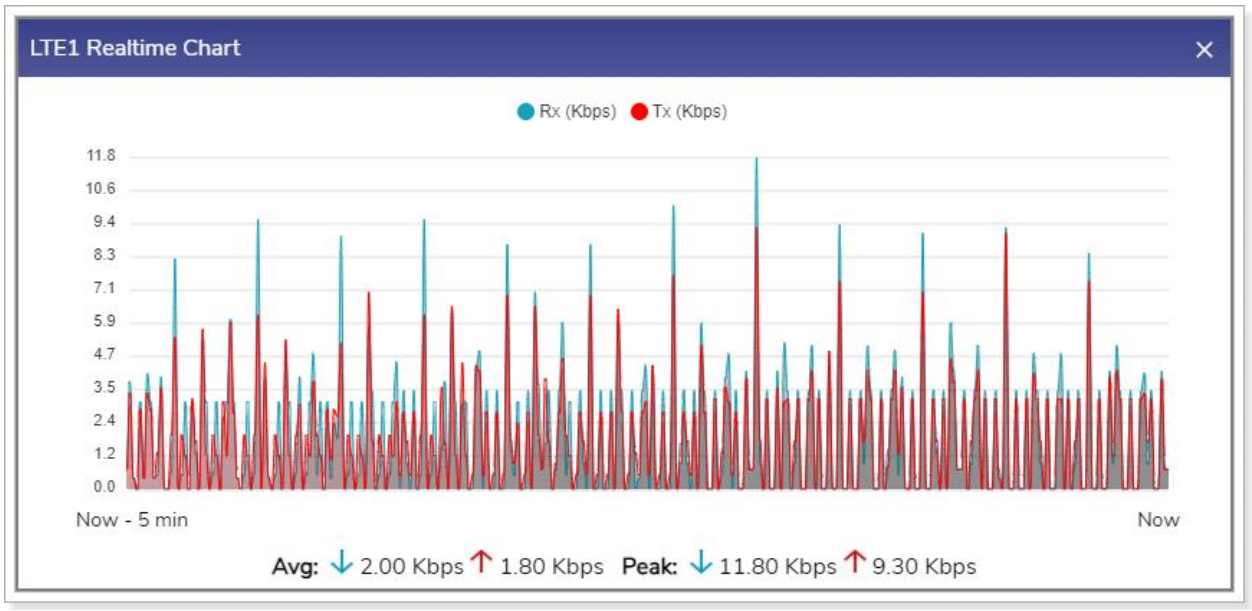

Figure 3-12 LTE Real time Chart

Return

Figure 3-13 Disable LTE Confirmation Message

Return

Figure 3-14 Enable LTE Confirmation Message

Return

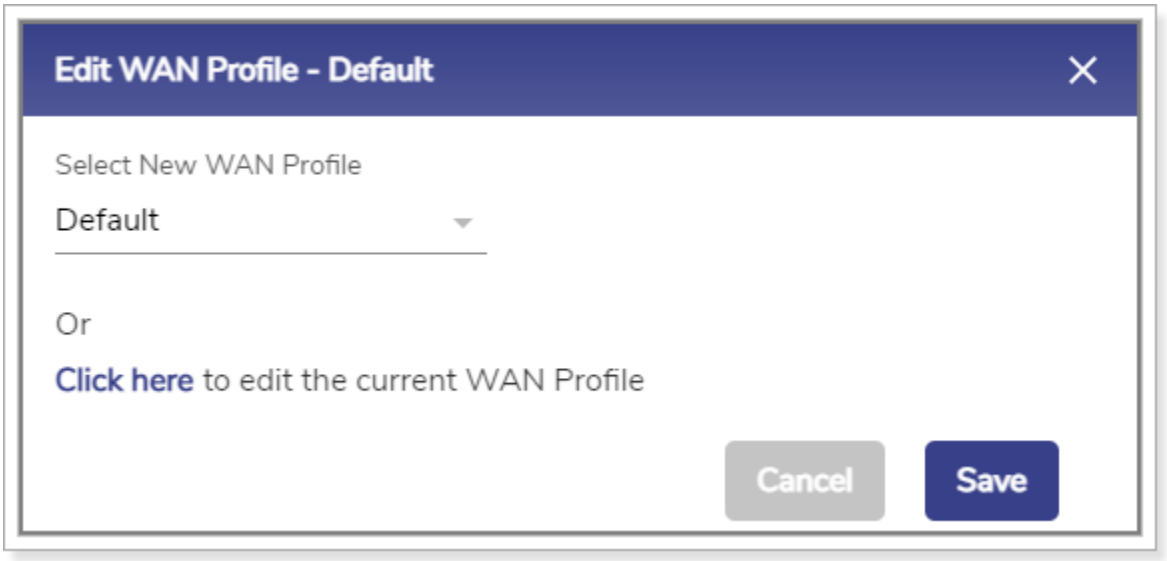

Figure 3-15 Modify WAN Profile

Return

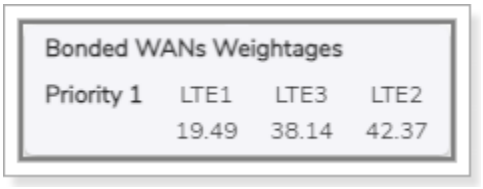

Figure 3-16 Bonded WAN Weightage

Return

Table 3-2 WAN Status Information

Fields	Description	Configuration
Auto-refresh	Whether the data on the page is to be refreshed automatically.	To automatically refresh the details about the WAN link, click the **Auto-refresh** check box.

Fields	Description	Configuration
	Data is updated at an interval of 30 seconds.	
Time Zone	To access the details about the WAN link basis on the time zone. By default, the UTC is configured.	In the **Time Zone** link, click a time zone, see *Figure 3-8*.
	To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where, • m is minutes • h is hours • d is days By default, the periodicity of 15m is configured.	Click the periodicity at the upper-right corner of the page.
Internet Status		
Internet Status	To view the status, speed, and operators of the WAN link or internet.	To view details about the internet status, point the mouse to  .
Internet	Following are the statuses of the internet. •  . Active. This indicates that the corresponding WAN link or internet is working and being used by the users on the vessel and the internet traffic is moving through that WAN link or internet. •  . Standby. This indicates that the corresponding WAN link or internet is working but not being used by the users on the vessel and the internet traffic is	To access the controller of the respective WAN link or internet, click the WAN link or internet. And, To disable or enable the WAN link or internet, click **Action**. To access the controller of the respective WAN, click the WAN link. The respective WAN controller page appears.

Fields	Description	Configuration
	not moving through that WAN link or internet. • . Disabled. This indicates that the corresponding WAN link or internet is disabled. Therefore, the internet will not work and the internet traffic will not move through that link or internet. • . Down. This indicates that the WAN link or internet is not working.	
Real time Chart	To view the real time chart of the WAN link.	To view the real time chart, click under the **Action**. The **Realtime Chart** page appears, see *Figure 3-12*.
Action	To disable or enable the WAN link or internet.	**To disable the internet, perform the following steps.** 1. Switch off **Action**. The **Disable** pop-up window appears, see *Figure 3-13*. 2. Click **Confirm**. Or, **To enable the internet, perform the following steps.** 1. Switch on **Action**. The **Enable** pop-up window appears, see *Figure 3-14*. 2. Click **Confirm**.
Perform Speed Test	Speed test only active internet can be performed.	**To perform the speed test, perform the following steps.** 1. Click **Perform Speed Test**. The **Perform Speed Test** page appears, see *Figure 3-9*. 2. In the **Select Internet Source** list, click an internet whose speed test is to be performed.

Fields	Description	Configuration
		NOTE: Before performing the speed test, you must ensure that the internet is up. 3. Click **GO**. The speed test result becomes available, see *Figure 3-10*.
Internet Profile Status		
Internet Profile Status	To view details about the profile of the WAN link or internet.	To view details about the internet profile status, point the mouse to  . For details, see *Figure 3-11*.
LAN Status		To access details about the network, click **LAN Status**. The **Access Networks** page appears, see *Figure 2-12*.
AP Status	This allows the devices that have the wireless capability to connect to the local network.	Initially, the AP Mode is enabled and Wi-Fi is unavailable. Therefore, you cannot configure the Marina Wi-Fi and cannot access the captive web portal. To connect to the local network, you must enable the AP mode, see *Enabling AP Mode* on page *107*.
Network Alias		**To assign the new WAN profile, perform the following steps.** 1. Click the WAN. The **Edit WAN Profile** pop-up window appears, see *Figure 3-15*. 2. In the **New WAN Profile** list, click the WAN profile. 3. Click **Save**. The WAN profile is changed.
		To modify the current WAN profile, perform the following steps. 1. Click the WAN. The **Edit WAN Profile** pop-up window appears, see *Figure 3-15*.

Fields	Description	Configuration
		2. Click the **Click here** link. The **WAN Profiles** page appears. To modify the WAN profile, see *Audit WAN Profiles* on page 66. The WAN profile is changed.
Profile	The name of the WAN or internet profile is displayed. The default bonded WAN profile is reflected as **Bonded***.	To view the bonded weightage of the default bonded WAN profile, point the mouse to the WAN profile. The **Bonded WANs Weightages** pop-up window appears, see *Figure 3-16*. To modify the WAN profile, click the profile. The WAN Profiles page appears. To modify the WAN profile, see *Audit WAN Profiles* on page 66.

3.2.4.1 Enabling AP Mode

To enable AP Mode, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-7*.
4. Click **AP Status**. The **Wi-Fi Settings** pop-up window appears, see *Figure 3-17*. To enter data in the respective fields, see *Table 3-3*.

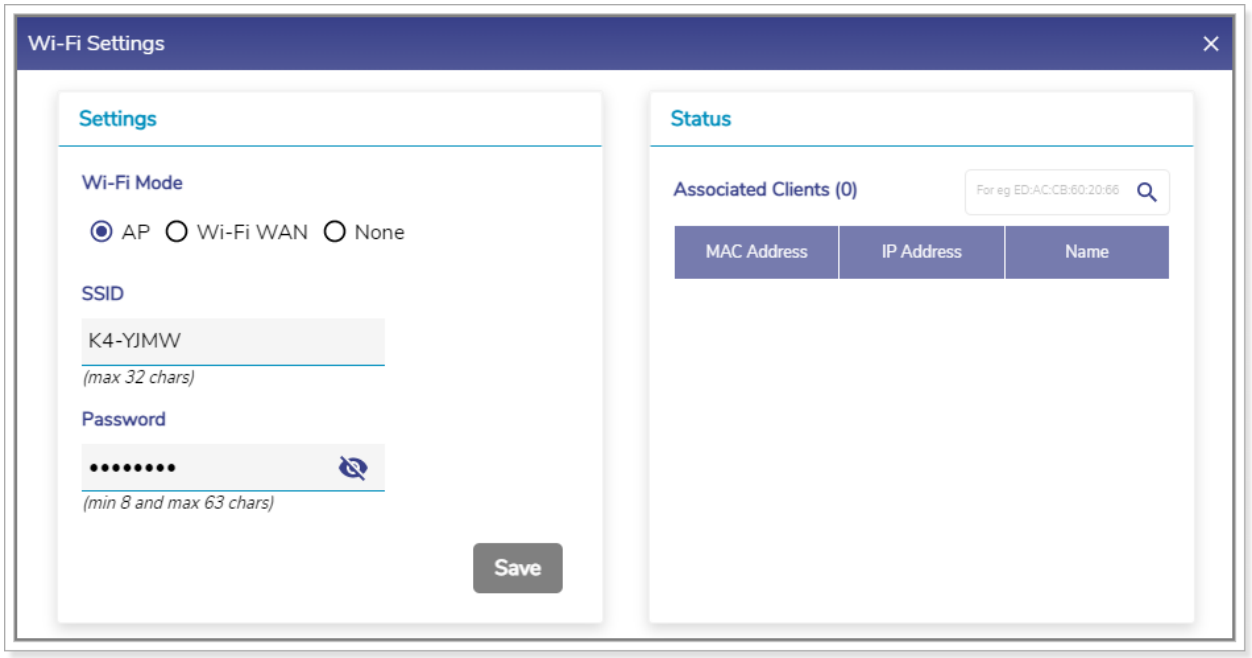

Figure 3-17 Wi-Fi Settings

Table 3-3 AP Status Information

Fields	Description
Settings	
Wi-Fi Mode	Click **AP**. By default, the **AP** option is selected.
SSID	Enter the unique name of the SSID.
Password	Enter the password.

5. Click **Save**.

The AP Mode is enabled and the device can connect to the network through the AP using the SSID and password. The count of the devices connected is displayed next to the **Associated Clients** under the **Status** section on the **Wi-Fi Settings** pop-up window. In addition to this, details of the devices connected using that SSID are displayed under the **Associated Clients** section.

Additionally, the count of the devices connected is displayed next to the **AP Status** and **LAN Status** on the **Internet Status** page.

The device is connected through the Default VLAN or network. To monitor the usage of the device, see *Usage Status* on page *123*.

3.2.4.2 Enabling Marina Wi-Fi

To enable Marina Wi-Fi, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-7*.
4. Click **AP Status**. The **Wi-Fi Settings** pop-up window appears, see *Figure 3-17*.
5. Click **Wi-Fi WAN**. The **Status** section becomes available, see *Figure 3-18*.

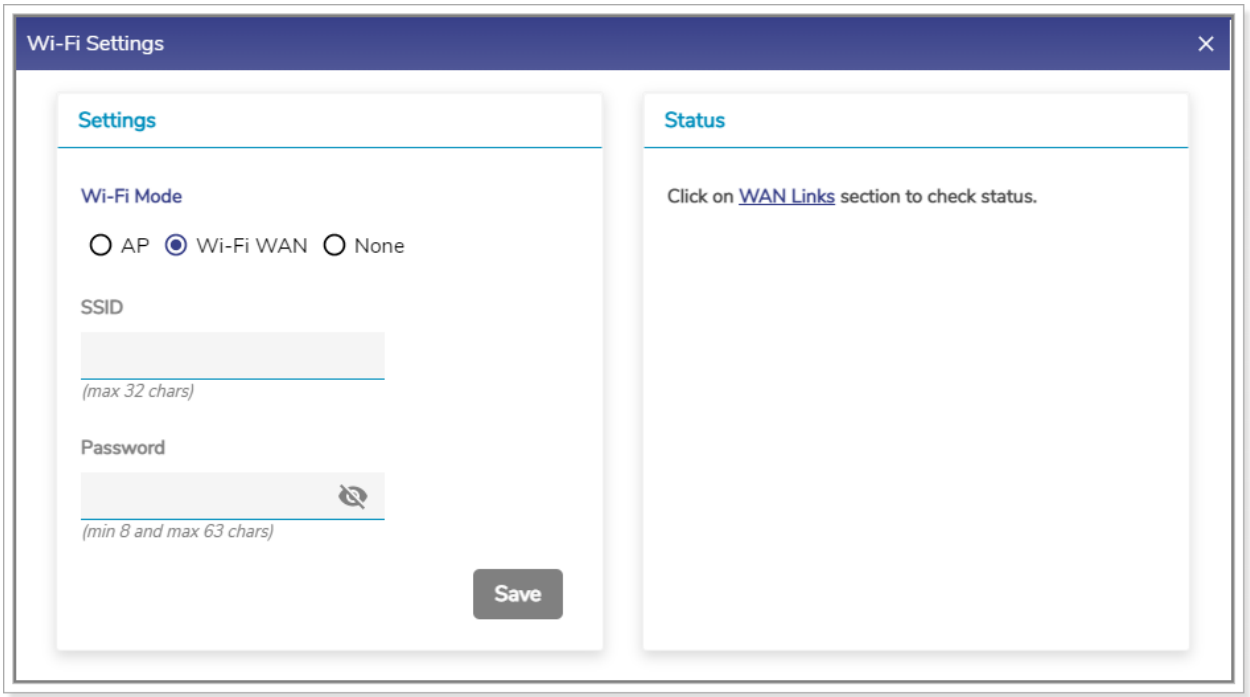

Figure 3-18 Wi-Fi WAN

6. Click **Save**.

The Wi-Fi is enabled and becomes available under the WAN field on the **WAN Links** page. The AP is unavailable, see *Figure 3-19*.

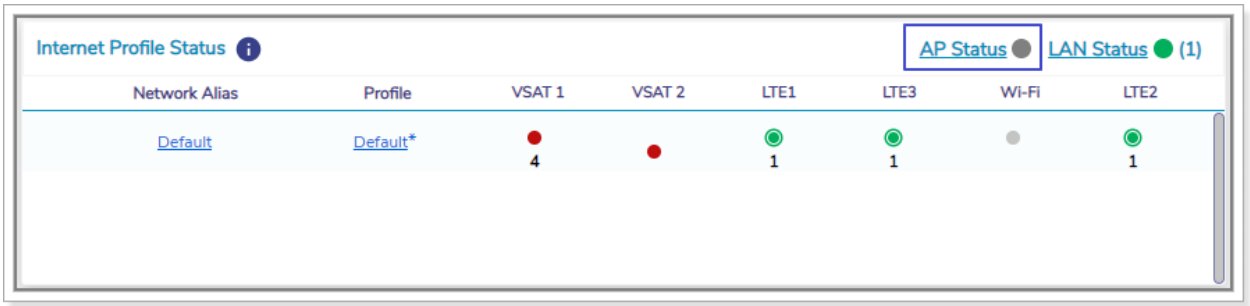

Figure 3-19 AP Status

In addition to this, you can configure the Wi-Fi. For details, see **Managing** Wi-Fi Controller on page *154*.

To block AP and Wi-Fi, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. **Internet Status** page appears, see *Figure 3-7*.
4. Click **AP Status**. The **Wi-Fi Settings** pop-up window appears, see *Figure 3-17*.
5. Click **None**.

The AP and Wi-Fi are unavailable. Therefore, the device can connect to the network through Ethernet, LTE, and VSAT WANs.

3.2.5 Accessing Captive Web Portal Network

Some Wi-Fi networks may require you to provide additional information, such as a password, payment information or simply acceptance of some condition. This will be accomplished through a ‘captive portal’ web-page. The K4 system will detect whether the Wi-Fi network requires this, and if it does then a ‘captive portal’ icon will be shown against the Wi-Fi WAN on the **WAN Links** page and **Internet Status** page.

The device taking these actions must be connected to the access network, they cannot be remotely connected via connect/VPN.

If the Marina Wi-Fi is enabled (AP Mode is disabled), then you can access the captive web portal.

To access the captive web portal network through the WAN Links page, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click **WAN Links**. The **WAN Links** page appears, see *Figure 3-20*.

Figure 3-20 WAN Links Page with Captive Portal Icon

3. Click the captive portal icon next to the **Wi-Fi** under the WAN field. The **Alert** pop-up window appears, see *Figure 3-21*.

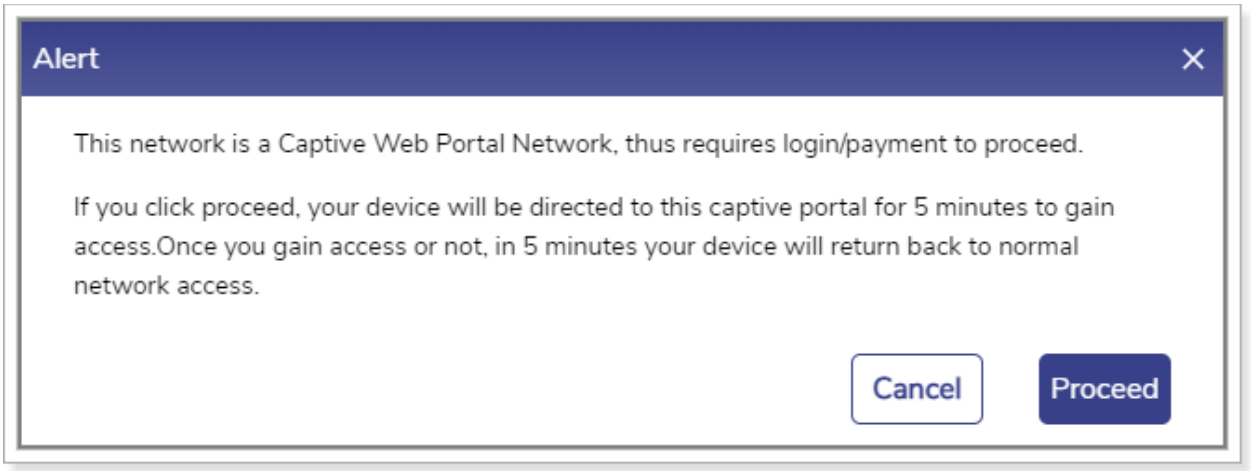

Figure 3-21 Captive Web Portal Alert

4. Click **Proceed**. The captive web portal page appears.

You must log on to the captive web portal within the duration of 5 minutes. If you cannot log on to the captive web portal within the duration of 5 minutes, then your device will return back to normal network access.

Or,

To access the captive web portal network through the Internet Status page, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-22*.

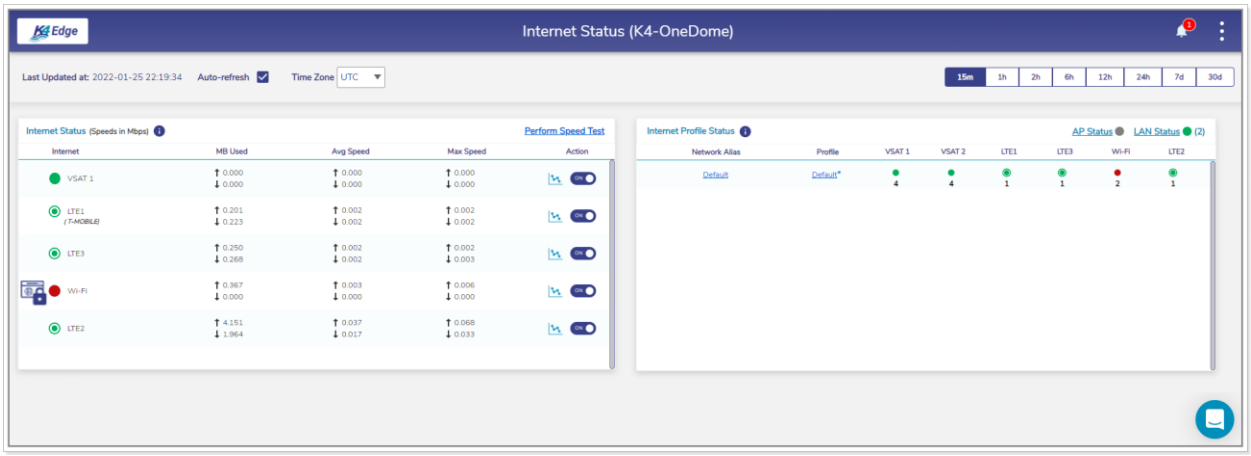

Figure 3-22 Internet Status Page with Captive Portal Icon

4. Click the captive portal icon next to the **Wi–Fi** under the **Internet Status** section, see *Figure 3-23*.

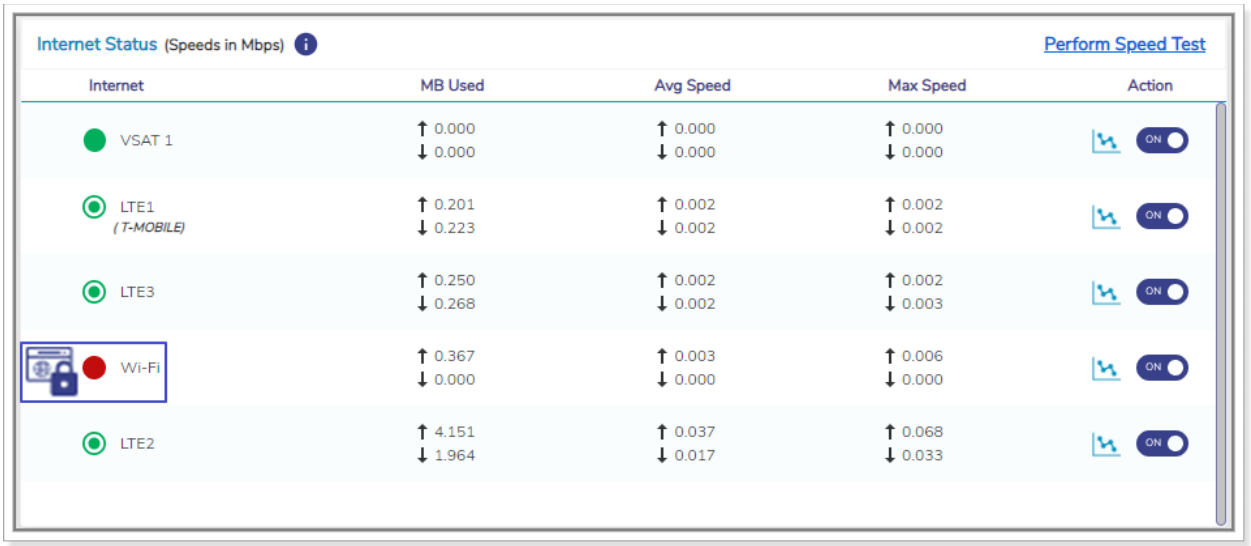

Figure 3-23 Captive Portal Icon

The **Alert** pop-up window appears, see *Figure 3-21*.

5. Click **Proceed**. The captive web portal page appears.

You must log on to the captive web portal within the duration of 5 minutes. If you cannot log on to the captive web portal within the duration of 5 minutes, then your device will return back to normal network access.

3.2.6 WAN Throttling

The K4 defines the throughput of the data of the WAN links. Once the monthly service plan quota is breached, the LTE link is throttled. This indicates that the LTE link speed decreases.

If the service plan quota is refilled, reset, or the service plan is top-up, then the throttled is removed. This indicates that the defined speed is resumed for the LTE link.

To view the LTE link throttle, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-24*.

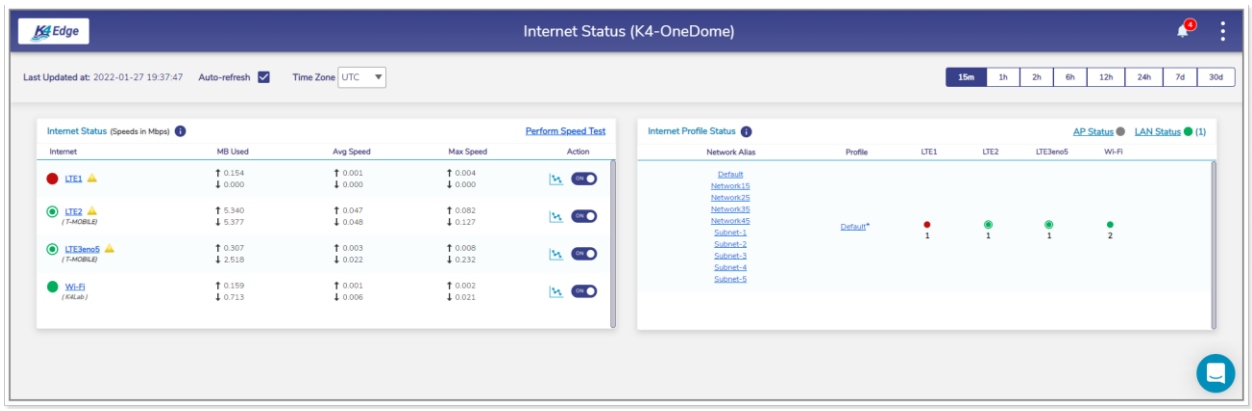

Figure 3-24 WAN Throttle

The throttle icon becomes available next to the LTE link, see *Figure 3-25*.

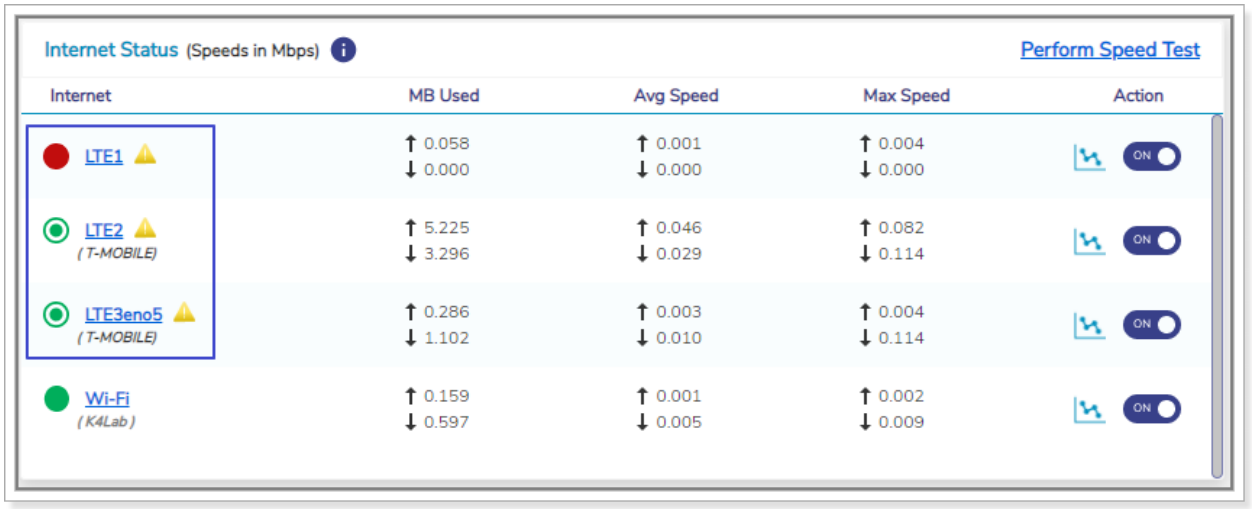

Figure 3-25 LTE Link Throttle Icon

In addition to this, the throttle alert is displayed. To view the alert, click **Notification**, see *Figure 2-5*. The **Notifications** pop-up window appears, see *Figure 3-26*.

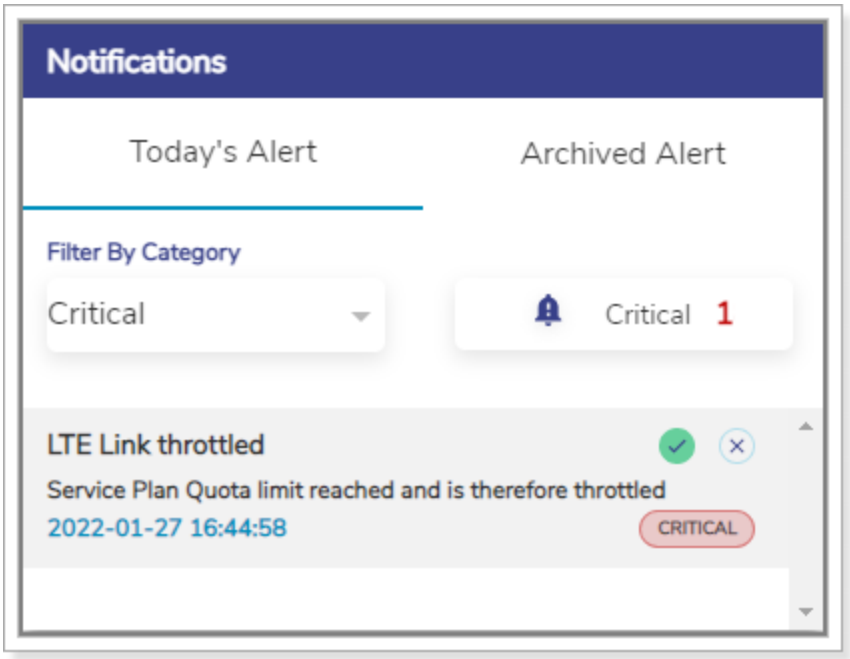

Figure 3-26 LTE Link Throttle Alert

Once the service quota is refilled, the throttle icon is removed and the LTE link speed alert is displayed, see *Figure 3-27*.

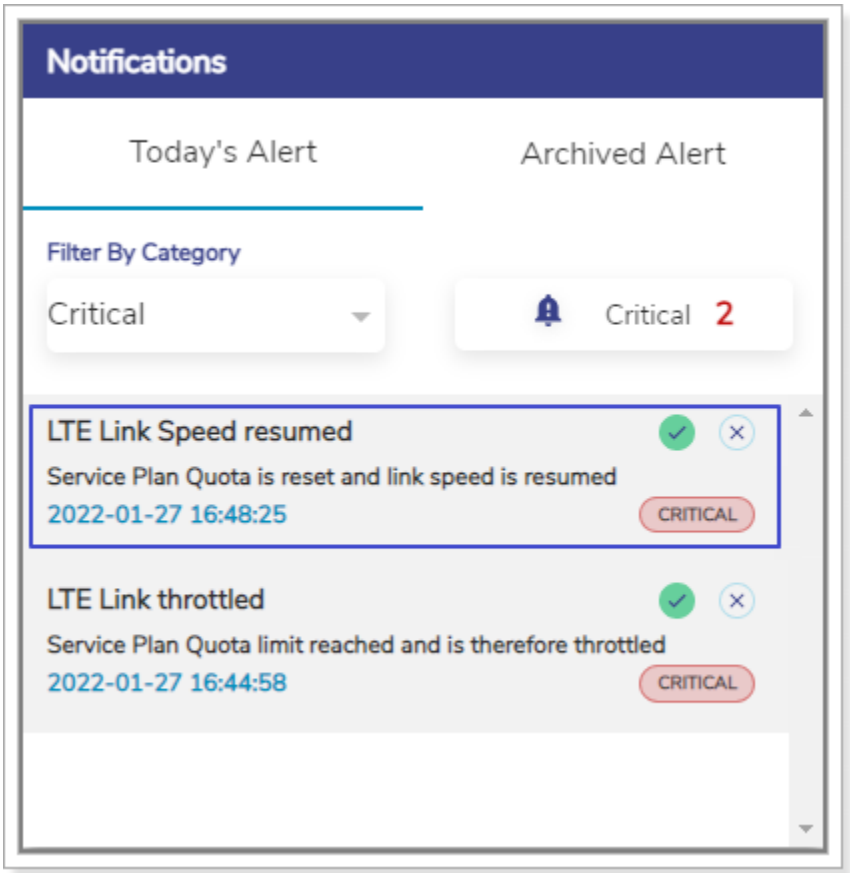

Figure 3-27 LTE Link Speed Resumed Alert

3.2.7 Performance Chart

Once the K4 OneDome is audited and possibly reconfigured, you can monitor the performance of the internet or WAN links of the vessel.

To view the performance charts, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Performance Charts**. The **Performance Charts** page appears, see *Figure 3-28*. For a description, see *Table 3-4*.

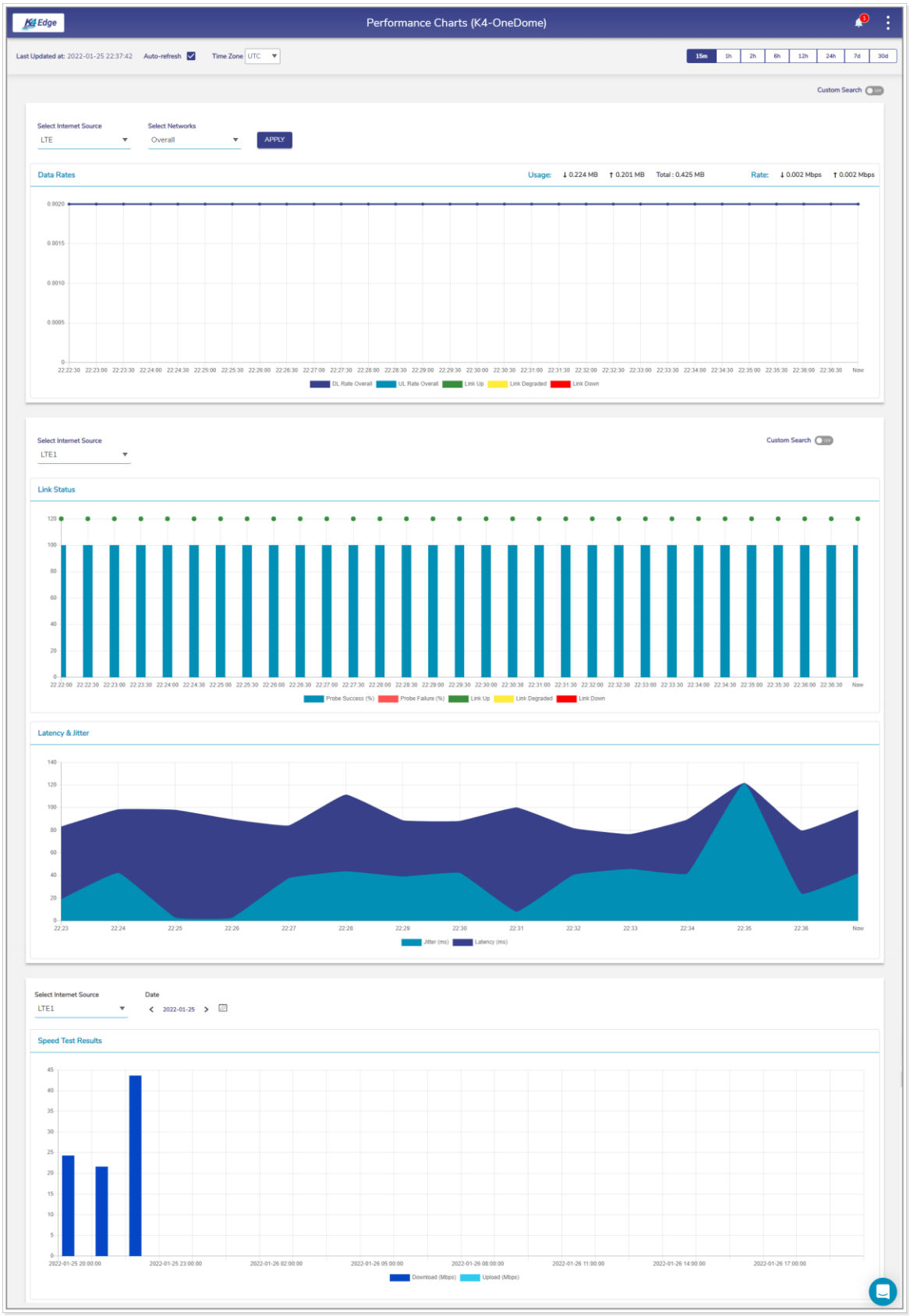

Figure 3-28 Performance Charts

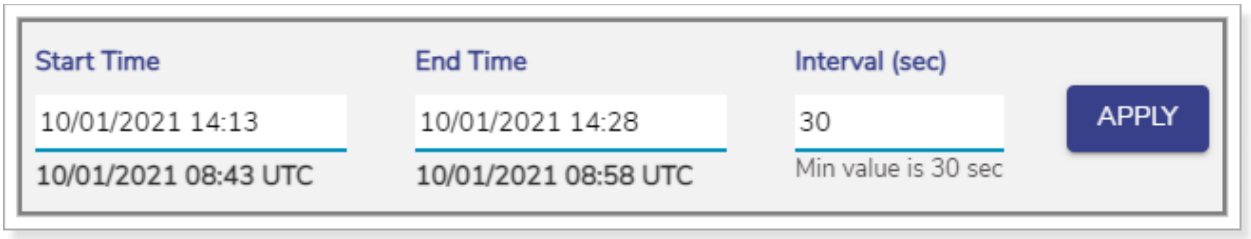

Figure 3-29 Custom Search of Link Status

Return

Table 3-4 Performance Chart Information

Fields	Description	Configuration
Auto-refresh	Whether the data on the page is to be refreshed automatically. Data is updated at an interval of 30 seconds.	To automatically refresh the details about the WAN link, click the **Auto-refresh** check box.
Time Zone	To access the details about the WAN link basis on the time zone. By default, the UTC is configured. To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where, • m is minutes • h is hours • d is days By default, the periodicity of 15m is configured.	In the **Time Zone** link, click a time zone, see *Figure 3-8*. Click the periodicity at the upper-right corner of the page.
Data Rates	DL/UL rates chart of the internet source for a specific network.	**To view the DU/DL rate chart for a network, perform the following steps.** 1. In the **Internet Source** list, click a WAN link or an internet source. 2. In the **Network** list, click single or multiple networks. 3. Click **Apply**. The performance chart is generated.

Fields	Description	Configuration
		To view the network level usages for VSAT and LTE, you must click either VSAT or LTE. The network level usages are not available for the VSAT1, VSAT2, LTE1, LTE2, LT3, and Wi-Fi, and Ethernet WAN links. If the network selected in the **Network** list is not applicable to the internet source selected in the **Internet Source** list, then the alert will be displayed.
Link Status		To view the link status chart for a network, in the **Internet Source** list, click a WAN link or an internet source. The performance chart is generated. **To view the link status chart for a network basis on a day and time, perform the following steps.** 1. Switch on the **Custom Search**. The custom search section appears, see *Figure 3-29*. 2. Click **Start Time**. The calendar becomes available. 3. Select the start day and time. The start day and time becomes available in UTC. 4. Click **End Time**. The calendar becomes available. 5. Select the end day and time. The start day and time becomes available in UTC. 6. In the Interval (sec) field, click the minimum interval specified. 7. Click **Apply**. The chart is generated.
Latency & Jitter	The latency and jitter chart.	NA
Speed Test Results		**To view the Speed Test Results chart, perform the following steps.**

Fields	Description	Configuration
		1. In the **Internet Source** list, click a WAN link or an internet source. 2. Click the calendar in the **Date** field and select the date of when the speed test result chart is to be generated. 3. Click **Apply**. The chart is generated.

3.2.8 Weighting Chart

Once the K4 OneDome is audited and possibly reconfigured, you can view the weighting % of the LTE 1, LTE 3, and LTE 2 at the periodicity of 10 seconds. If the US internet is up, then the **K4 PEP - Peak Rate Estimate** and **K4 PEP - RTT** charts become available. Therefore, the weighting of the LTE 1, LTE 3, and LTE 2 is performed based on the **K4 PEP - Peak Rate Estimate** and **K4 PEP - RTT**. If the US internet is down, then the **Native - Peak Rate Estimate** and **Native - RTT** charts become available. Therefore, the weighting of the LTE 1, LTE 3, and LTE 2 is performed based on the **Native - Peak Rate Estimate** and **Native - RTT**.

To view the weighting %, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Weighting Charts**. The **Weighting Charts** page appears, see *Figure 3-30*. For a description, see *Table 3-5*.

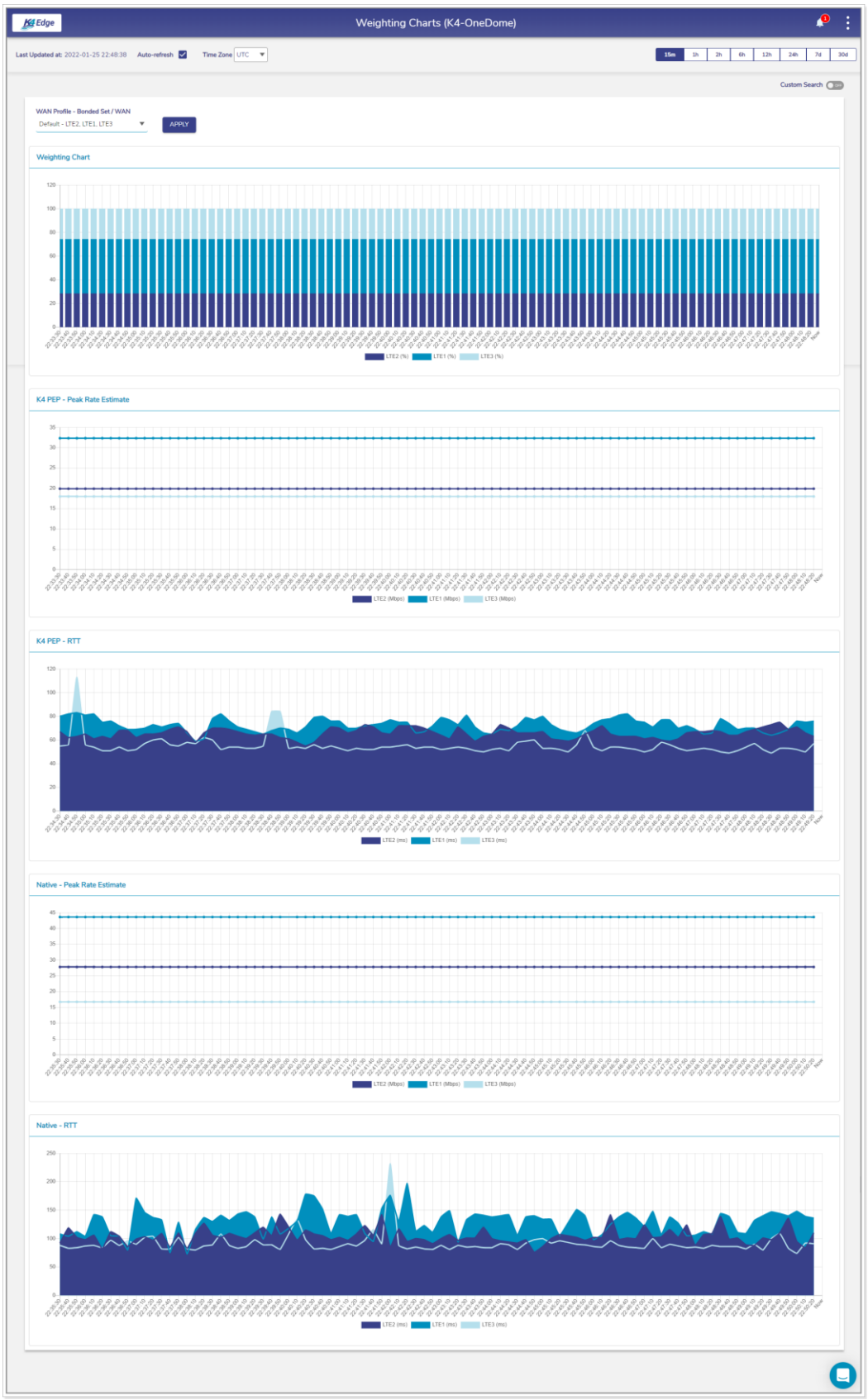

Figure 3-30 Weighting Chart

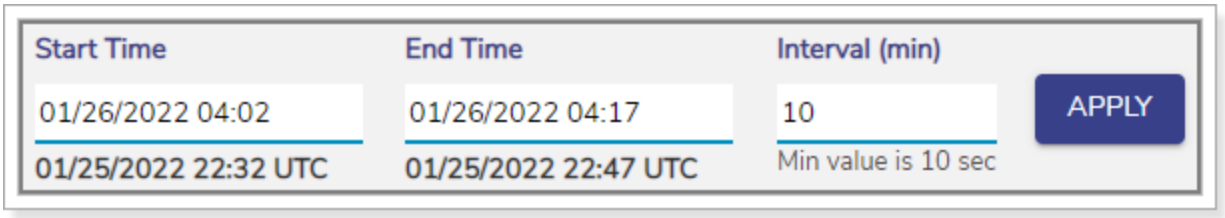

Figure 3-31 Weighting Custom Search

Return

Table 3-5 Weighting Chart Information

Fields	Description	Configuration
Auto-refresh	Whether the data on the page is to be refreshed automatically. Data is updated at an interval of 30 seconds.	To automatically refresh the details about the WAN link, click the **Auto-refresh** check box.
Time Zone	To access the details about the WAN link basis on the time zone. By default, the UTC is configured. To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where, • m is minutes • h is hours • d is days By default, the periodicity of 15m is configured.	In the **Time Zone** link, click a time zone, see *Figure 3-8*. Click the periodicity at the upper-right corner of the page.
Custom Search		**To view the weighting chart basis on a day and time, perform the following steps.** 1. Switch on the **Custom Search**. The custom search section appears, see *Figure 3-31*. 2. Click **Start Time**. The calendar becomes available. 3. Select the start day and time. The start day and time becomes available in UTC.

Fields	Description	Configuration
		4. Click **End Time**. The calendar becomes available. 5. Select the end day and time. The start day and time becomes available in UTC. 6. In the Interval (sec) field, click the minimum interval specified. 7. Click **Apply**.

3.2.9 Usage Status

Once the K4 OneDome is audited and possibly reconfigured, you can monitor the usage of the networks and devices associated with the network. The K4 OneDome typically has one Access network and client IP address from the SDWAN system – thus a very simple single network and IP view on usage.

To view the usage charts, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-33*.

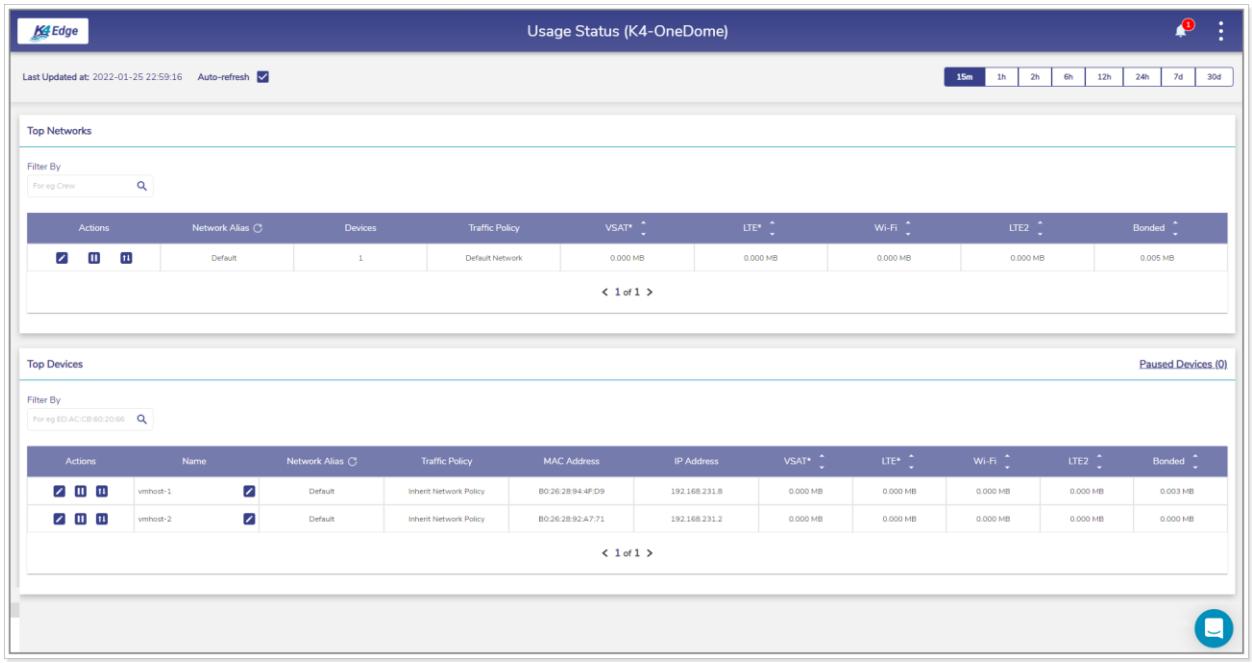

Figure 3-32 Usage Status

NOTE: Initially, the **Default** network and top devices are available. Once, the networks and devices are configured, the networks and devices become available on the **Usage Status** page. See Figure 3-33.

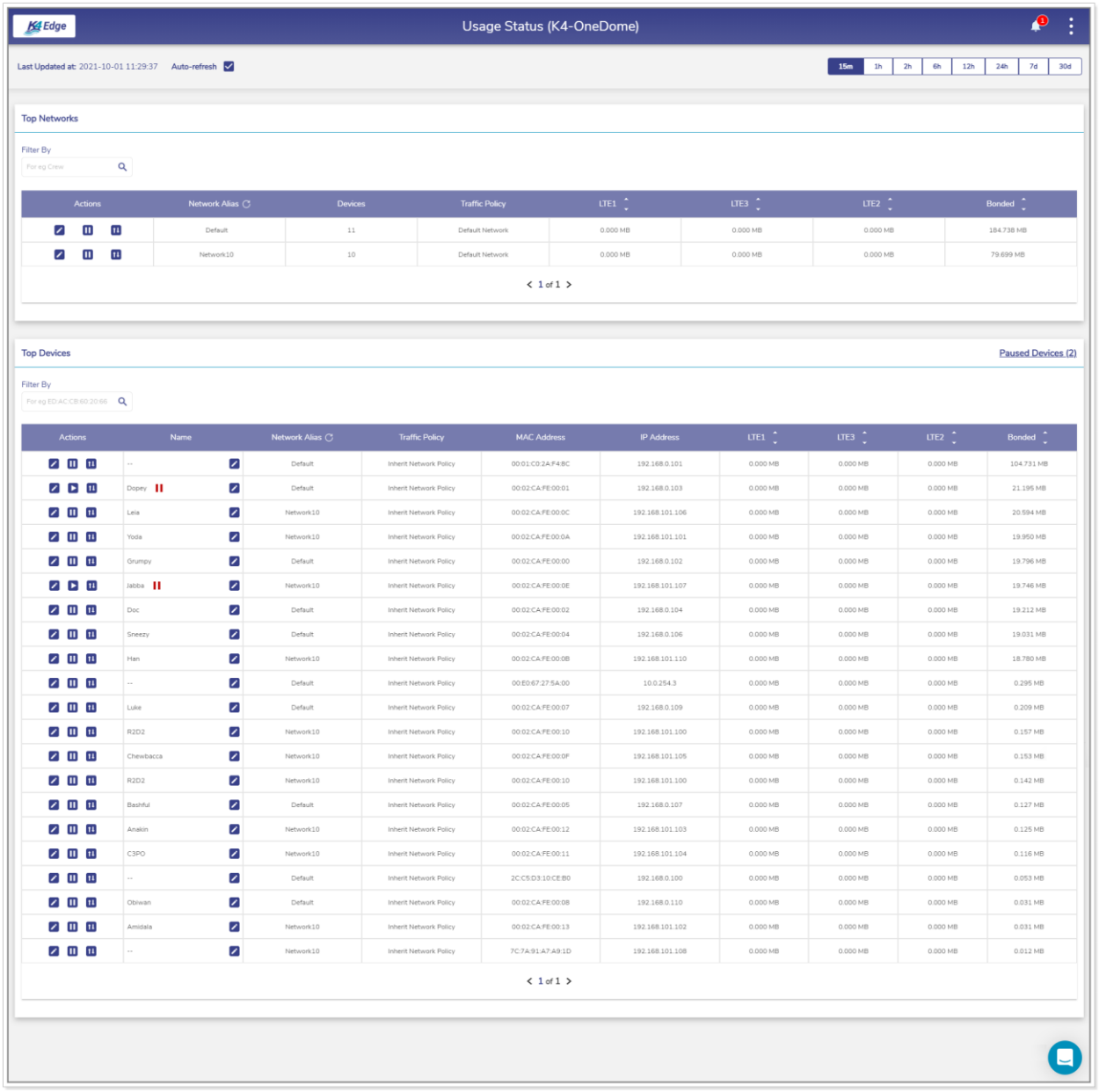

Figure 3-33 Configured Usage Status

The **Usage Status** page includes the **Top Network** and **Top Devices** sections.

3.2.9.1 Top Networks

The following details are available under the **Top Networks** section.

36. Traffic policy assigned to the network.
37. Data usage of every WAN in the network.
38. Count of the devices connected to the network.
39. The routed access network and corresponding grouping.
40. View details about the specific network, you can search that network.

To search the network, enter the name of the network in the Filter By field. Details of the network become available. The name of the network is displayed under the Network Alias field.

To view the details about the network based on periodicity, click the duration in the upper right of the page.

To modify the traffic policy of the network, perform the following steps.

1. Click corresponding to the routed network in the Action field under the **Top Networks** section. The **Edit Traffic Policy profile** page appears, see *Figure 3-34*.

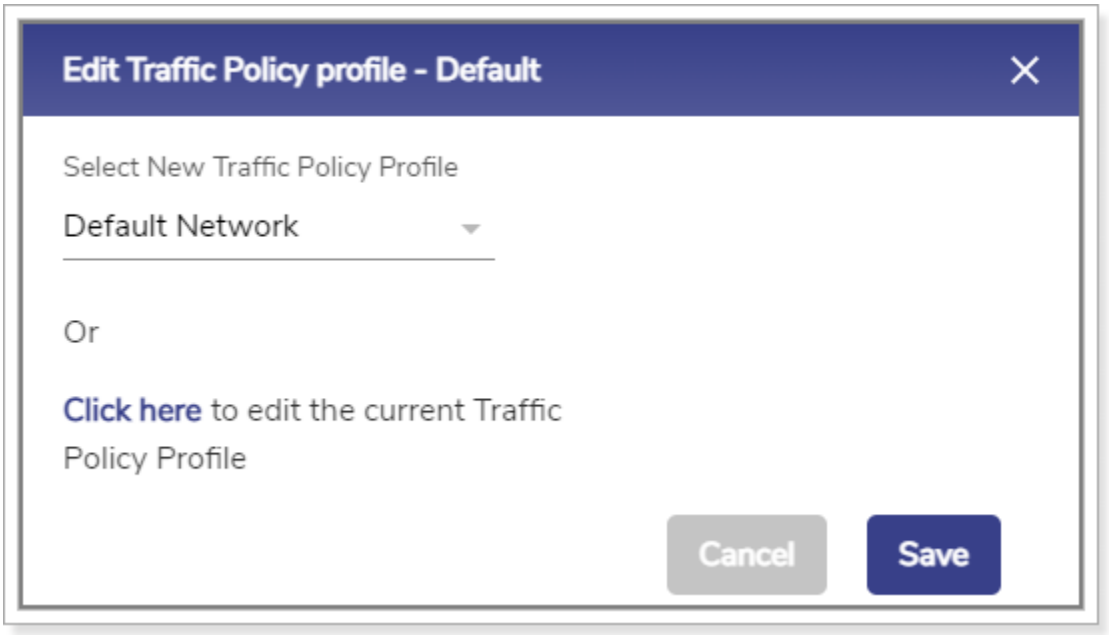

Figure 3-34 Edit Traffic Policy

2. In the **Select New Traffic Policy Profile** list, click a new traffic policy.

   Or,

   To modify the current traffic policy, click **Click here**. The **Traffic Policies** page appears. For details, see *Audit Traffic Policies* on page *71*.

3. Click **Save**.

To pause the internet of the network, perform the following steps.

1. Click corresponding to the routed network in the Action field under the **Top Networks** section. The **Pause Internet** page appears, see *Figure 3-35*.

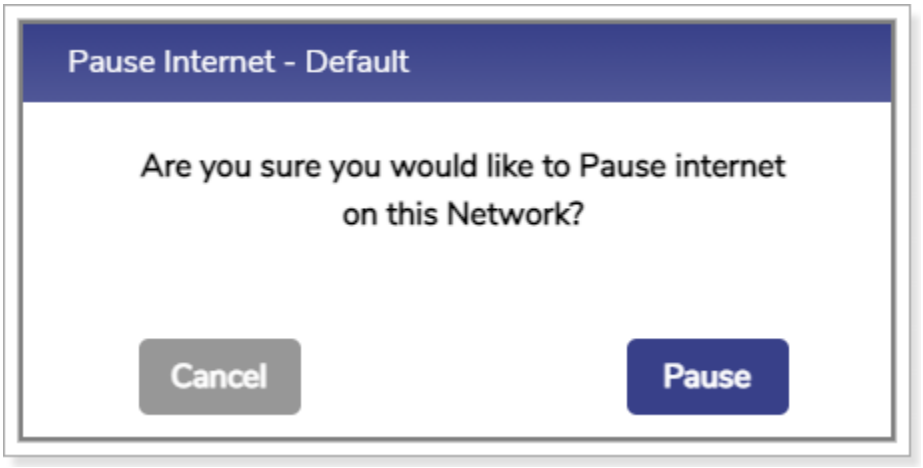

Figure 3-35 Pause Internet

2. Click **Pause**. The resume button becomes available.

   The internet is paused. However, it will not impact the other networks.

To resume the internet of the network, perform the following steps.

1. Click corresponding to the routed network in the Action field under the **Top Networks** section. The **Resume Internet** page appears, see *Figure 3-36*.

Figure 3-36 Resume Internet

2. Click **Resume**.

   The internet starts.

To view details about the traffic of the network, click corresponding to the routed network in the Action field under the **Top Networks** section. The **Traffic Details** page appears, see *Figure 3-37*.

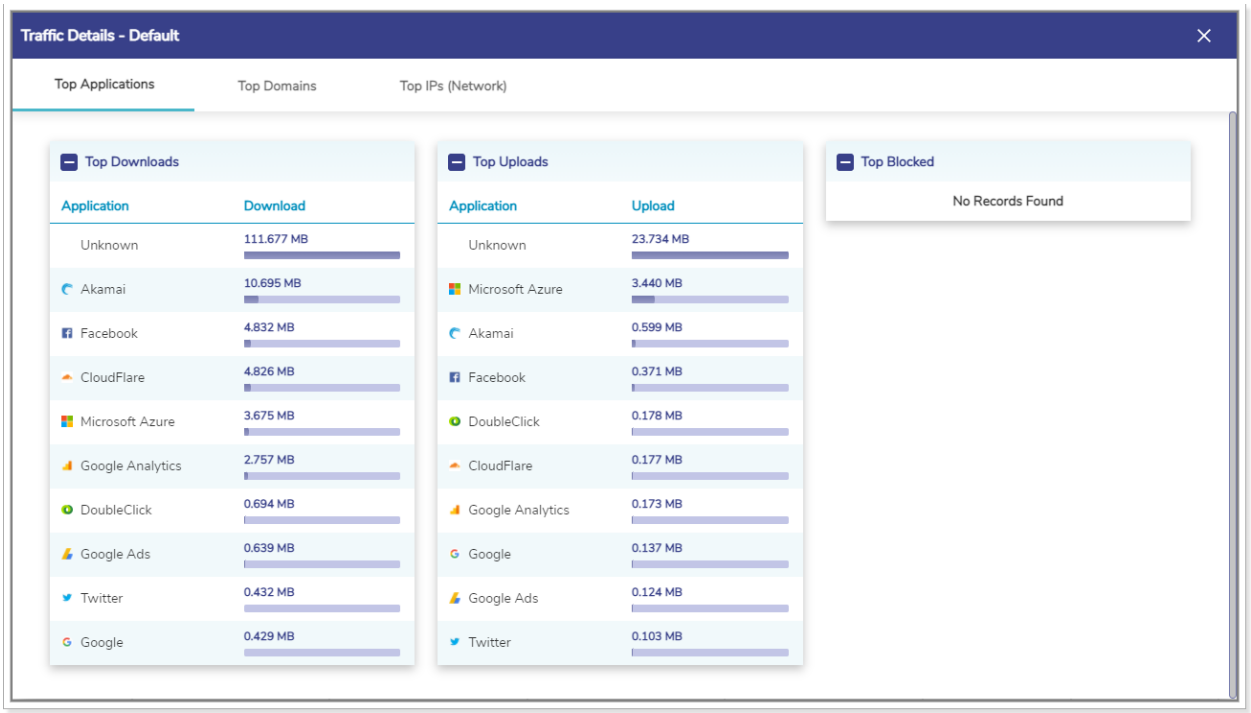

Figure 3-37 Traffic Details

To view details about the top applications, click **Top Applications**. By default, details about the top applications are available.

To view details about the top domains, click **Top Domains**.

To view details about the top IPs, click **Top IPs (Network)**.

3.2.9.2 Top Devices

The following details are available under the **Top Devices** section.

41. All the devices connected to the entire network. Following is an example.

    If the sum of the devices in the Devices field under the **Top Network** section is 20, then the details about the entire 20 devices become available.

42. Data consumed by the WANs in the network.

43. MAC address of the device.

To search the device, enter the name of the network in the Filter By field. Details of the network become available. MAC address of the device is displayed under the MAC Address field.

To pause the internet of the device, perform the following steps.

1. Click corresponding to the device in the Action field under the **Top Devices** section. The **Pause Internet** page appears.
2. Click **Pause**. The resume button becomes available.

   The internet is paused. However, it will not impact the other devices in the network

To resume the internet of the device, perform the following steps.

1. Click corresponding to the device in the Action field under the **Top Devices** section. The **Pause Internet** page appears.
2. Click **Resume**.

   The traffic starts.

To view details about the traffic of the device, click corresponding to the device in the Action field under the **Top Devices** section. The **Traffic Details** page appears.

You can view details of the devices whose internet is paused. To view details of the devices whose internet is paused, click **Paused Devices** at the upper-right in the **Top Devices** section. The **Total Paused Devices** pop-up window appears, see *Figure 3-38*.

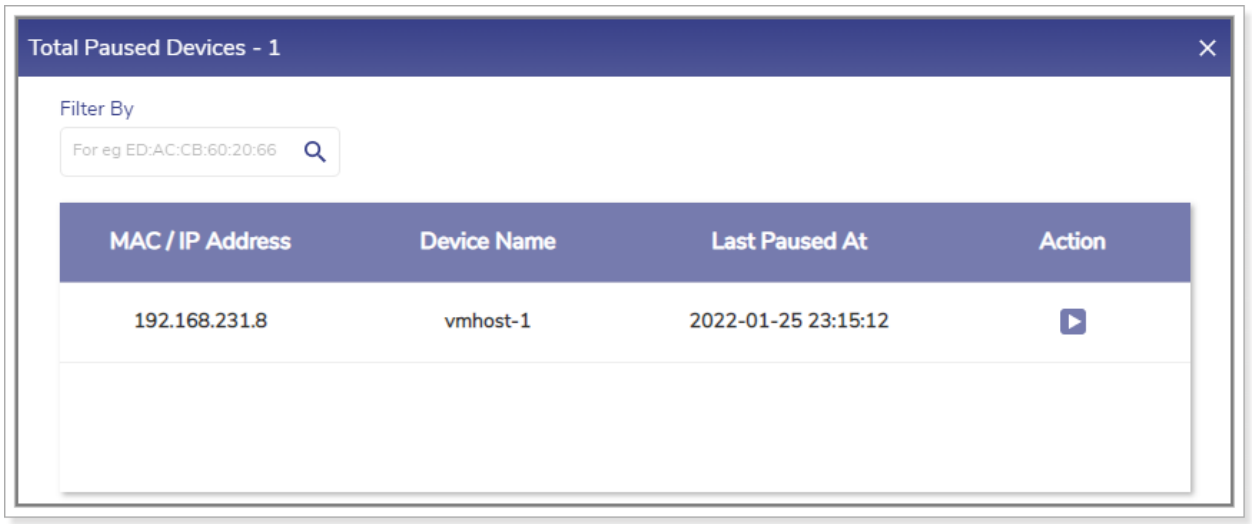

Figure 3-38 Paused Devices

You resume the internet of the devices.

3.2.10 LTE Controller

Once the K4 OneDome is audited and possibly reconfigured, you can view analytics from the LTE1, LTE2, and LTE3 modems.

To manage the LTE controller, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **LTE Controller**. The **LTE Controller** page appears, see *Figure 3-39*. For details about the LTE controller, see *Table 3-6*.

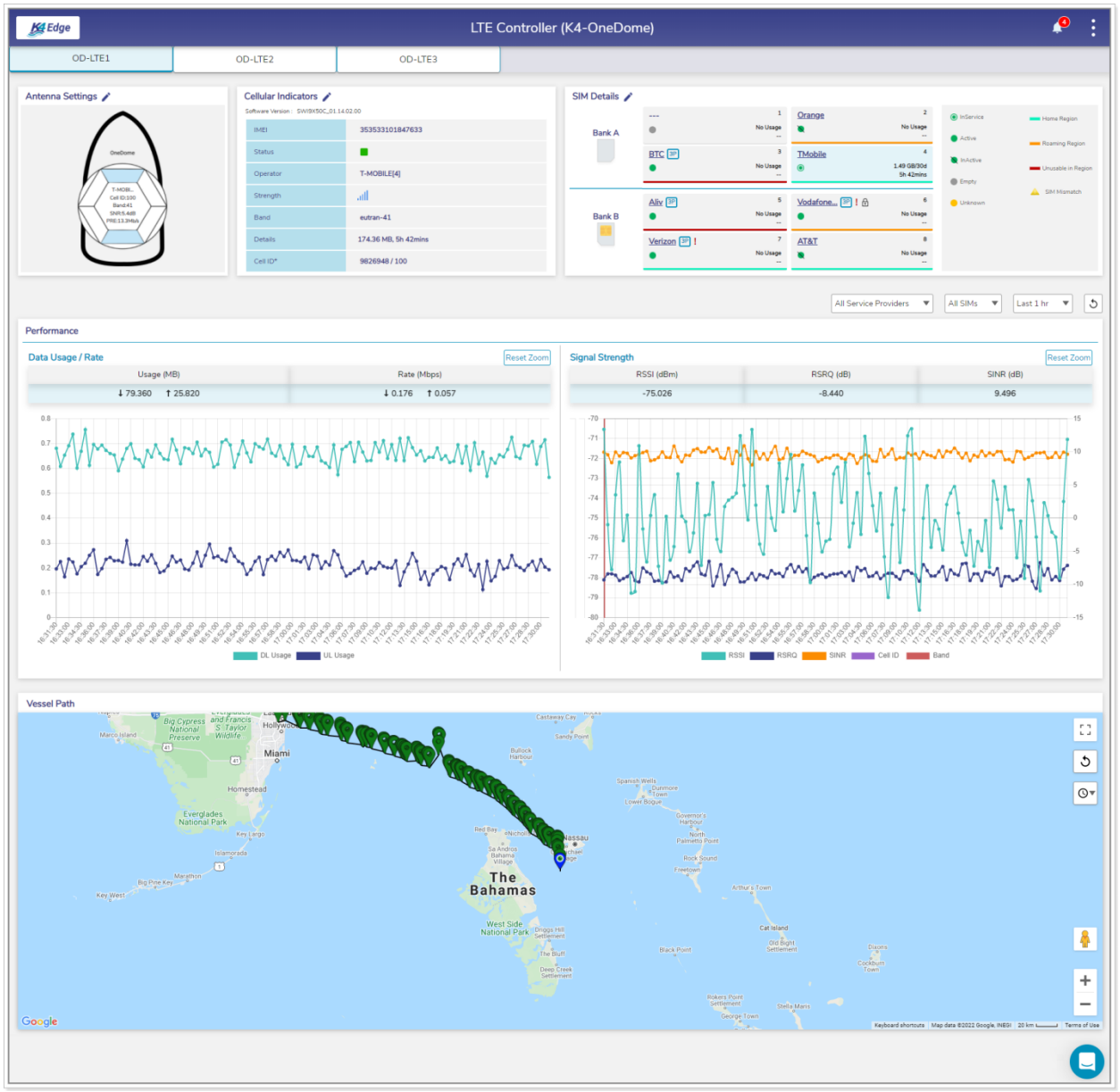

Figure 3-39 LTE Controller

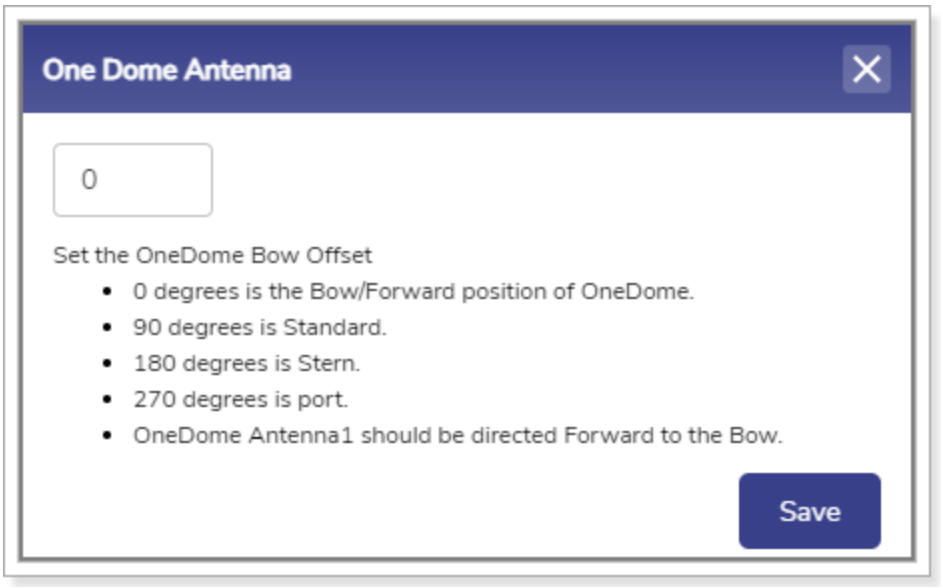

Figure 3-40 Modify K4 OneDome Antenna Settings

Return

Figure 3-41 Cellular Actions

Return

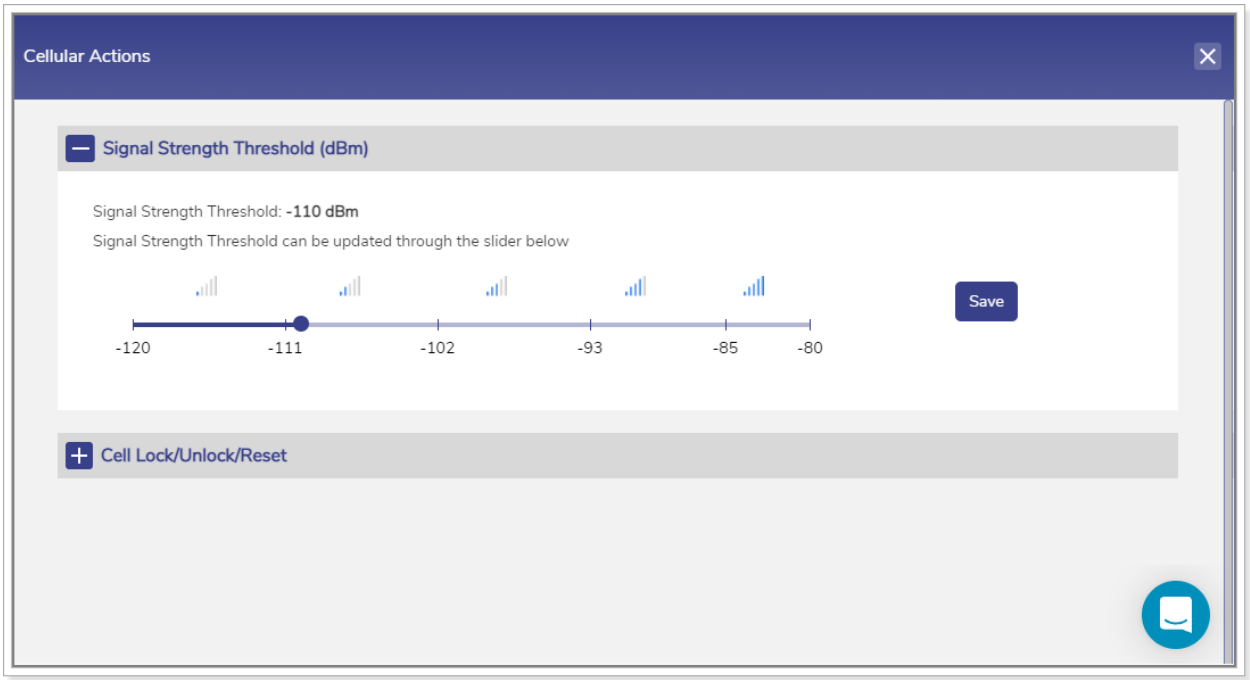

Figure 3-42 Signal Strength Threshold

Return

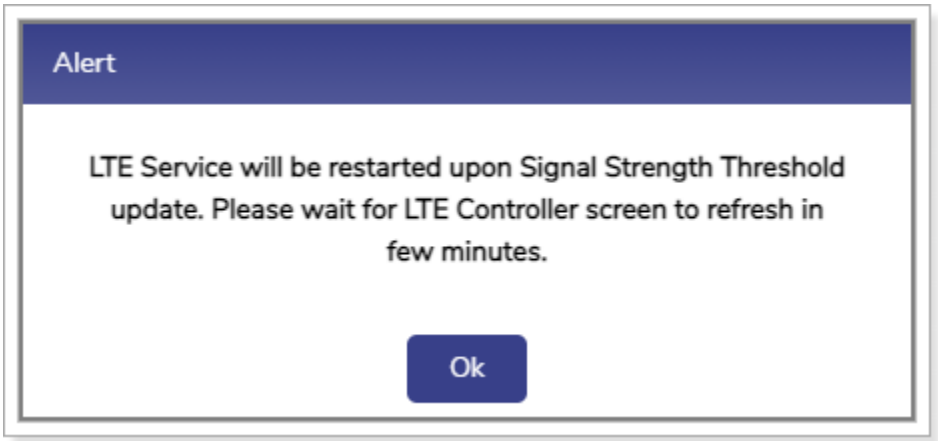

Figure 3-43 Signal Strength Threshold Alert

Return

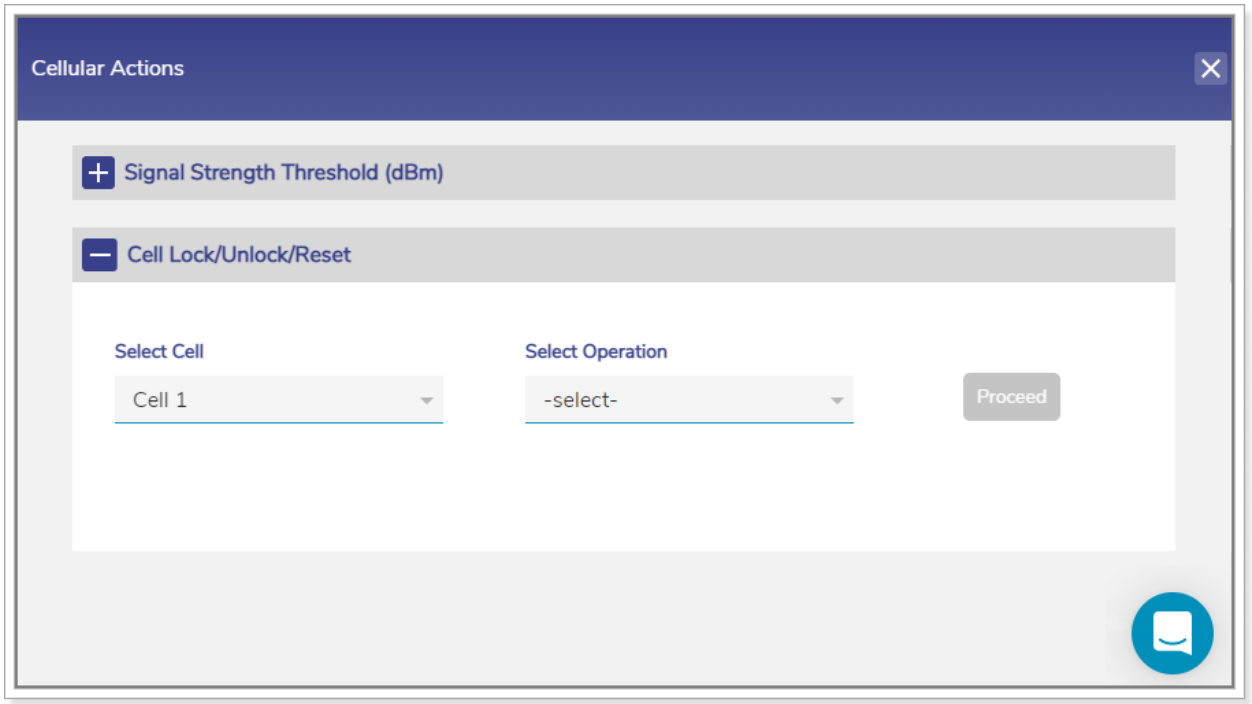

Figure 3-44 Lock, Unlock, Reset Cell

Return

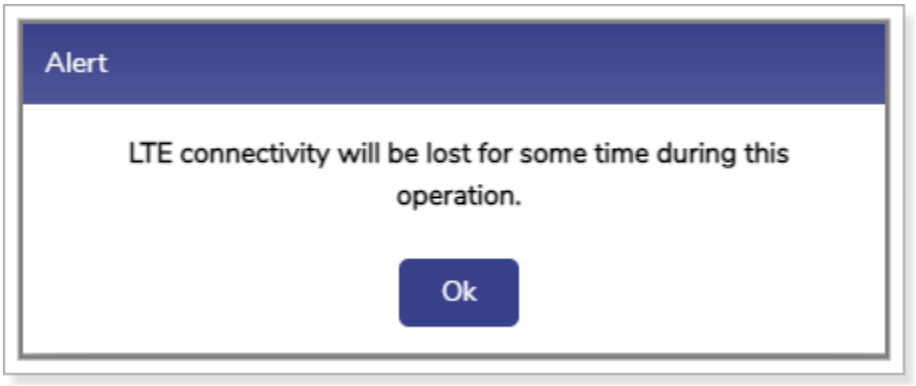

Figure 3-45 Modem Lock Alert

Return

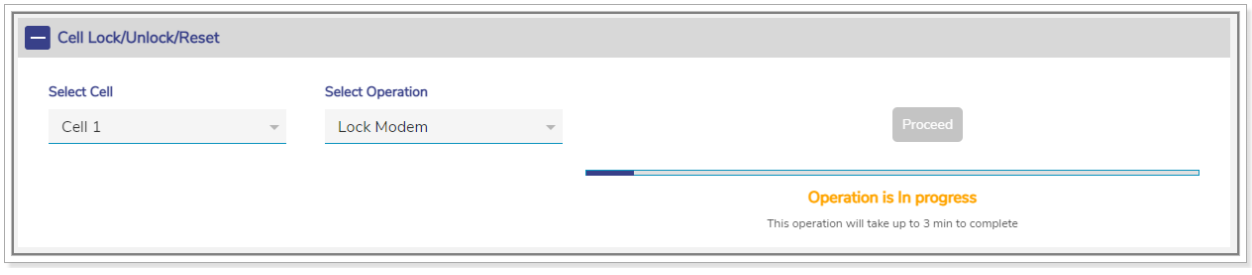

Figure 3-46 Modem Lock Progress

Return

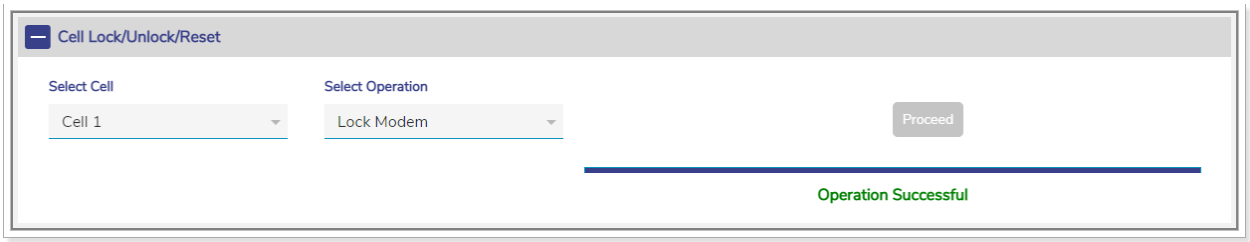

Figure 3-47 Modem Locked

Return

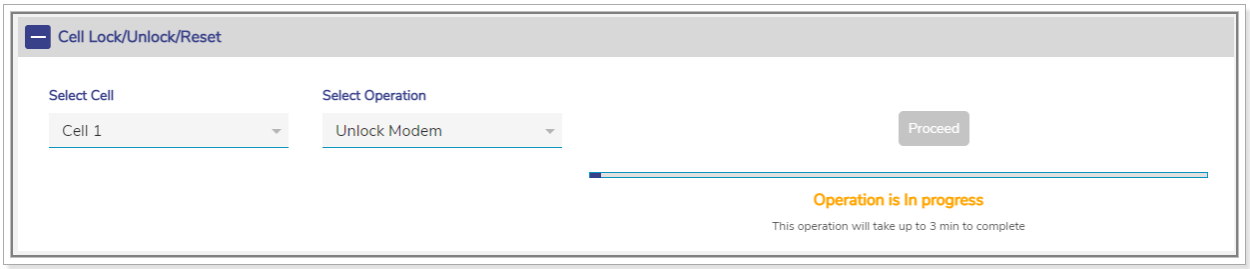

Figure 3-48 Modem Unlock Progress

Return

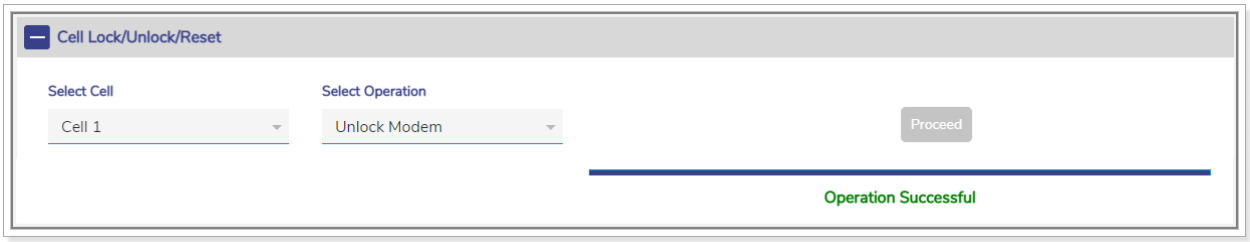

Figure 3-49 Modem Unlocked

Return

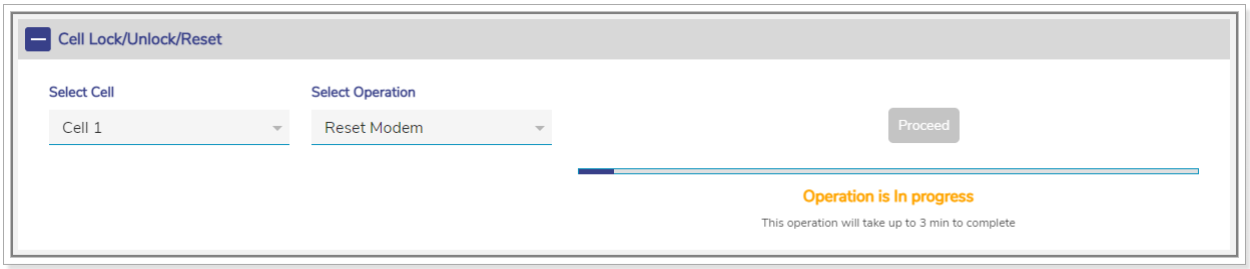

Figure 3-50 Modem Reset Progress

Return

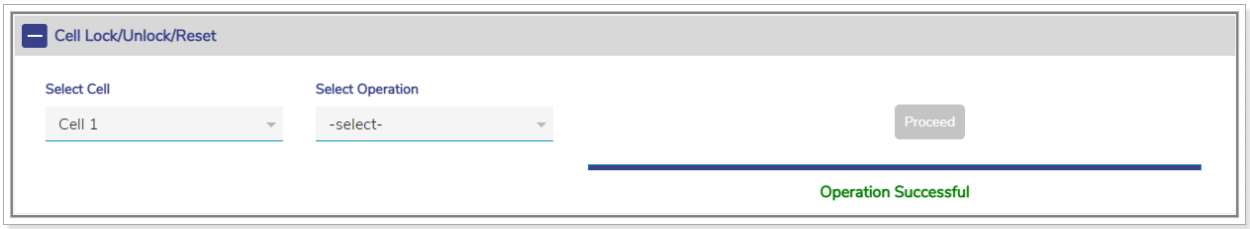

Figure 3-51 Modem Reset

Return

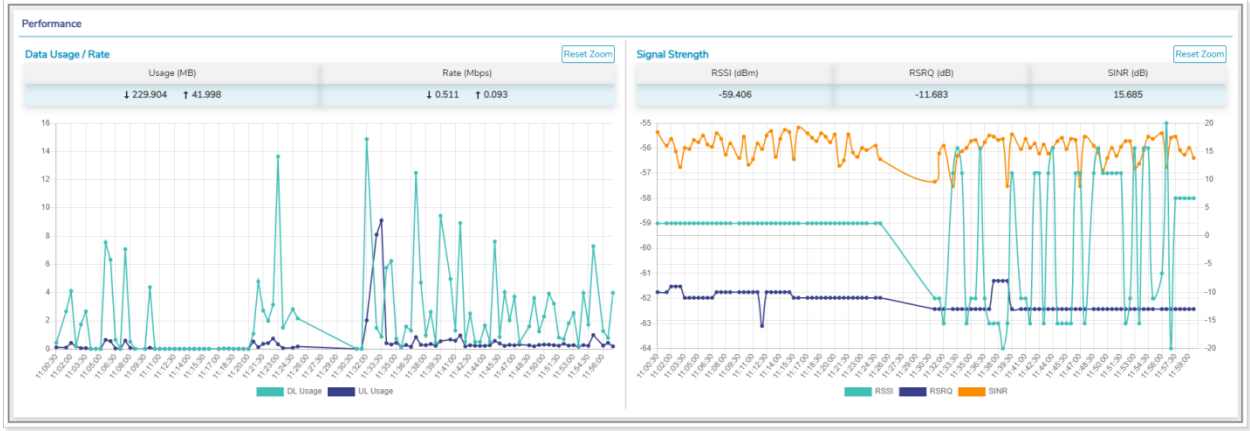

Figure 3-52 Performance Chart

Return

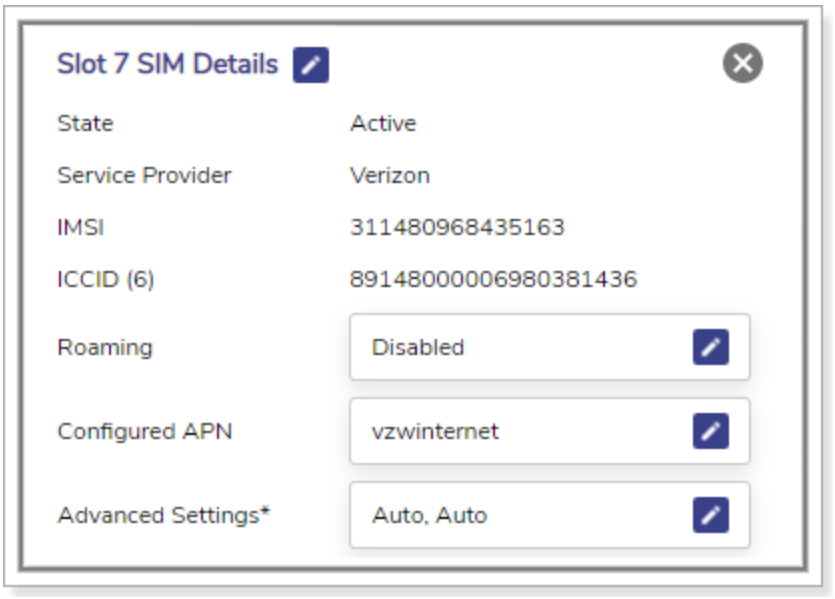

Figure 3-53 SIM Details

Return

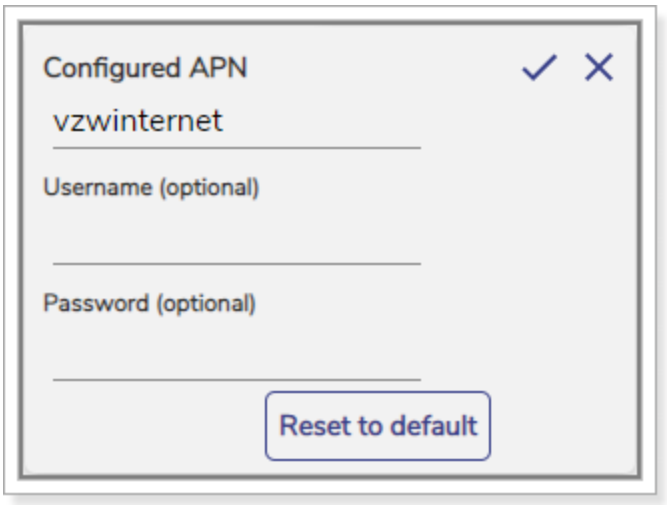

Figure 3-54 Configured APN

Return

Figure 3-55 SIM Action

Return

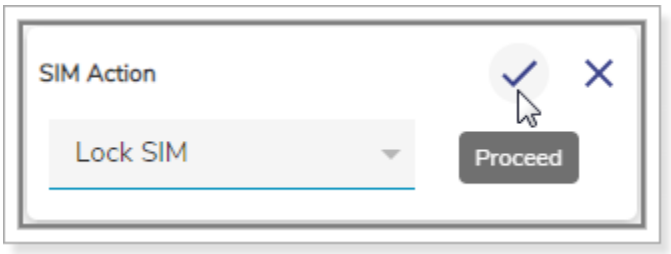

Figure 3-56 Proceed Button Becomes Available

Return

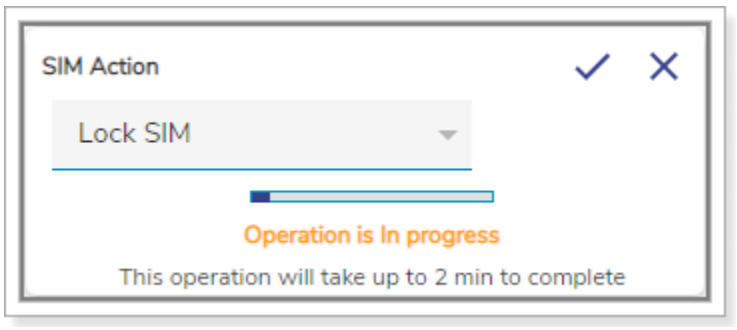

Figure 3-57 SIM Lock Progress

Return

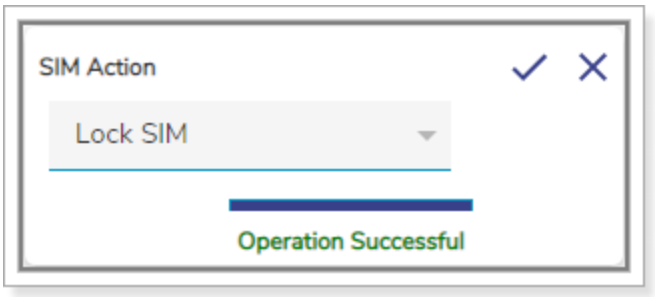

Figure 3-58 SIM Locked

Return

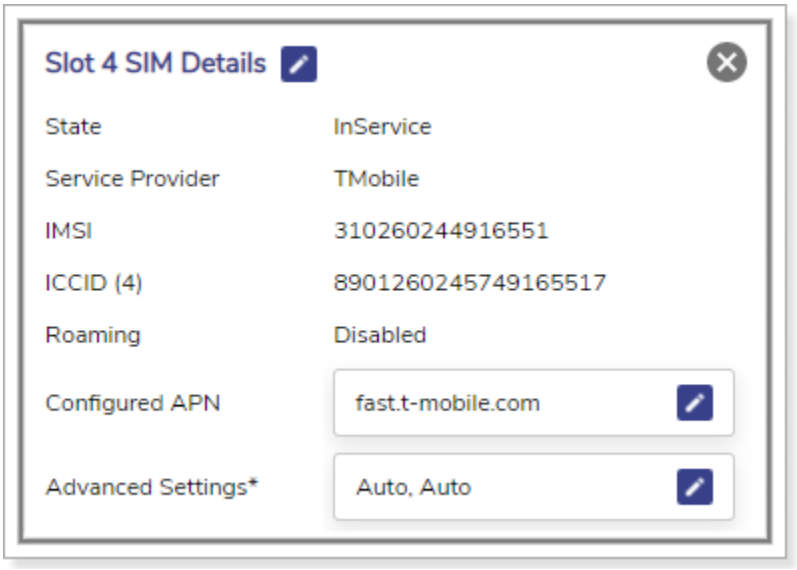

Figure 3-59 InService SIM Details

Return

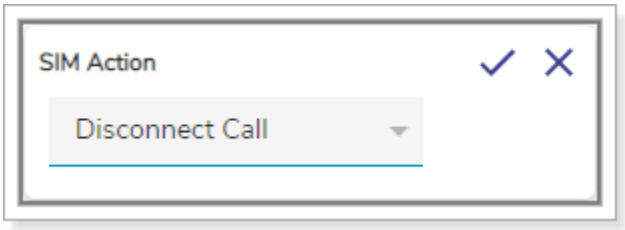

Figure 3-60 SIM Action Disconnect Call

Return

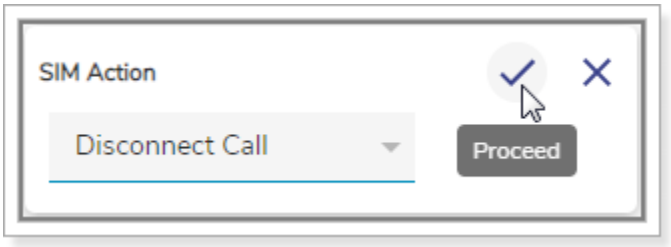

Figure 3-61 Proceed Button Becomes Available

Return

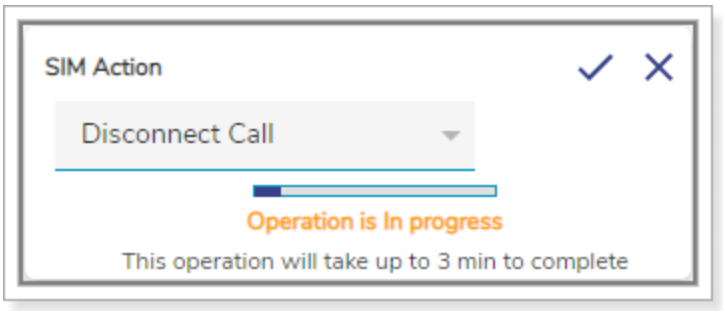

Figure 3-62 Call Disconnect Progress

Return

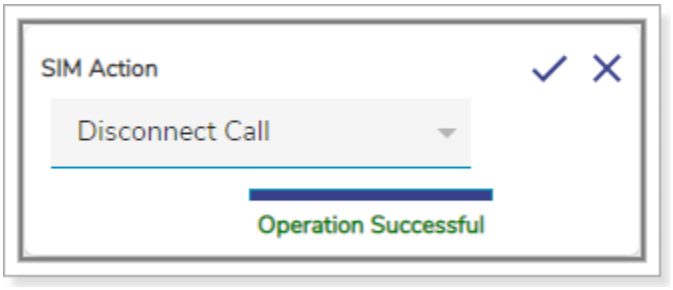

Figure 3-63 Call Disconnected

Return

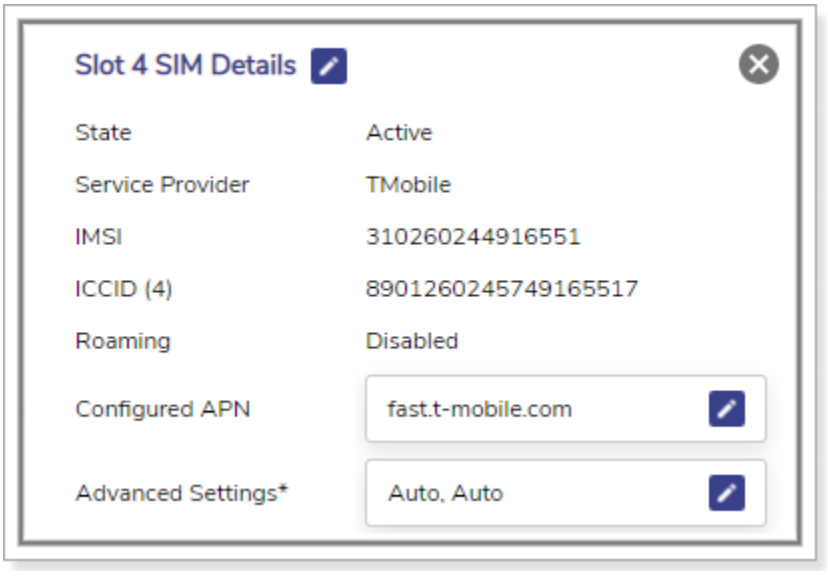

Figure 3-64 SIM Slot Details and Active Status

Return

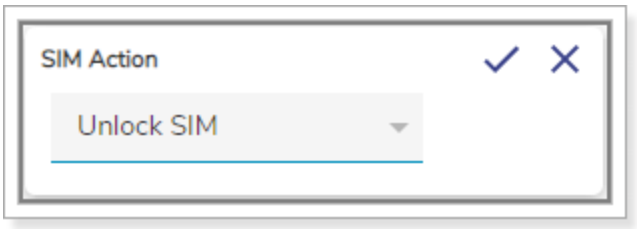

Figure 3-65 SIM Unlock

Return

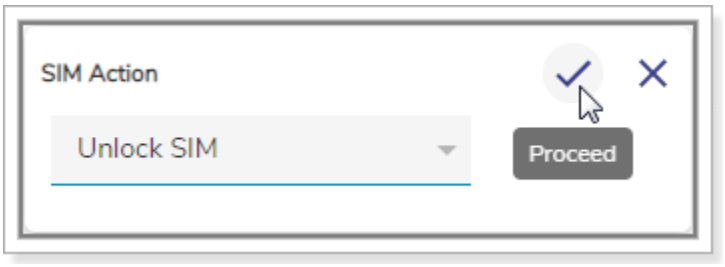

Figure 3-66 Proceed Button for SIM Unlock

Return

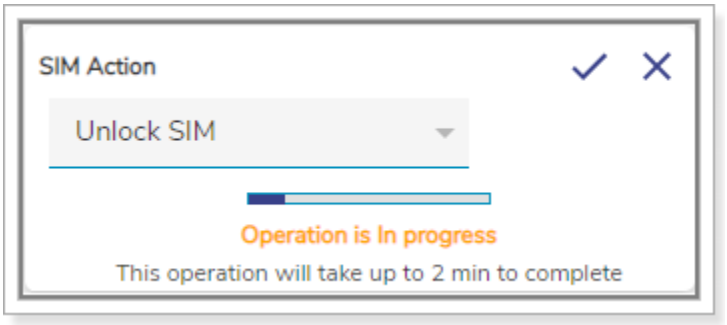

Figure 3-67 SIM Unlock Progress

Return

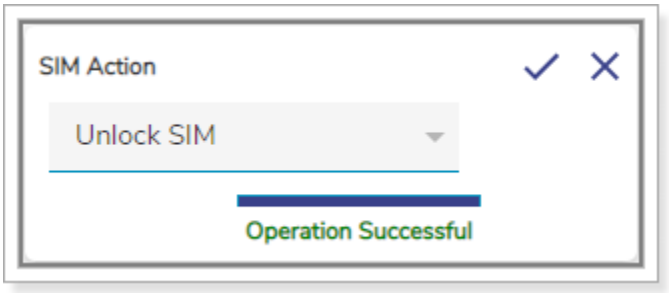

Figure 3-68 SIM Unlocked

Return

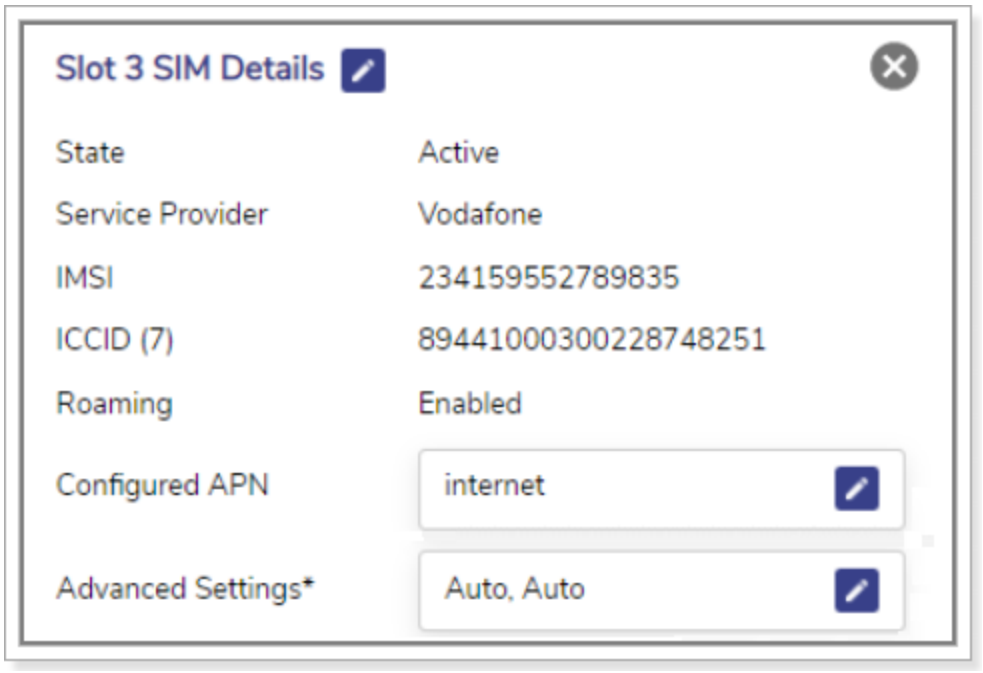

Figure 3-69 Advanced Settings on Slot SIM Details

Return

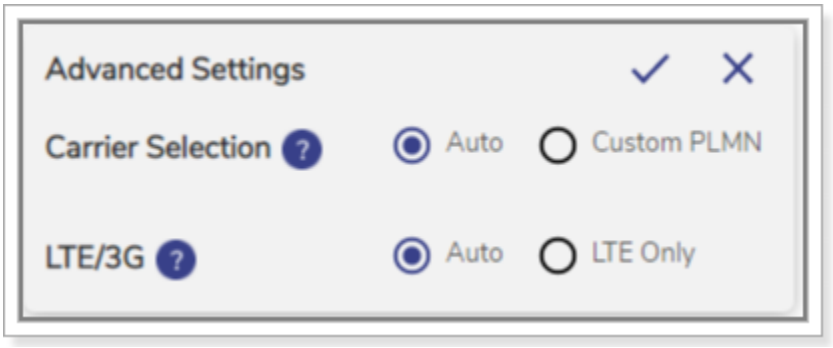

Figure 3-70 Network Selection and Carrier Selection

Return

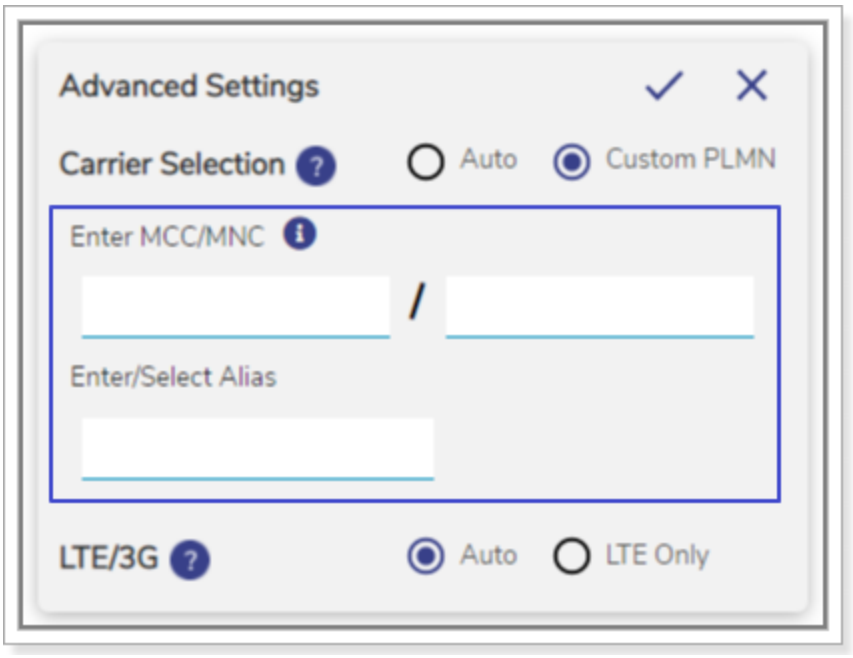

Figure 3-71 MCC/MNC and Alias

Return

Figure 3-72 Custom PLMN

Return

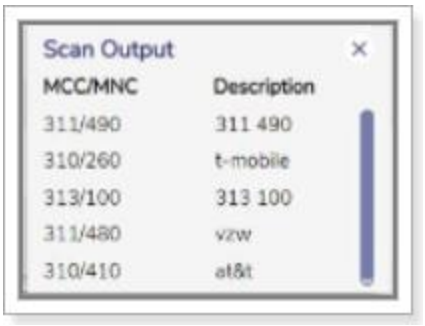

Figure 3-73 Scan Output

Return

Figure 3-74 MCC/MNC Reference Link

Return

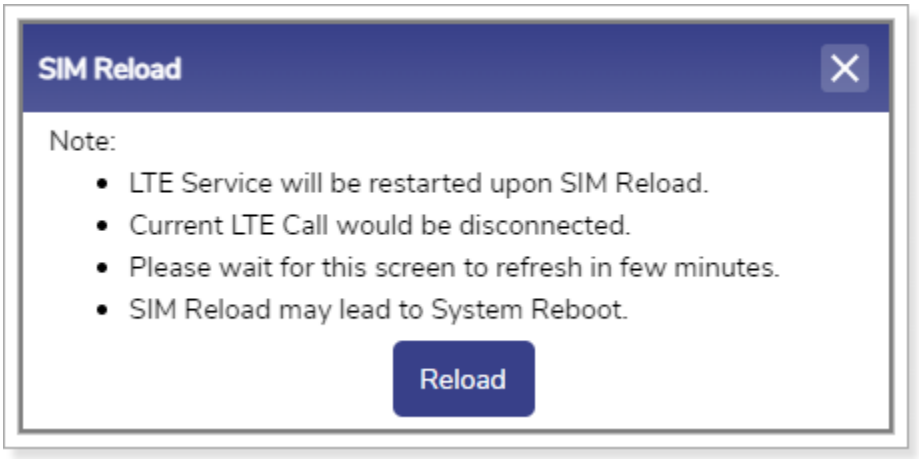

Figure 3-75 SIM Reload

Return

Table 3-6 LTE Controller Information

Sections	Description	Configuration
OD – LTE 1, OD – LTE 2, and OD – LTE 3	These are the tabs available on the LTE controller UI to view the details about the parent LTE 1 and child LTE 3, and LTE 2.	To view details of the LTE 2, click **OD – LTE 2**. And, To view details of the LTE 3, click **OD – LTE 3**.

Sections	Description	Configuration
Antenna Settings	To modify the settings of the K4 OneDome antenna. Therefore, it will impact the child LTE 3 and LTE 2.	**To modify the settings of the antenna, perform the following steps.** 1. Click corresponding to the **Antenna Settings**. The **One Dome Antenna** pop-up window appears, see *Figure 3-40*. 2. Enter the K4 OneDome bow offset. 3. Click **Save**.
Cellular Indicators		
Software Version	The version of the LTE Modem Firmware.	NA
IMEI	IMEI of the LTE modem.	NA
Status	Displays one of the statuses of the respective modem. • . This indicates that the modem is active and in use. • . This indicates that the modem is inactive and not in use.	NA
Operator	The name of the home network operator and the SIM slot number of that operator is displayed in the following format. Home network operator [Current SIM Slot number of the home network operator] The following is an example. VERIZON [6] Or, If the vessel is roaming, then the name of the visited network operator	NA

Sections	Description	Configuration
	and the SIM slot number of that home network operator is displayed in the following format. Visited network operator [Current SIM Slot number of the home network operator] The following is an example. The vessel is on roaming with the Vodafone SIM that is in SIM slot 7. The visitor is connected to the visited network operator AT&T. Therefore, the following operator is displayed. AT&T [7]	
Strength	• The strength of the signal is displayed. • You can configure the signal strength threshold. If the current signal strength is less than the signal strength threshold, then the signal strength is considered as bad signal strength. Therefore, the network having the signal strength more than the signal strength threshold is searched. Or, If the current signal strength is more than the signal strength threshold, then the signal strength is	To view the signal strength of the cell, point the mouse to the signal corresponding to the Strength field. **To update the signal strength threshold, perform the following steps.** 1. Click corresponding to the **Cellular Indicators**. The **Cellular Actions** page, appears, see *Figure 3-41*. 2. Click **Signal Strength Threshold (dBm)**. The signal strength threshold section becomes available, see *Figure 3-42*. **NOTE:** dBm stands for decibels per milliwatt and dB stands for decibels. 3. Click the desired signal strength. 4. Click **Save**. The **Alert** pop-up window appears, see *Figure 3-43*. 5. Click **OK**.

Sections	Description	Configuration
	considered as good signal strength.	The signal strength threshold is updated.
	You can lock the Modem.	**To lock the modem, perform the following steps.** 1. Click corresponding to the **Cellular Indicators**. The **Cellular Actions** page, appears, see *Figure 3-41*. 2. Click **Cell Lock/Unlock/Reset**. The cell lock/unlock becomes available, see *Figure 3-44*. 3. In the Select Cell list, click a cell whose modem is to be locked, or unlocked, or reset. 4. In the Select Operation list, click the **Lock Modem**. The **Proceed** button becomes available. 5. Click **Proceed**. The **Alert** pop-up window appears, see *Figure 3-45*. 6. Click **OK**. The cell locking process starts, see *Figure 3-46*. Once the modem is locked, a successful message is displayed, see *Figure 3-47*.
	You can unlock the Modem.	**To unlock the modem, perform the following steps.** 1. Click corresponding to the **Cellular Indicators**. The **Cellular Actions** page, appears, see *Figure 3-41*. 2. Click **Cell Lock/Unlock/Reset**. The cell lock/unlock becomes available, see *Figure 3-44*. 3. In the Select Cell list, click a cell whose modem is to be locked, or unlocked, or reset. 4. In the Select Operation list, click the **Unlock Modem**. The **Proceed** button becomes available.

Sections	Description	Configuration
		5. Click **Proceed**. The cell unlocking process starts, see *Figure 3-48*. Once the modem is unlocked, a successful message is displayed, see *Figure 3-49*.
	You can reset the Modem.	**To reset the modem, perform the following steps.** **1.** Click corresponding to the **Cellular Indicators**. The **Cellular Actions** page, appears, see *Figure 3-41*. **2.** Click **Cell Lock/Unlock/Reset**. The cell lock/unlock becomes available, see *Figure 3-44*. **3.** In the Select Cell list, click a cell whose modem is to be locked, or unlocked, or reset. **4.** In the Select Operation list, click the **Unlock Modem**. The **Proceed** button becomes available. **5.** Click **Proceed**. The **Alert** pop-up window appears, see *Figure 3-45*. **6.** Click **OK**. Modem reset starts, see *Figure 3-50*. The modem will be down and the status of the cell is reflected by the red square. Therefore, the LTE connectivity will be down. Once the modem resets a successful message is displayed, see *Figure 3-51*. In addition to this, the LTE controller will again scan and select the operator to connect for the LTE connectivity.
Band	The band of the signal is displayed.	NA
Details	If the modem is active, then the quantum of the data consumed with duration is displayed.	NA

Sections	Description	Configuration
	Otherwise, the status of the operator is displayed.	
Cell ID	The ID of the LTE Modem is displayed.	NA
SIM Details		
SIM Details	The K4 EdgeOne supports third party SIMs. The SIM that is not provided by the K4 is deemed to be the third party SIM. This is reflected by 3P next to the service provider.	NA
	The K4 EdgeOne supports 8 SIMs and can be loaded in the following two SIM banks. • Bank A. This includes four SIMs out of eight SIMs. • Bank B. This includes other four SIMs out of eight SIMs. The following details are displayed in the banks. • SIM orientation. • Name of the service provider. • Physical slot number. • Duration since the SIM is in use or service. • Data usage. • Registration details. • One of the following states of the SIM.	To create the performance chart based on the data usage and signal strength, click ● under the service provider. The chart becomes available, see *Figure 3-52*. To view details about a SIM, click the service provider. The **Slot SIM Details** pop-up window appears, see *Figure 3-53*. If the SIM registration is denied, then ! is displayed next to the name of the service provider. Point the mouse to !, the registration denied message is displayed. In addition to this, MCC and MNC are displayed.

Sections	Description	Configuration
	• . InService. This indicates that the SIM is in use. • . Active. This indicates that the SIM is available, but it is not in use. • . InActive. This indicates that the information about the SIM is unavailable. • . Empty. This indicates that the SIM is ready to use. • . Unknown. This indicates that the SIM is available in the slot but details about that SIM are not available in the database.	
	You can lock the SIM whose current state is defined as **Active** or **InActive**. Once the SIM is locked, you cannot perform the intended tasks from that SIM. You cannot lock the SIM whose status is defined as **Unknown**.	**To lock the SIM whose status is defined as Active or InActive, perform the following steps.** 1. Click the service provider. The **Slot SIM Details** pop-up window appears, see *Figure 3-53*. 2. Click next to the **Slot SIM Details**. The **SIM Action** pop-up window appears, see *Figure 3-55*. By default, the **Lock SIM** is specified in the **SIM Action** list. 3. Point the mouse to . The **Proceed** button becomes available, see *Figure 3-56*. 4. Click **Proceed**.

Sections	Description	Configuration
		The SIM lock process begins, see *Figure 3-57*. The SIM is locked and a successful message is displayed, see *Figure 3-58*. The locked SIM is reflected by next to the name of the service provider. Once the SIM is locked, you cannot perform the intended tasks from that SIM. You can lock the SIM whose status is defined **Active** or **InActive**. In addition to this, you cannot lock the SIM whose status is defined as **Unknown**.
	You can lock the SIM that is in use or whose current state is defined as **InService**.	**To lock the SIM whose status is defined as InService, perform the following steps.** 1. Click the service provider. The **Slot SIM Details** pop-up window appears, see *Figure 3-59*. 2. Click next to the **Slot SIM Details**. The **SIM Action** pop-up window appears, see *Figure 3-60*. By default, the click **Disconnect Call** is specified in the **SIM Action** list. 3. Point the mouse to . The **Proceed** button becomes available, see *Figure 3-61*. 4. Click **Proceed**. The call disconnection process begins, see *Figure 3-62*. The call is disconnected and a successful message is displayed, see *Figure 3-63*. The SIM state is defined as **Active**. 5. Click next to the **Slot SIM Details**, see *Figure 3-64*. The **SIM Action** pop-up window appears, see *Figure 3-55*. 6. In the **SIM Action** list, click **Lock SIM**.

Sections	Description	Configuration
		7. Point the mouse to  . The **Proceed** button becomes available, see *Figure 3-56*. 8. Click **Proceed**. The SIM lock process begins, see *Figure 3-57*. The SIM is locked and a successful message is displayed, see *Figure 3-58*. The locked SIM is reflected by  next to the name of the service provider. Once the SIM is locked, you cannot perform the intended tasks from that SIM. You can lock the SIM whose status is defined **Active** or **InActive**. In addition to this, you cannot lock the SIM whose status is defined as **Unknown**.
	You can unlock the SIM.	**To unlock the SIM, perform the following steps.** 1. Click the service provider. The **Slot SIM Details** pop-up window appears, see *Figure 3-53*. 2. Click  next to the **Slot SIM Details**. The **SIM Action** pop-up window appears, see *Figure 3-65*. By default, the **Unlock SIM** is specified in the **SIM Action** list. 3. Point the mouse to  . The **Proceed** button becomes available, see *Figure 3-66*. 4. Click **Proceed**. The SIM unlock process begins, see *Figure 3-67*. The SIM is unlocked and a successful message is displayed, see *Figure 3-68*. Once the SIM is unlocked you can perform the intended tasks.

Sections	Description	Configuration
	By default, the APN is configured for every SIM to connect to the specific service provider. However, you can manually configure the APN.	**To modify the APN, perform the following steps.** 1. Click  in the **SIM Details** pop-up window, see *Figure 3-53*. The **Configured APN** section becomes available, see *Figure 3-54*. 2. Modify the details and then click ✓. Or, To reset the APN to default, click **Reset to default**. The APN is reset to the default configuration.
	By default, the LTE/3G (**Auto**) is selected. Therefore, the SIM will connect to the LTE or 3G network of the service provider (carrier). However, you can configure the SIM to connect only to the LTE network of the service provider (carrier).	**To configure the SIM to connect only to the LTE network, perform the following steps.** 1. Click  in the **SIM Details** pop-up window, see *Figure 3-69*. 2. Click  corresponding to the Advanced Settings field, see *Figure 3-69*. The **Advanced Settings** pop-up window appears, see *Figure 3-70*. 3. Click **LTE Only** in the LTE/3G field. 4. Click **Save**. By default, **Auto** is selected in the LTE/3G field. For more details, click  next to the LTE/3G field. **NOTE:** You must select the **LTE Only** while configuring the PLMN. If the SIM is in use with a current Cellular radio, then the call will drop using that SIM
	You can configure the cellular parameters, PLMN MCC & MNC settings of the service	**To configure the network selection, perform the following steps.**

Sections	Description	Configuration
	provider (carrier) for every SIM to connect only to the specific service provider (carrier). By default, the carrier selection for every SIM is configured to **Auto**.	1. Click  in the **SIM Details** pop-up window, see *Figure 3-69*. 2. Click  corresponding to the Advanced Settings field, see *Figure 3-69*. The **Advanced Settings** pop-up window appears, see *Figure 3-70*. 3. Click **Custom PLMN**. The MCC/MNC and Alias fields become available, see *Figure 3-71*. 4. Enter the unique 3 digits MCC in the Enter MCC/MNC field, see *Figure 3-71*. 5. Click the MCC. **NOTE:** You must enter the 3 digits MCC and MNC in the respective fields. If it does not comply with the 3 digits MCC/MNC, then it will not connect to the carrier. Therefore, if the Scanned List has 344/3, then you must enter MCC as 344 and MNC as 003. 6. Enter the unique 3 digits MNC in the Enter MCC/MNC field, see *Figure 3-71*. 7. Click the MNC. **NOTE:** You must enter the 3 digits MCC and MNC in the respective fields. If it does not comply with the 3 digits MCC/MNC, then it will not connect to the carrier. Therefore, if the Scanned List has 344/3, then you must MCC as 344 and MNC as 003. 8. Enter the Alias name in the Enter/Select Alias field. **NOTE:** It is best practice to enter an Alias name that signifies the location and operator.
	The MCC/MNC (PLMN) settings of the SIM are associated with a country and a service provider (carrier). Therefore, the PLMN settings are limited to geographical location. The SIM continues to function in the current geographical location but may not function in a distinct geographical location. This is an example. If the vessel is in geographical location A, then based on the PLMN settings, the SIM continues to work in that geographical location. If the vessel sails to geographical location B, then based on the PLMN settings, the SIM may not work in that geographical location. To ease the simplify MCC/MNC for the SIM based on the current geographical location, the K4 Edge system provides Cellular Scan Output and updates for that SIM.	

Sections	Description	Configuration
		Therefore, it can easily be referenced in the future. This is an example. StMartin-Voda Or, 1. Click  next to the Enter MCC/MNC field under the **Carrier Selection** section. The Scan Output pop-up window appears, see *Figure 3-73*. 2. Click the MCC/MNC in the Scan Output. The MCC/MC and Alias name is displayed in the respective fields. For MCC/MNC reference, click  next to the **Carrier Selection**, see *Figure 3-74* and then click **here**. 9. Click the Alias Name. 10. Click  . The PLMN is configured. In addition to this, the Custom PLMN, LTE Only is displayed corresponding to the Advanced Settings field, see *Figure 3-72*.
	If the existing SIM is reloaded in the SIM slot of the bank, or, a new SIM is loaded in the SIM slot of the bank, or, details of the SIM are unavailable, then the **SIM Reload** procedure must be performed. LTE service must be restarted. Therefore, the SIM bank will restart.	**To perform the SIM Reload procedure, perform the following steps.** 1. Click  next to the **SIM Details**. The **SIM Reload** pop-up window appears, see *Figure 3-75*. 2. Click **Reload**. The LTE service restarts. Therefore, the SIM banks are reset. Details about the SIMs become available.
	Provides information about the SIM that is not available in the slot. However, details about	To view details about the missing SIMs, click  . A list of the missing SIMs is displayed.

Sections	Description	Configuration
	the SIMs are available in the database.	

The Vessel Path displays the path traveled by the vessel.

To view the performance chart of the service providers, in the **All Service Providers** list, click a service provider.

To view the performance chart of the SIM, in the **All SIMs** list, click a SIM.

To view the performance chart of the cellular, in the **All Cellular** list, click a cell. The data usage rate chart and signal strength chart become available under the **Performance** section. For details about the signal strength, see *Table 3-7*.

Table 3-7 LTE Signal Strength

Signal Strength Range	Status
Reference Signal Received Power (RSRP) dBm	
-80 or near to zero (0)	Excellent
-80 to -90	Good
-90 to -100	Mid Cell
-100 or less	Poor
Reference Signal Received Quality (RSRQ) dB	
-10 or near to zero (0)	Excellent
-10 to -15	Good
-15 to -20	Mid Cell
-20 or less	Poor
Signal to Interference & Noise Ratio (SINR) dB	
>=20	Excellent
13 to 20	Good
0 to 13	Mid Cell
<=0	Poor

3.2.11 Managing Wi-Fi Controller

The EdgeOne Supports a Wi-Fi interface that can be an Access Point (AP) supporting an SSID for local access, or the interface can be configured as a Wi-Fi Client for Marina Wi-Fi Access. The default configuration for Wi-Fi is as an AP.

3.2.11.1 Wi-Fi Interface AP or Client Mode

By default, the EdgeOne Wi-Fi interface operates as an Access Point, and this is observable in the EdgeOne Internet Page (here).

1. 1. Notice within Internet Status the Wi-Fi link is “greyed out” and “Off”.
2. 2. Notice within Internet Profile Status the “AP Status” is Green.

The previous two items make clear the OneDome Wi-Fi interface is operating as an Access Point, and thus can provide local LAN access for clients, however, cannot be utilized for Marina Wi-Fi access. Details on how to configure the OneDome AP is in the section *Enabling AP Mode* on page *107* and to configure back as a Wi-Fi Client is in the section *Enabling Marina Wi-Fi* on page *109*.

Figure 3-76 Internet Status – Wi-Fi is greyed out as a WAN source since it is operating as an Access Point

3.2.11.2 Adding SSID Profile

To add a new SSID profile, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.

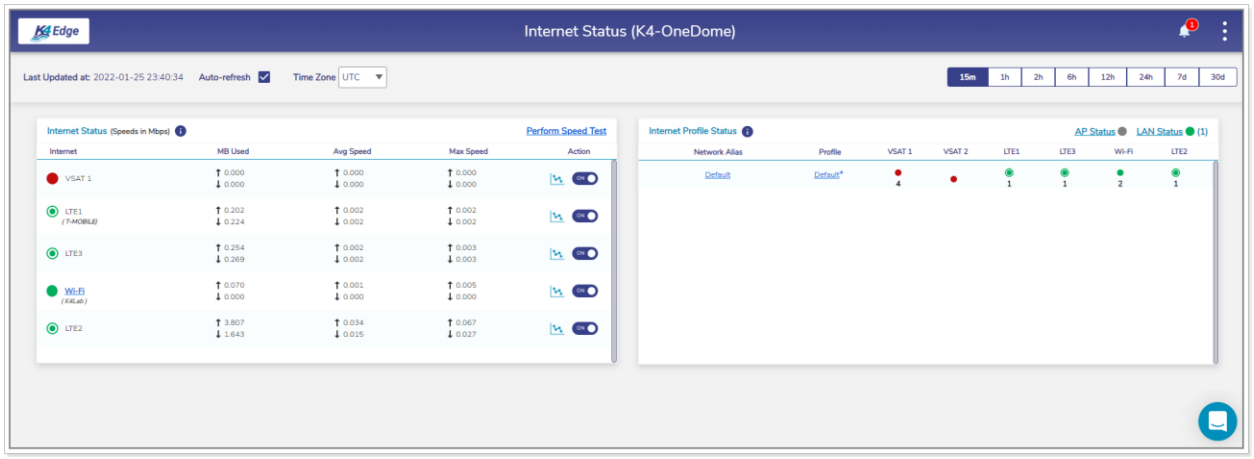

Figure 3-77 Wi-Fi Active

4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-78*.

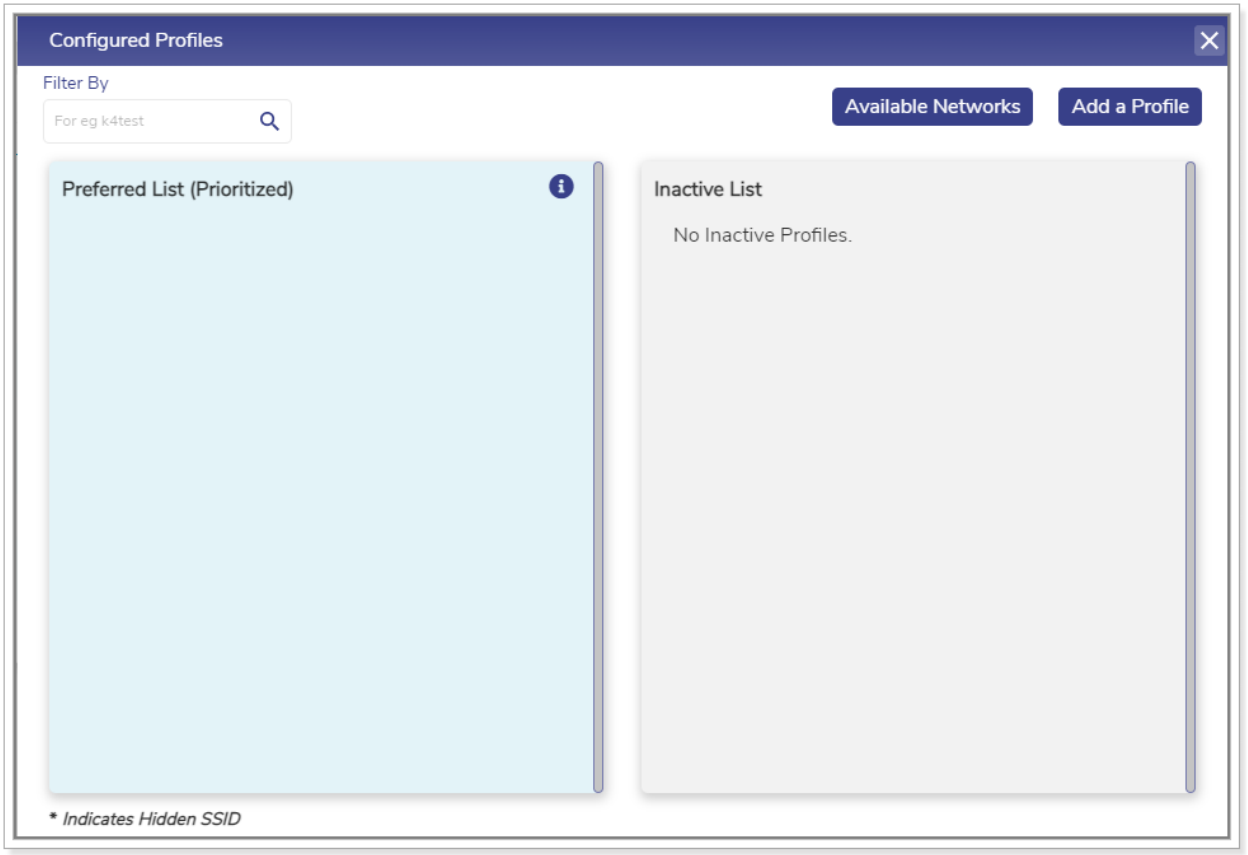

Figure 3-78 Configured Profiles

5. Click **Add a Profile**. The **Available Networks** pop-up window appears, see *Figure 3-79*. For details of the SSID information, see *Table 3-8*.

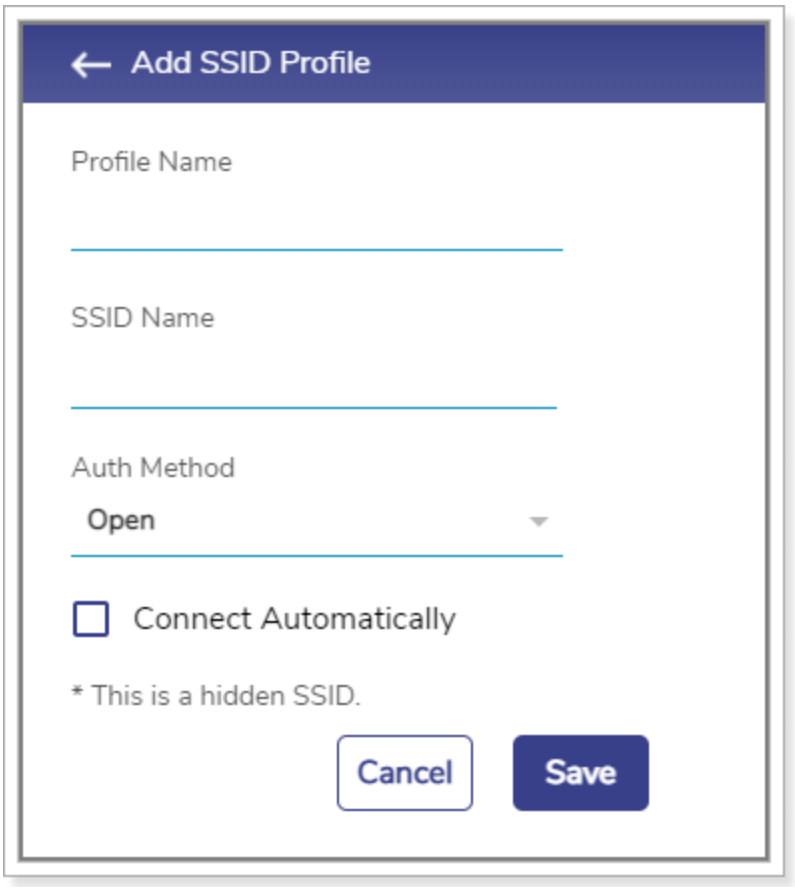

Figure 3-79 Add SSID Profile

Table 3-8 Details about SSID Profile

Fields	Description
Profile Name	Enter the unique name of the profile.
SSID Name	Enter the unique name of the SSID.
Channel	In the **Channel** list, click a channel to be used for the wireless network.
Auth Method	In the **Auth Method** list, click one of the following authentication methods. • **Open**. To allow the user to connect to the Wi-Fi without authentication, click **Open**. **NOTE:** The wireless client doesn't need the credentials. • **WPA-PSK**. To make the wireless network secure by authenticating the user, click **WPA-PSK**.

Fields	Description
	The Password field becomes available.
Password	Enter the unique password of the SSID. **NOTE:** If you specify the **WPA-PSK** authentication method in the Auth Method field, then the **Password** field becomes available.
	To view the password, click  next to the password.
	To automatically connect to the W-Fi, click the Connect Automatically check box.

6. Click **Save**.

The SSID profile is successfully added and becomes available in the **Available Networks** list. By default, the SSID is hidden. This indicates that the SSID is invisible publicly. Therefore, the SSID cannot be accessed publicly. However, the SSID is visible only privately.

The **Available Networks** list includes also the scanned SSIDs.

3.2.11.3 Adding Network in Preferred List (Prioritized)

To add a new network in the Preferred List (Prioritized), perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.

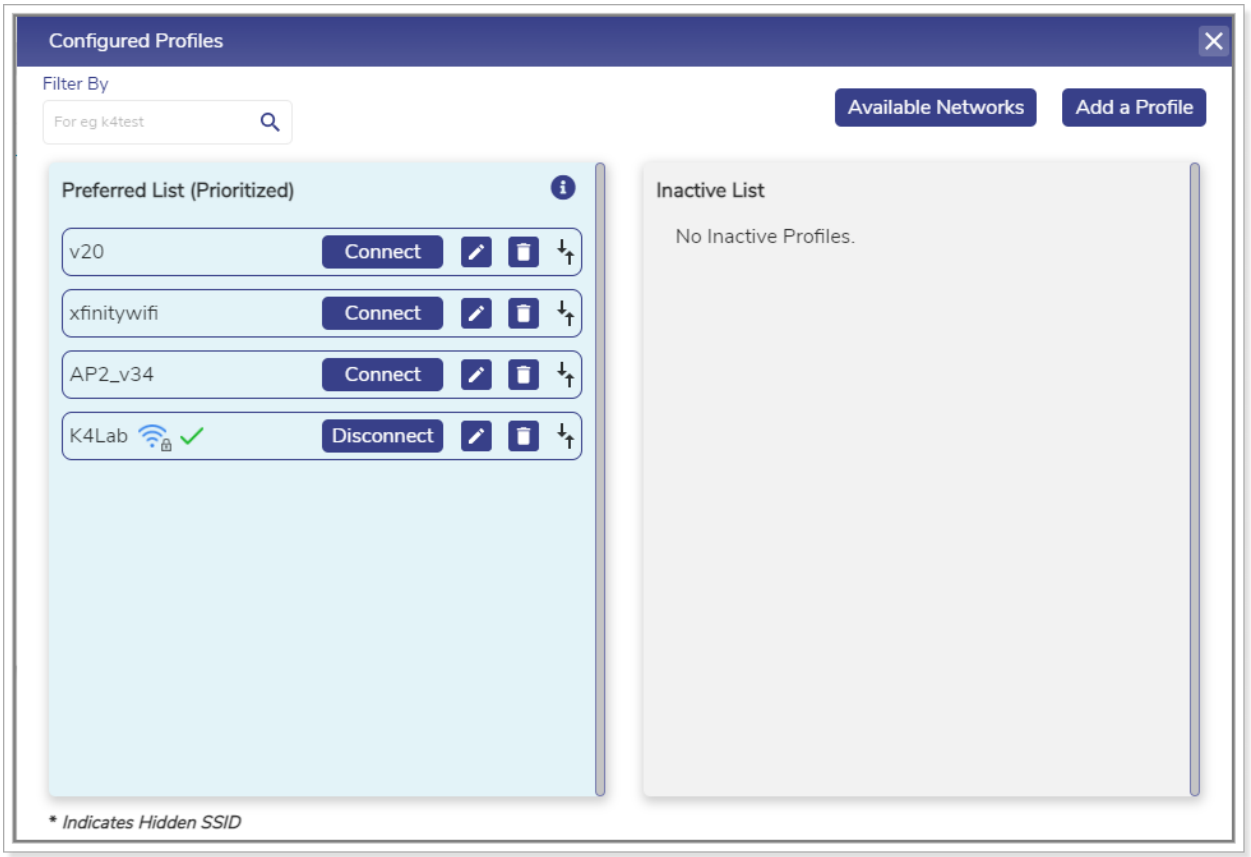

Figure 3-80 Existing SSIDs List

5. Click **Available Networks**. The **Available Networks** pop-up window appears, see *Figure 3-81*.

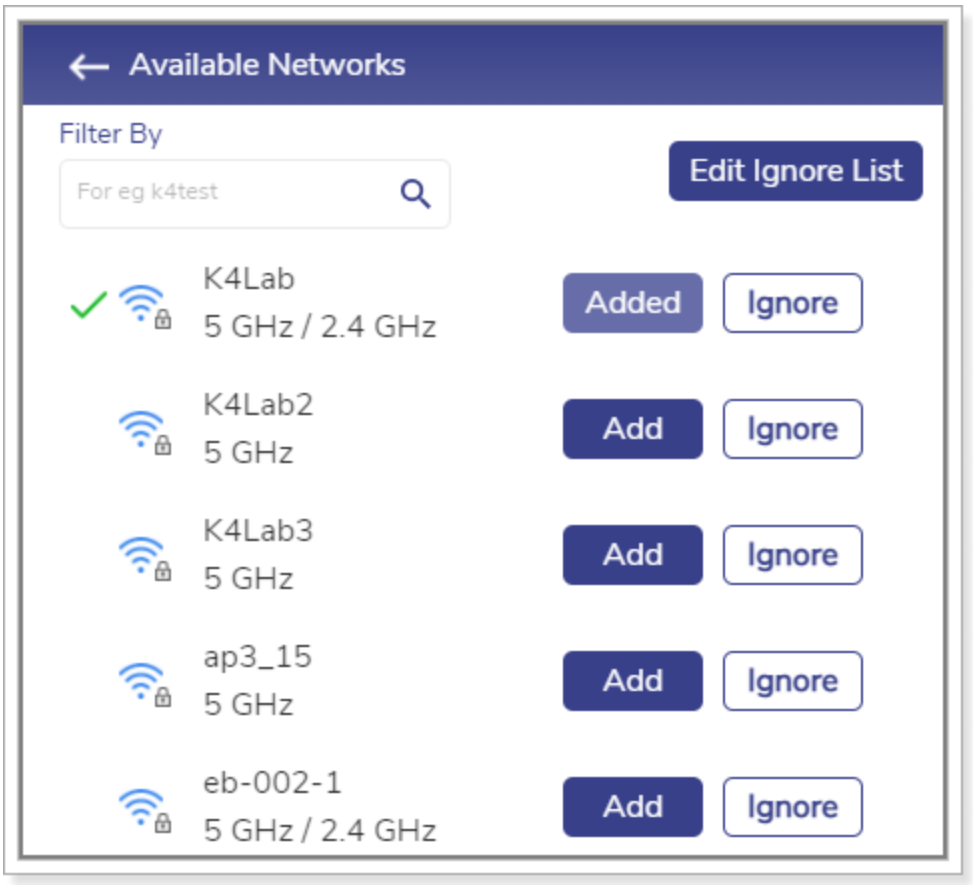

Figure 3-81 Available Wireless Networks List

6. Click **Add**. The **Add SSID Profile** pop-up window appears, see *Figure 3-82*. For details of the SSID information, see *Table 3-8*.

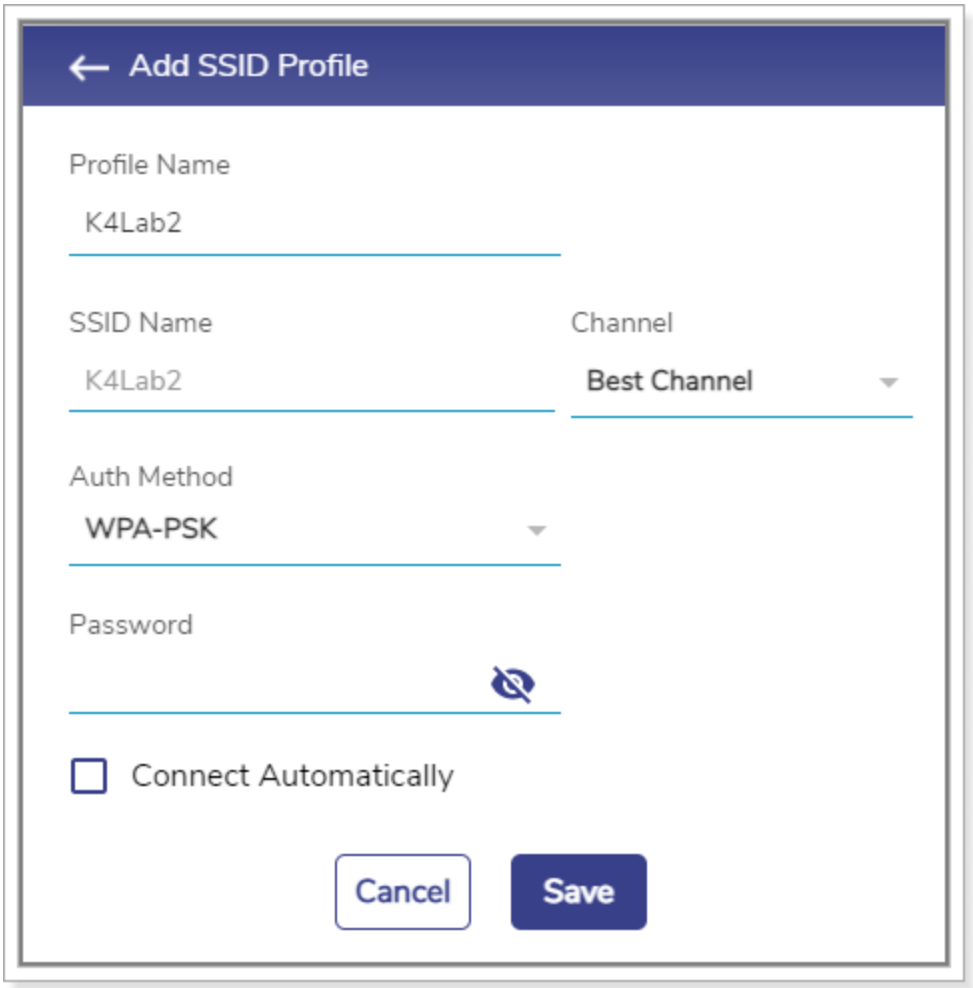

Figure 3-82 Modifying SSID Profile

7. Click **Save**.

The SSID becomes available in the **Preferred List (Prioritized)**. In addition to this, the **Add** button is not available.

3.2.11.4 Ignoring Wireless Network

To ignore the wireless network, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.

5. Click **Available Networks**. The **Available Networks** pop-up window appears, see *Figure 3-81*.
6. Click **Ignore** corresponding to the wireless network to be ignored. The **Ignore Confirmation** pop-up window appears, see *Figure 3-83*.

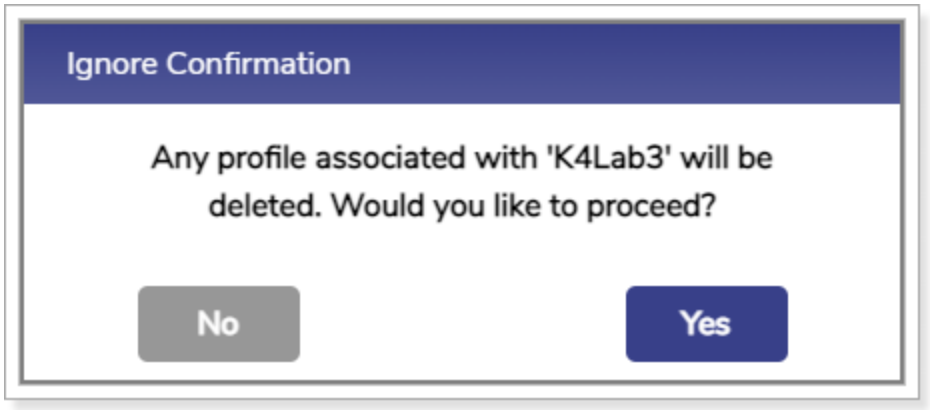

Figure 3-83 Confirm to Ignore Wireless Network

7. Click **Yes**.

The network is added to the ignored list. Therefore, it will be ignored while searching the network.

3.2.11.5 Viewing Ignored List

To view the ignored wireless network, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click **Available Networks**. The **Available Networks** pop-up window appears, see *Figure 3-81*.
6. Click **Edit Ignore List**. The **Ignore List** pop-up window appears, see *Figure 3-84*.

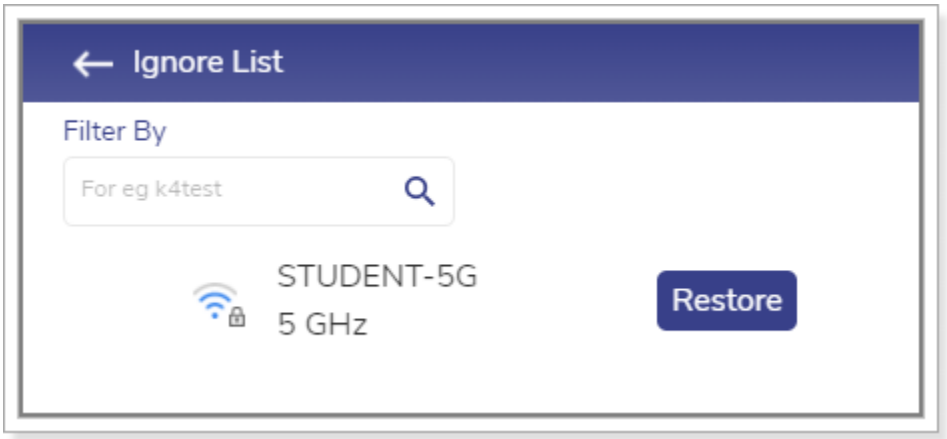

Figure 3-84 Ignore List

3.2.11.6 Restoring the Ignored Wireless Network

To restore the ignored wireless, perform the following steps

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click **Available Networks**. The **Available Networks** pop-up window appears, see *Figure 3-81*.
6. Click **Edit Ignore List**. The **Ignore List** pop-up window appears, see *Figure 3-84*.
7. Click **Restore** corresponding to the wireless network.

The wireless network becomes available in the **Available Networks** list.

3.2.11.7 Connecting to Wi-Fi

To connect to the Wi-FI, perform the following.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click **Connect** corresponding to the wireless network in the **Preferred List (Prioritized)**.

The user is connected to the Wi-Fi.

3.2.11.8 Disconnecting Wi-Fi

To disconnect the Wi-FI, perform the following.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click **Disconnect** corresponding to the wireless network in the **Preferred List (Prioritized)**.

The user is not connected to the Wi-Fi.

3.2.11.9 Modifying Details of SSID Profile

To modify details of the SSID profile, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click  corresponding to the wireless network. The **Edit SSID Profile** pop-up window appears, see *Figure 3-85*. For details of the SSID information, see *Table 3-8*.

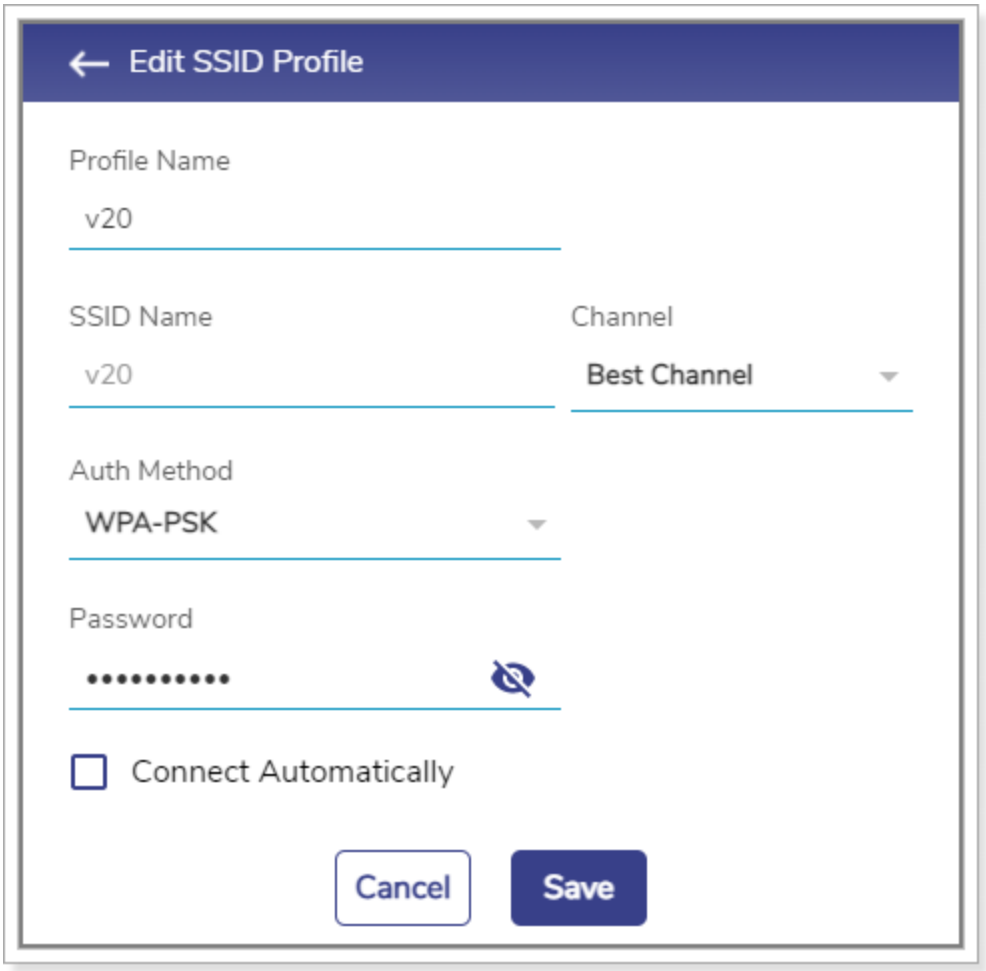

Figure 3-85 Modifying Details of SSID Profile

6. Click **Save**.

Details of the profile network are successfully modified.

3.2.11.10 Deleting the SSID

To delete the SSID, perform the following.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click corresponding to the SSID.

SSID is deleted. The users will be automatically logged out.

3.2.11.11 Modifying the Preferred List

To modify the sequence of the SSIDs, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click corresponding to the SSID and drag-and-drop the SSID in the list.

The priority of the SSID is modified.

3.2.11.12 Configuring Signal Strength Threshold

To configure the signal strength threshold, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click . The **Signal Strength Threshold (dBm)** pop-up window appears, see *Figure 3-86*.

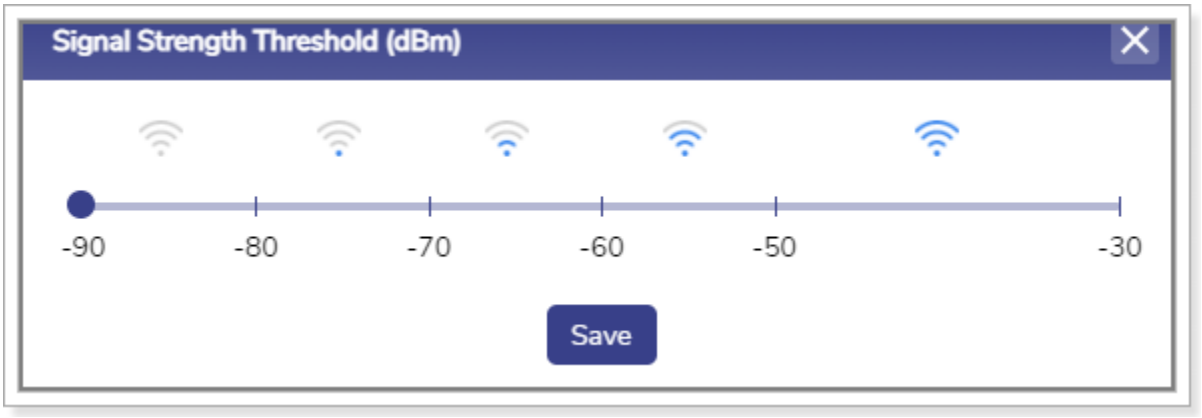

Figure 3-86 Signal Strength Threshold

6. Click the signal frequency.
7. Click **Save**.

The signal strength threshold is configured.

3.2.11.13 Blocking the SSID

To block the SSID, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-80*.
5. Click corresponding to the SSID and drag-and-drop that SSID in the **Inactive List** section, see *Figure 3-87*.

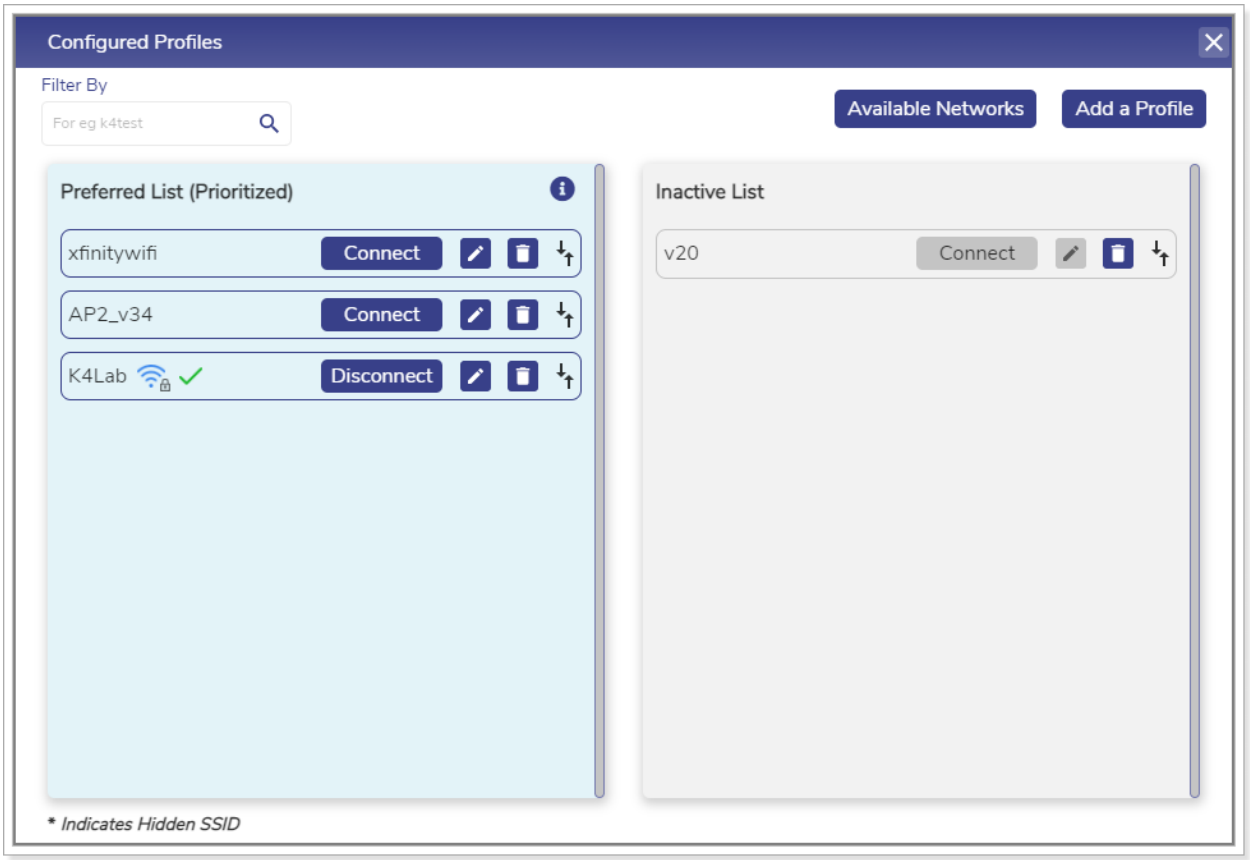

Figure 3-87 Inactive List

The user cannot connect to the SSIDs that are added in the **Inactive List**.

You can delete and move the SSID.

3.2.11.14 Unblocking the SSID

To unblock the SSID, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Internet (WAN) Status**. The **Internet Status** page appears, see *Figure 3-77*.
4. Click **Wi-Fi** in the **Internet Status** section. The **Configured Profiles** pop-up window appears, see *Figure 3-87*.
5. Click  corresponding to the SSID and drag-and-drop that SSID in the **Preferred List (Prioritized)** section.

The user can connect to the SSIDs that are available in the **Preferred List (Prioritized)**.

4 Installing K4 OneDome Ethernet to SDWAN System

Now that the Ethernet, IP Networking, and LTE status are validated for the K4 OneDome, the Ethernet cable/connection from the K4 OneDome can be moved from the Laptop to the SDWAN System WAN port.

The SDWAN system configuration should allow for:

44. WAN port supports 1000BaseT Ethernet.
45. The WAN port has DHCP Client services enabled such that the K4 OneDome can assign IP info to the SDWAN system.
46. The K4 OneDome will assign the following.
47. Client IP
48. Client IP Subnet mask
49. GW IP
50. DNS IP
51. The IP space utilized by default is 192.168.231.0/24; the K4 OneDome will utilize 192.168.231.1

The SDWAN system can monitor the K4 OneDome link state using ICMP, HTTP, DNS, or other similar probing services. If the SDWAN system is a K4 Edge service, it is not recommended to run Advanced Bonding via the K4 OneDome. For more details please contact your K4 representative.

To manage and access the K4 OneDome Edge Portal, see *Commissioning K4 OneDome* on page *31*.

5 Debugging

You can debug or troubleshoot the common issues that arise on the vessel

5.1 Client cannot connect to the network

If the MAC address of the device of the client is not assigned to the network, then the client cannot connect to the network.

To verify whether the MAC address of the device is assigned to the network, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Configuration Wizard**. The home page appears, see *Figure 2-4*.
4. Click **Access Networks**. The **Access Networks** page appears, see *Figure 2-12*.
5. Perform steps to view network usage. For details, see *Viewing Network Usage Data* on page *60*.

   If the MAC address of the device is unavailable, then the client cannot connect to the network.

However, you can view the historical details about the network and device to verify whether the MAC address of the device is assigned to the network.

To view the historical details about the network, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-33*.
4. Perform steps to view details about the network and device. For details, see *Top Networks* on page *125* and *Top Devices* on page *127*.

   If the MAC address of the device is unavailable, then the client cannot connect to the network.

5.2 Client cannot access the internet

If the internet of a network is paused, then the entire device connected to that network cannot access the internet. If the internet of a specific device is paused, then that device cannot access the internet.

To verify the status of the internet of the network and device, perform the following steps.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Usage Status**. The **Usage Status** page appears, see *Figure 3-33*.
4. Verify whether the internet is paused for the network under the **Top Networks** section. If the internet is paused, then resume the internet. For details, see *Top Networks* on page *125*.

   Or,

   Verify whether the internet is paused for the device under the **Top Devices** section. If the internet is paused, then resume the internet. For details, see *Top Devices* on page *127*.

5.3 Client cannot access an application

If the application, or domain, or IP address of the domain is blocked while configuring the traffic policy, then the client cannot access the application.

To verify the device traffic policy, perform the following policy.

1. Log on to the K4 OneDome server. The home page appears, see *Figure 2-4*.
2. Click vertical ellipsis, see *Figure 2-5*. The options become available, see *Figure 3-2*.
3. Click **Other Settings**. The **Other Settings** page appears, see *Figure 2-46*.
4. Access the **Device Traffic Policies** section.
5. Verify the device traffic policy.
6. Click **Traffic Policies**. The **Traffic Profiles** page appears, see *Audit Traffic Policies* on page *71*.
7. Click **Device**.
8. Click  corresponding to the traffic policy.
9. Access the **Application Policy Profile** section.

Verify the rules configured and allow the application.

Index