

EdgeOS System

User Guide

About EdgeOS System User Guide

The EdgeOS System User Guide provides information on how to manage and monitor the EdgeOS System.

Target Audience

This guide will be helpful for both beginners and experienced system hardware engineers that participate in installing, commissioning, and monitoring the EdgeOS System.

This guide includes the following chapters:

1. [Installing EdgeOS System](#) - This chapter introduces the EdgeOS System and its interfaces.
2. [Registering EdgeOS System](#) – This chapter provides the steps to register (Assign Site and Name) the EdgeOS System.
3. [Commissioning EdgeOS System](#) - This chapter provides the steps to commission the EdgeOS System.
4. [Monitoring](#) - This chapter provides the steps to monitor the EdgeOS System after its physical installation.
5. [Debugging](#) - This chapter provides the steps to debug and resolve issues raised by the users and clients.

The following conventions are used throughout the guide:

- *Italic* - Figures and tables links are in italic.
- **Bold** - Buttons and the name of the pages are in **Bold**.

Table of Contents

About EdgeOS System User Guide	1
1 Installing EdgeOS System.....	7
1.1 Enterprise Internet and LAN Management System	7
1.2 EdgeOS System - Physical Design	9
2 Registering EdgeOS System	11
2.1 Pre-requisites for Registration	11
2.1.1 Activating personalized Account.....	12
2.1.2 Installing Edge Mobile App	14
2.1.3 Powering up EdgeOS System and connecting to Internet	15
2.2 Registration Process.....	17
2.2.1 Registering EdgeOS System with SPORT	17
2.2.2 Registering EdgeOS System with Edge Mobile App.....	20
2.2.3 Login to EdgeOS via EdgeOS Portal	23
2.2.4 Viewing EdgeOS System through SPORT	25
3 Commissioning EdgeOS System.....	27
3.1 Interfaces	29
3.1.1 Viewing configured Interfaces details.....	29
3.1.2 Updating an existing Interface.....	31
3.1.2.1 Updating a WAN Interface	35
3.1.2.2 Configuring a WAN Interface as Starlink	36
3.1.2.3 Configuring a WAN Interface as L-Band	37
3.1.2.4 Configuring UWAN1 Interface as Ext5G.....	38
3.1.2.5 Updating a LAN Interface	40
3.1.2.6 Updating a VSAT Mgmt Interface	41
3.1.3 Adding a New Sub Interface.....	43
3.2 Access Network	64
3.2.1 Adding New Connected Network.....	64

3.2.2	Adding a Managed Routed Network	76
3.2.3	Modifying Network.....	79
3.2.4	Modifying Device Profile	80
3.2.5	Viewing Network Usage Data.....	81
3.2.6	Configuring Captive Access Network	86
3.2.7	Configuring Konnect VPN	89
3.2.8	LAN Monitoring.....	90
3.2.8.1	Configuring Periodicity of Monitoring	92
3.2.8.2	Adding to Konnect.....	93
3.2.8.3	Removing from Konnect	94
3.2.8.4	Deleting the Monitored Devices	95
3.2.9	Pausing or Resuming Network Traffic.....	96
3.2.10	Deleting Network	98
3.3	WAN Profiles	99
3.3.1	WAN Profile Types.....	99
3.3.1.1	Strict Priority.....	99
3.3.1.2	Bonding.....	99
3.3.1.3	Advanced Bonding.....	100
3.3.2	Enabling Advanced Bonding	101
3.3.3	Creating a new WAN Profile	102
3.3.4	Editing a WAN Profile.....	107
3.3.5	Deleting a WAN Profile.....	108
3.4	Traffic Policies	109
3.4.1	Creating a new Network Traffic Policy	109
3.4.2	Creating a new Device Policy	124
3.4.3	Editing an existing Traffic Policy	125
3.4.4	Deleting a Traffic Policy	126
3.5	General Settings	127
3.5.1	Device Traffic Policies	127
3.5.1.1	Configuring Device Traffic Policies	127
3.5.2	Static Routes Configuration	132
3.5.2.1	Configuring Static Routes.....	132

3.5.3	Firewall Settings	134
3.5.3.1	Modifying Firewall Rule	139
3.5.3.2	Disabling Firewall Rule	140
3.5.3.3	Enabling Firewall Rule.....	141
3.5.3.4	Deleting Firewall Rule	148
3.5.3.5	Defining New Priority of the Firewall Rules	142
3.5.3.6	Resetting the Number of Packets.....	143
3.5.4	DNS Proxy Settings.....	144
3.5.4.1	Configuring DNS Proxy Settings.....	144
3.5.5	Multicast Settings	149
3.5.5.1	Disabling the Multicast Traffic	149
3.5.5.2	Enabling the Multicast Traffic	151
3.5.6	Konnect VPN	152
3.5.6.1	Konnect VPN Server Settings.....	153
3.5.6.2	Adding a new VPN Client	154
3.5.6.3	Adding a New VPN Connection	156
3.5.7	Quality of Service	158
3.5.7.1	Disabling QoS	159
3.5.8	Config Backup/Config Upload	160
3.5.8.1	Creating new Configuration Backup	160
3.5.8.2	Uploading Configuration from Backup	162
4	Monitoring EdgeOS System.....	165
4.1	Monitoring Alerts	165
4.1.1	Viewing Alerts	165
4.1.2	Clearing an Alert.....	168
4.1.3	Deleting an Alert.....	169
4.1.4	Clearing all Alerts.....	170
4.2	System Information	171
4.2.1	Viewing System Information.....	171
4.2.2	Installing latest Firmware	176
4.2.3	Viewing System Uptime.....	179
4.3	Manage Accounts.....	180

4.3.1	Adding a User Account.....	180
4.3.2	Disabling a User Account.....	187
4.3.3	Deleting a User Account.....	190
4.3.4	Changing the Login Password.....	192
4.3.5	Changing EdgeOS Login Password.....	194
4.4	Configuration Wizard.....	196
4.5	Internet (WAN) Status.....	198
4.5.1	Viewing Internet Status Page	198
4.5.2	Viewing Interfaces Status.....	201
4.5.2.1	Viewing Realtime Chart.....	203
4.5.2.2	Viewing Controllers.....	203
4.5.2.3	Performing Speed Test on an Interface.....	204
4.5.2.4	Disabling an enabled Interface	205
4.5.2.5	Enabling a disabled Interface	205
4.5.2.6	Viewing Performance Chart for an Interface	207
4.5.3	Network Usage Level	209
4.5.3.1	Viewing Usage for an Interface	209
4.5.3.2	Viewing Top Applications	210
4.5.4	LAN Status	213
4.5.5	Konnect VPN	214
4.5.6	Internet Profile	217
4.5.6.1	Performing Speed Test on a Bonded Link.....	219
4.5.6.2	Viewing detailed status of WAN Profiles	220
4.5.7	Geolocation	222
4.6	Performance Charts	223
4.6.1	Viewing Performance Charts.....	223
4.7	Weighting Charts	227
4.7.1	Viewing Weighting Charts	228
4.8	Usage Status.....	232
4.8.1	Top Networks.....	234
4.8.1.1	Modifying Traffic Policy of a Network.....	235
4.8.1.2	Pausing Traffic on a Network	236

4.8.1.3	Resuming Traffic on a Network	237
4.8.1.4	Viewing Top Applications for a Network	238
4.8.2	Top Devices	239
4.8.2.1	Viewing list of Paused Devices	240
4.8.2.2	Editing Traffic Policy of a device	241
4.8.2.3	Pausing internet on a device	242
4.8.2.4	Resuming internet on a Device	243
4.8.2.5	Viewing Top Applications for a Device	250
4.9	VSAT Controller	245
4.9.1	Viewing VSAT Analytics	245
4.9.2	Viewing Starlink Analytics	252
4.10	Cellular Controller	257
4.10.1	Viewing Cellular Analytics	257
4.10.2	Viewing Ext5G Analytics	263
4.11	Shell Interface	288
4.11.1	Accessing the Shell Interface	288
5	Debugging	290
5.1	Client cannot connect to the network	290
5.2	Client cannot access the internet	292
5.3	Client cannot access an application	293
6	Appendix	294
6.1	Viewing EdgeOS System through Konnect VPN	294
	Revision History	307

1 Installing EdgeOS System

1.1 Enterprise Internet and LAN Management System

The EdgeOS System supports the following interfaces:

- Gigabit Ethernet (GE) to support high-speed internet for Enterprise internet access.
- USB 5G Cellular Adaptor.
- Any Ethernet LAN source, such as a VSAT modem or hard-wired broadband internet connection.

The EdgeOS System runs the EdgeOS Platform services. It can be managed seamlessly through an integrated web portal and the Edge mobile Application. In a traditional mobile internet application, multiple devices are required to provide access to cellular internet, manage WAN sources, and route IP traffic.

The EdgeOS System supports an array of services efficiently and effectively, reducing complexity and simplifying installations. K4's software, application, Cloud systems, and advanced analytics choose the best network for the location and conditions while providing users the tools to customize their system for the best user experience. For configuration and functionality, see **Figure 1.1 Configuration of Equipment**.

The EdgeOS System efficiently integrates multiple systems into a small package that can be mounted or placed in a convenient location. See **EdgeOS System - Physical Design** for physical dimensions.

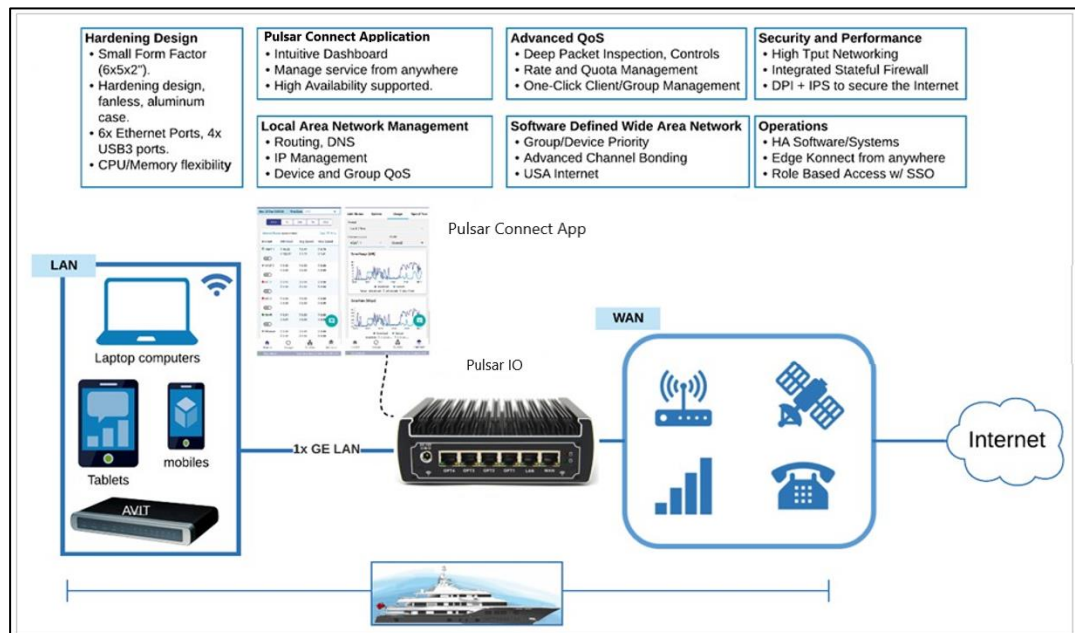


Figure 1.1 Configuration of Equipment

1.2 EdgeOS System - Physical Design

The EdgeOS System is a Small Form Factor (SFF) industrial-grade server that hosts an Intel multi-core CPU running the EdgeOS software and hosts the Mobility's carrier card. The following figures show the primary interfaces and connections of the EdgeOS System.

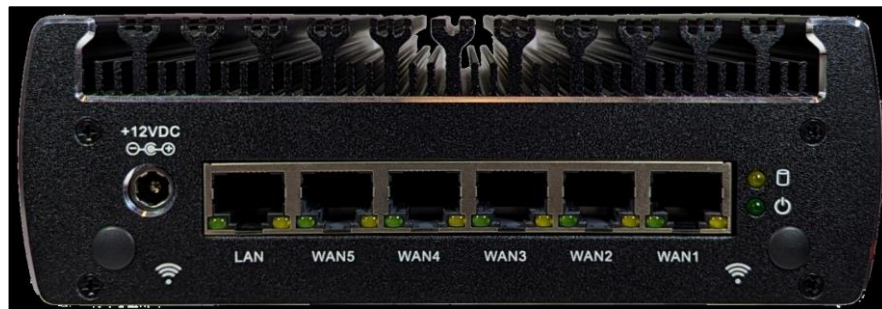


Figure 1.2 Rear View of EdgeOS System

The EdgeServer Rear contains DC input (+12V nominal), power/disk LED, LAN, and WAN Ethernet ports.



Figure 1.3 Front View of EdgeOS System

The EdgeServer Front contains a power button, HDMI, 4x USB 3.0 (SS) connections. The USB 3.0 ports provide system management and additional WAN/LAN Ethernet ports.

For details of the external interfaces and primary limits or technical specifications, refer the below table.

External Interfaces	Primary Limit or Specification
WAN Management	Supports up to 12x WAN Sources.
Ethernet	6x GE ports, additional 4x GE ports using USB expansion.
Network Configurability	Up to 500 Clients, 30 VLAN Networks; Stateful Firewall.
Compute Power	Intel i3 Dual Core 7020 at 2.3 GHz; 8 GB RAM, 128 GB Storage.
Expansion	4x USB 3.0 ports - GE or 10GE ethernet; 5G modem adapter supported.
Cooling	Passive, Fanless – Silent.
Mounting	Standalone / VESA / Rack mount kit available.
Power	+12VDC (50W Max); 100-240 VAC, 50-60 Hz (AC/DC Power Supply Included)
Physical	6.1" x 5" x 2.1" / 15.5 x 12.7 x 5.3 cm - 2.25 lbs / 1 kg
Environmental	Operating temperature: -10 to +50 C; Humidity up to 95%, non-condensing.
Warranty	1 Year limited.

Table 1.1 Technical Specifications

2 Registering EdgeOS System

The registration process associates the EdgeOS System with the user's account and the location where it is or will be installed, thus allowing full management via proprietary applications viz SPORT (Cloud Portal, also called Service Portal), Edge Mobile App and Konnect VPN.

2.1 Pre-requisites for Registration

The pre-requisites for registration process are as follows.



- Group should be existing within the K4 organization. This activity is done by Sales team as part of Group Onboarding and out of scope of this document.
- The user should have an active email account on which the Group Admin can send an activation request.
- The user should have the Edge Mobile App installed on their Mobile device.
- The EdgeOS System to be registered must be connected to the Internet.

Steps to meet these pre-requisites are as follows.

2.1.1 Activating personalized Account

To activate the personalized Account, perform the following steps.

Steps

- Share the email account that would be used for the purpose of accessing the EdgeOS System and related applications.
- The Group Admin will initiate account activation based on the user's email account, upon which the user will receive an email from Accounts, see [Figure 2.1 Invitation to Register Account](#).
- Click on  button at the bottom of the email body. The user is directed to the Account Registration System, see [Figure 2.2 Registration Page](#).
- Enter the required details in the form.
- Click  button.

The account will be activated successfully. At this point the user can access the EdgeOS Portal, Edge Mobile App, Konnect Application and SPORT.

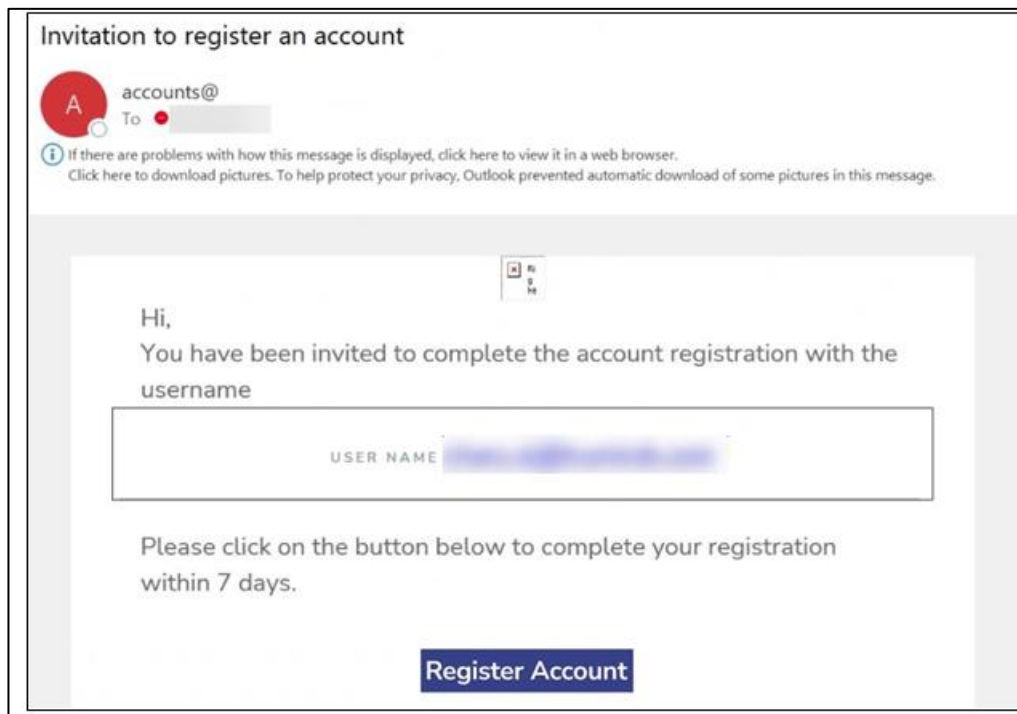


Figure 2.1 Invitation to Register Account

This is a screenshot of a web registration page titled "Registration". It instructs the user to "Please fill following fields for the Username : test_juried_jur_2011@madinator.com to complete the registration." The form includes several input fields: "FIRST NAME*", "LAST NAME*", a phone number field with a dropdown menu showing a flag and "+1", "PASSWORD*", and "CONFIRM PASSWORD*". Each of the last four fields has a small eye icon to toggle visibility. A note specifies: "Note: Password length should be minimum 5 characters and maximum 29 characters". A light blue "REGISTER" button is located at the bottom right of the form.

Figure 2.2 Registration Page

2.1.2 Installing Edge Mobile App

To install the Edge Mobile App, perform the following steps.

Steps

- On the Mobile device, open the App Store or Play Store.
- Search for the '**K4 Edge**' App and download it.
- Open the app to see login screen, see [Figure 2.3 Application Login Page](#).
- Login to the app with the activated account credentials.

The user is successfully logged into the Edge Mobile App.

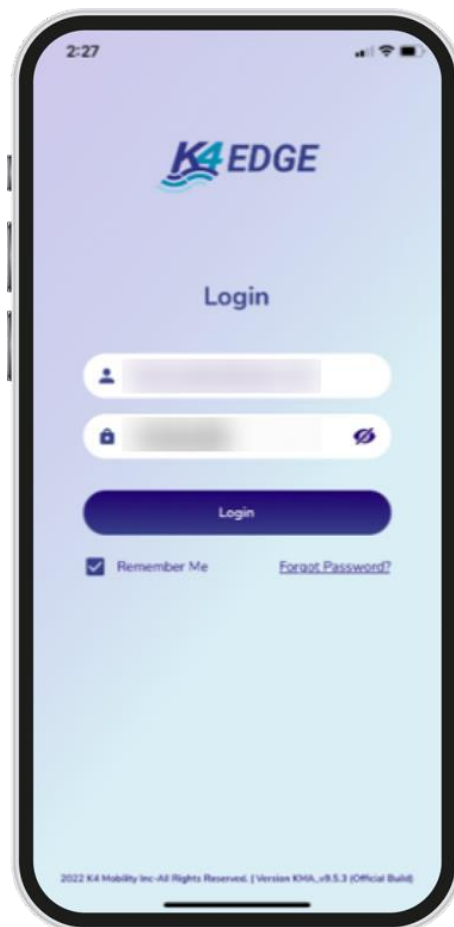


Figure 2.3 Application Login Page

2.1.3 Powering up EdgeOS System and connecting to Internet

Before getting started, the user must ensure that the EdgeOS System is installed and powered up as defined in the previous section [1.1 Installing EdgeOS](#).

If there is some doubt, then audit the system, and it is reasonable to power cycle the EdgeOS System before starting. The proper power cycle procedure is to disconnect the EdgeOS System AC Power plug from a UPS AC Outlet for 20 seconds and then re-insert. The EdgeOS System 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.

IT IS VERY IMPORTANT that POWER SUPPLY to the EdgeOS System is stable and does NOT blink on/off frequently, thus UPS connectivity and clean power off/on requirements are stated. Please contact the system administrator to recommend appropriate UPS solutions for the EdgeOS System.

If the EdgeOS System is properly powered up, verify the LAN Ethernet link from the EdgeOS System is operating as intended.

To verify the LAN Ethernet link and IP connectivity to the EdgeOS System, perform the following steps.

Steps

- Connect a laptop Ethernet port to the EdgeOS System RJ45 LAN Ethernet port, see section [1.2 EdgeOS System - Physical Design](#)— leftmost port. The laptop Ethernet port should be configured for DHCP Client services and will request an IP from the EdgeOS System.
- 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 EdgeOS System by default has DHCP enabled and will assign the IP

address within the 192.168.230.0/24 space. The EdgeOS System will have the GW IP address of 192.168.230.1 and DNS of 8.8.8.8.

Depending on the connectivity of the CELL (LTE) system, the user may/may-not have Internet connectivity.

- 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 is up and IP is assigned to the laptop, then the system is ready for registration.

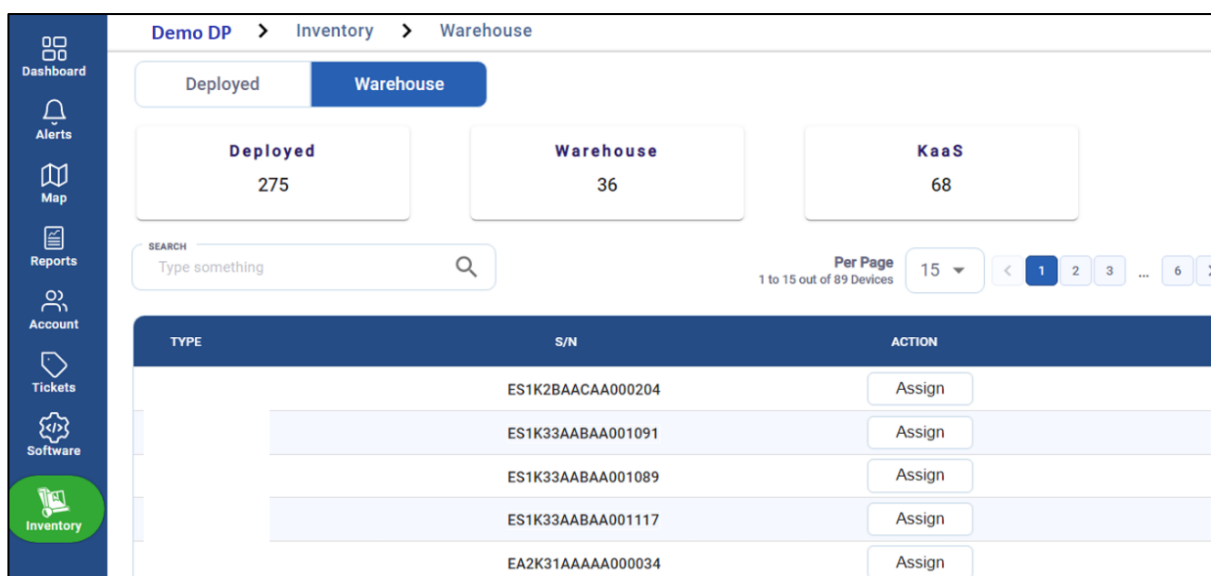
2.2 Registration Process

2.2.1 Registering EdgeOS System with SPORT

After the pre-requisites are met, the user can go ahead with the registration process. To do the registration using SPORT, follow the steps described below.

Steps


- Open SPORT using the link <https://www.sportK4mobility.com/>
- Login with valid credentials.
- Select Inventory from the left menu bar.
- Click the Warehouse tab. The list of all available devices displays in the table below.

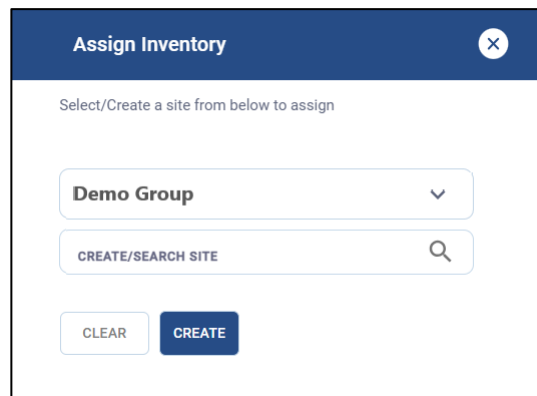


The screenshot shows the 'Warehouse' tab in the SPORT interface. The left sidebar contains navigation links: Dashboard, Alerts, Map, Reports, Account, Tickets, Software, and Inventory (highlighted). The main content area has a breadcrumb trail 'Demo DP > Inventory > Warehouse' and two tabs: 'Deployed' and 'Warehouse' (selected). Below the tabs are three summary cards: 'Deployed' with 275, 'Warehouse' with 36, and 'KaaS' with 68. A search bar with the placeholder 'Type something' and a magnifying glass icon is present. To the right of the search bar, it says 'Per Page 15' and '1 to 15 out of 89 Devices'. Below this is a table with columns 'TYPE', 'S/N', and 'ACTION'. The table lists five devices with their S/N numbers and an 'Assign' button for each.

TYPE	S/N	ACTION
	ES1K2BAACAA000204	Assign
	ES1K33AABAA001091	Assign
	ES1K33AABAA001089	Assign
	ES1K33AABAA001117	Assign
	EA2K31AAAAA000034	Assign



Figure 2.4 Warehouse Tab

- Note the serial number of the device as mentioned on the box. In the SEARCH field, enter this serial number of the device.
- The table displays the device details corresponding to the serial number.
- To assign the device to a Group and Site, click the  Assign button. The Assign Inventory dialog box opens.
- Select the required Group from first dropdown menu.



The image shows a dialog box titled "Assign Inventory" with a close button (X) in the top right corner. Inside the dialog, there is a subtitle "Select/Create a site from below to assign". Below this, there is a dropdown menu currently showing "Demo Group" with a downward arrow. Underneath the dropdown is a search field labeled "CREATE/SEARCH SITE" with a magnifying glass icon. At the bottom of the dialog, there are two buttons: a light blue "CLEAR" button and a dark blue "CREATE" button.

Figure 2.5 Assign Inventory Dialog Box

- Next the user has to select the site. The Site Name must be unique for the Group deployment. Multiple EdgeOS nodes can be in a single Site. The options here are to use an existing Site or add a new Site.
- In the CREATE/SEARCH SITE field, type the name of the required site.
- Select the site from the list of existing sites in the system.
- Click  ASSIGN to assign the device to the selected site.
- To add a new Site, enter the name of the site and click  CREATE. This will create a new site and assign the device to that site.
- Once assigned, the device gets moved from the Warehouse tab and is displayed under the Deployed tab.

- The table in the Deployed tab displays information such as Site name, Device type, Serial number, Registration date, Organization name etc.

Deployed

Warehouse

Deployed

170

Warehouse

36

KaaS

65

SEARCH

Type something

Per Page

1 to 15 out of 117 Sites

15

< 1 2 3 ... 8 >

SITE	TYPE	S/N	REG. DATE	ORGANIZATION	ACTION
<div>1000</div>					

Figure 2.6 Deployed Tab

This completes the Registration Process.

2.2.2 Registering EdgeOS System with Edge Mobile App

The registration process can also be done using the Edge Mobile App. The workflow is depicted in the figure below.

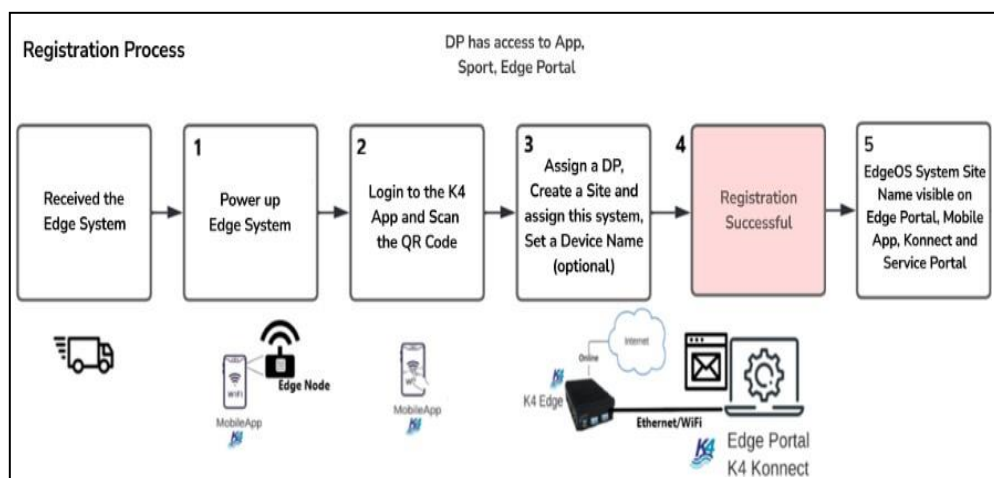






Figure 2.7 Registration Workflow



To register the EdgeOS System, perform the following steps, see [Figure 2.8 Registration Flow via Edge Mobile App](#).

The workflow detailed below is using the Edge Mobile App.

Steps

- Login to the Edge Mobile App. The landing screen of the application will open.
- Click on  Register New Product button.
- Click on  Scan QR Code button. The QR Code scan option becomes available.
- Scan the QR Code available on the EdgeOS System box. The system is identified, and its serial number and type is displayed in the table below.
- Click on  Set Distribution Partner button. This is an optional step and is required only when the system needs to be assigned to a Sub-Group within the currently assigned Group.
- Click on  Set Site Name button. A Site is a Vessel, Store, Car, Truck,

etc. where the EdgeOS System will remain present and can reliably be identified by management. The Site Name must be unique for the Group deployment. Multiple EdgeOS nodes can be in a single Site. The options here are to use an existing Site or add a new Site.

- Click on the Select Sites drop down. To add a new Site, click on Add New Site option. The Add Site popup appears. Enter the new Site Name. The Site Name is successfully updated. To assign to an existing Site, select the site from the drop down and click on  Set Site button at the bottom of the screen.
- Click on Set Location Details. This is an optional step to add Site Address, IMO, MMSI. Enter one or all details and click Submit button.
- Click on Set Device Name. This is also an optional step to identify the EdgeOS System uniquely on a particular site. Enter the Device name and click Save button.
- Click  Done button.

A success popup will be displayed for a few seconds, and the user is directed back to the Home Screen of the Edge Mobile App. This completes the Registration Process.

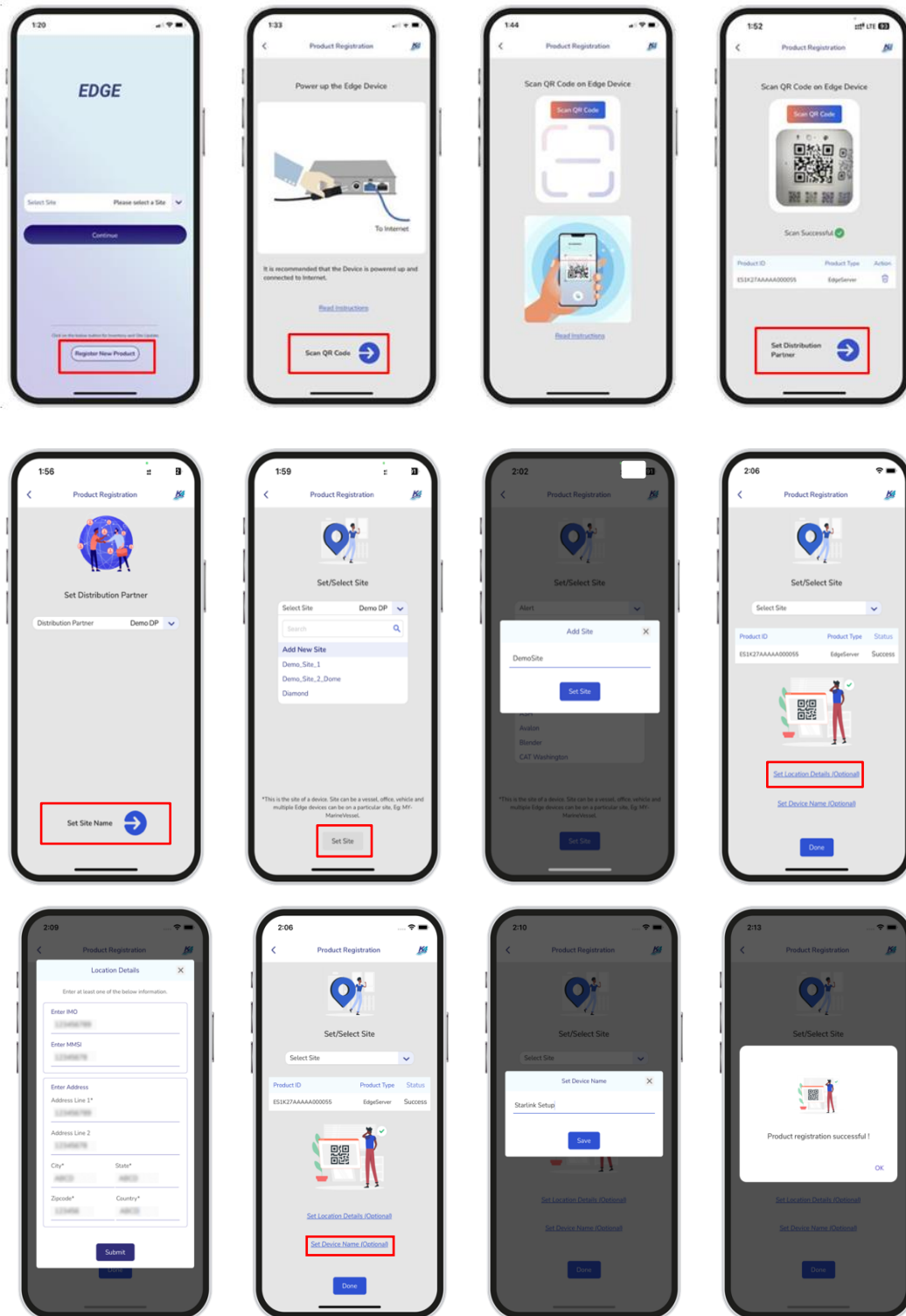


Figure 2.8 Registration Flow via Edge Mobile App

2.2.3 Login to EdgeOS via EdgeOS Portal

This section describes how to log on to the EdgeOS System via EdgeOS Portal after successful registration.

To login to the EdgeOS System via EdgeOS Portal, perform the following steps.

Steps

- Open any browser.
- Enter the IP address of <http://10.0.254.1> and hit return – The EdgeOS System IP can be accessed. The **Login** page appears, see **Figure 2.9 Login Page**.
- Enter the personalized account credentials.
- Click Login button.

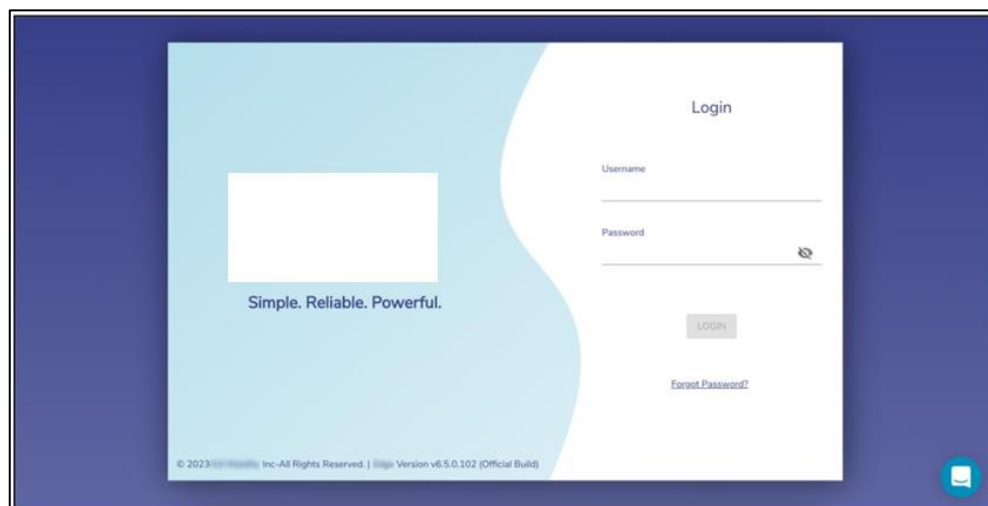


Figure 2.9 Login Page

Note: It is also possible to login to the EdgeOS Portal via a temporary login with **Username/Password** as **edge/edge**. It is possible to change the password for EdgeOS login account, see [Changing EdgeOS Login Password](#). It is however recommended to use the personalized account to view and use full functionality of the EdgeOS Portal.

- After successful login, the user will be routed to the Home Page i.e., the Configuration Wizard. EdgeOS System Configuration Steps are detailed in [Commissioning EdgeOS System](#).

To logout from the EdgeOS Portal, click on the Menu on the top right and then click **Logout**, see the figure below.

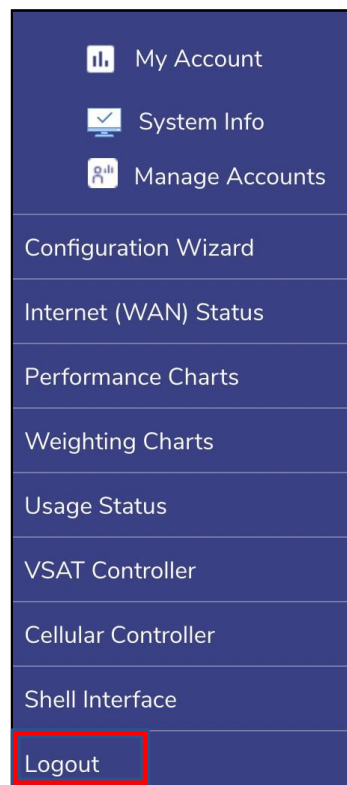


Figure 2.10 Logout Menu Option

2.2.4 Viewing EdgeOS System through SPORT

- The EdgeOS System becomes accessible via the SPORT. This portal is available on Cloud and is useful to monitor the health of the EdgeOS System and its vital statistics.

To view the EdgeOS System on SPORT, perform the following steps.

Steps

- Open <https://sport.k4mobility.com/> on the laptop's browser. The SPORT login screen appears, see [Figure 2.11 SPORT Login Page](#).
- Login to the SPORT with valid account credentials. The Site and System become available on the Home Screen. The status of the System and its Interfaces can be viewed along with other vital statistics, see [Figure 2.12 SPORT Portal](#).

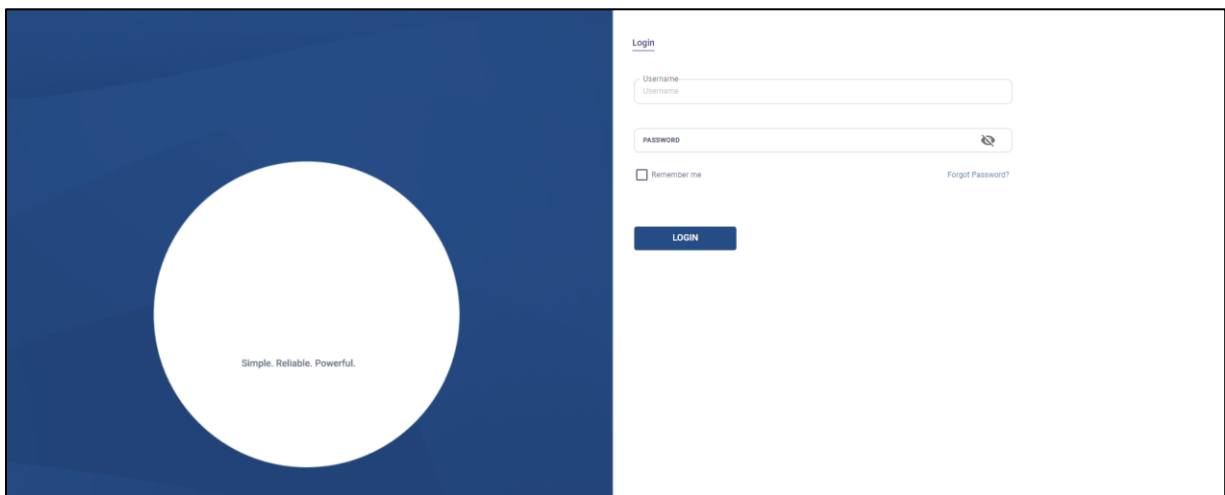


Figure 2.11 SPORT Login Page

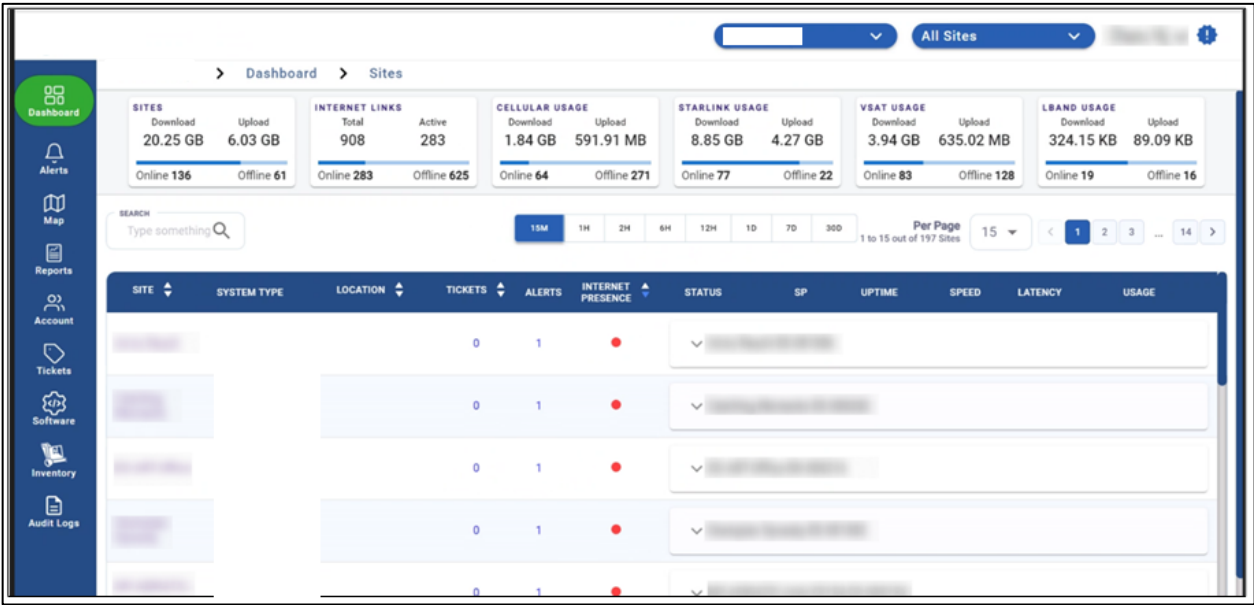


Figure 2.12 SPORT Portal

3 Commissioning EdgeOS System

Once the system is registered, it must be configured as per requirements. The steps specified to configure the EdgeOS System are defined here and performed using flow of the Configuration Wizard.

After successful login, the user will be routed to the Home Page i.e., the Configuration Wizard, see figure below.



Figure 3.1 Configuration Wizard

To understand the home page, see figure below.

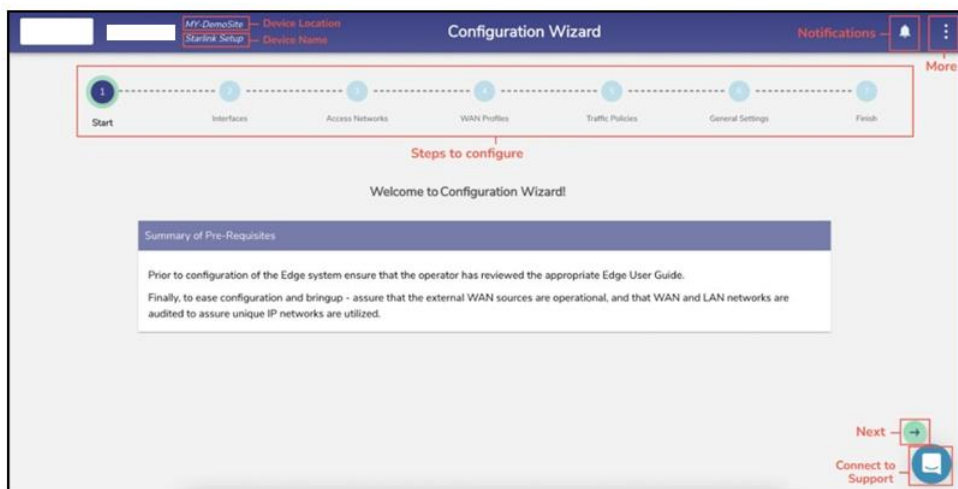


Figure 3.2 Classification of Home Page

The home page comprises of the following sections. Refer to the table below.

Sections	Description
Site Name/ Device Name	The Site Name of the System and the Device Name as configured through the Registration Process is displayed at the top left of a page.
Notifications	This displays the system alerts.
Menu	This includes additional Menu options.
Configuration Steps	These steps need to be followed to configure the EdgeOS System.

Table 3-1 Sections of Home Page

3.1 Interfaces

The user can view and update the configuration of the Interfaces present on the EdgeOS System.

3.1.1 Viewing configured Interfaces details

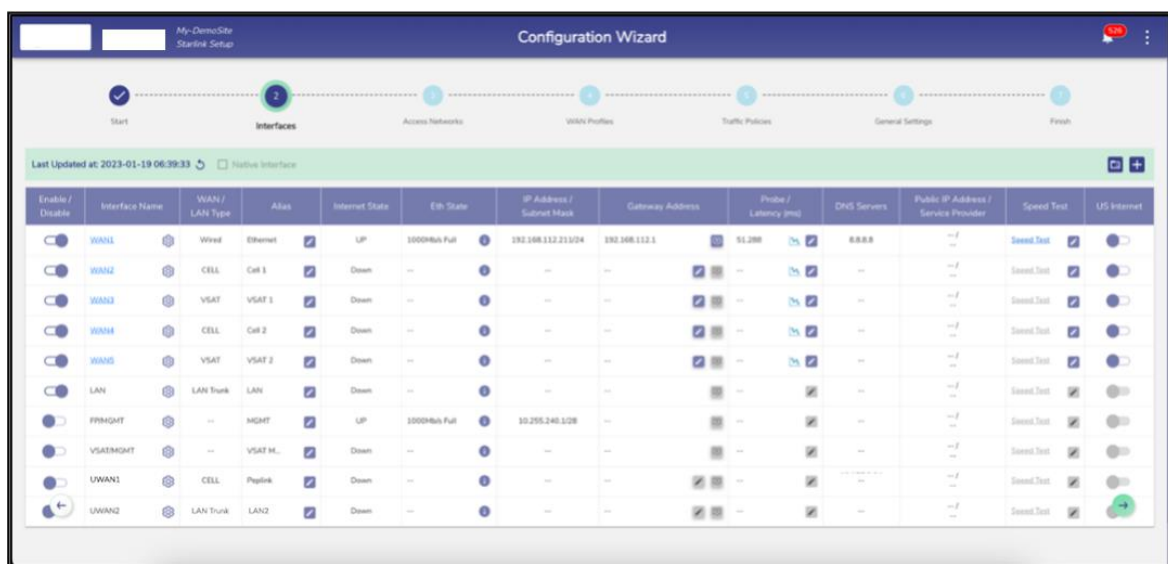
To view details of the Interfaces pre-configured on the EdgeOS System, perform the following steps.

There is a flexibility that any ethernet interface on the EdgeOS System (applicable for all products) can be configured as either WAN interface, LAN interface or for VSAT management. Along with this flexibility, VLANs can be configured on the interfaces and the same can be configured as WAN sub-interface or as LAN access port.

Note: Though some of the interfaces are physically labeled on the servers as WAN/LAN, they can be configured as per the need.

Steps



- Click  on the **Start** page or click **Interfaces**, see below.





Enable / Disable	Interface Name	WAN / LAN Type	Alias	Internet State	Eth State	IP Address / Subnet Mask	Gateway Address	Probe / Latency (ms)	DNS Servers	Public IP Address / Service Provider	Speed Test	US Internet
	WAN1	Wired	Ethernet		UP	1000Mbps Full	192.168.112.21/24	192.168.112.1		8.8.8.8		
	WAN2	CELL	Cell 1		Down	---	---			---		
	WAN3	VSAT	VSAT 1		Down	---	---			---		
	WAN4	CELL	Cell 2		Down	---	---			---		
	WAN5	VSAT	VSAT 2		Down	---	---			---		
	LAN	LAN Trunk	LAN		Down	---	---			---		
	PFWMGHT	---	MGHT		UP	1000Mbps Full	10.255.240.1/28			---		
	VSATMGHT	---	VSAT M...		Down	---	---			---		
	UWAN1	CELL	Peplink		Down	---	---			---		
	UWAN2	LAN Trunk	LAN2		Down	---	---			---		

Figure 3.3 Interface Screen

Details of the Interfaces present on the EdgeOS System are listed on the [Interfaces Screen](#) page.

NOTE: By Default, only enabled Interface are shown. To see all the interfaces, check the  All Interfaces .on the top. When checked  All Interfaces the user will be able to see all the Interfaces.

The user can also press on the refresh button  to refresh the page and get the latest data. By default, this screen refreshes every 30 seconds.

The user can upload configuration from available backup by clicking on  icon. See [3.2.1 Adding New Connected Network](#) for details.

3.1.2 Updating an existing Interface

There are three types of Interfaces i.e., WAN, LAN and VSAT Mgmt.

If the Status of an Interface is **Up**, then the various details such as State of the link, IP address or Subnet Mask populate on the Interfaces Screen. For details of attributes of each row, See tables below.



Fields	Description	Configuration
Enable/Disable 	This slider allows the user to enable or disable this network interface. User can modify an interface only when it is in the disabled state.	N/A

Table 3-2 Enable Interface

Fields	Description	Configuration
Interface Name	This indicates the network interface that is available on the vessel, along with some pre-configuration. User can edit the network interface by disabling it and then clicking on the 'gear' icon.	<p>To edit the interface, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none">• Disable the Interface.• Click the 'gear'  icon. The user will be presented with a configuration dialog. <p>In this dialog, they can modify:</p> <p>The Interface Type: WAN, LAN or VSAT Mgmt. See Figure 3.4 Interface Dialogue Box.</p>

		The 'Alias', a name for the interface.
		<p>If the Interface Type is 'WAN', user can also configure the WAN Type, which is one of:</p> <ul style="list-style-type: none"> • Cell • Wi-Fi • Wired • VSAT • VSAT-FBB (L-Band) • VSAT-LEO (Starlink) <p>See Figure 3.5 WAN Configuration.</p> <p>If Interface Type is 'LAN', user can also configure the LAN Type, which is one of:</p> <ul style="list-style-type: none"> • LAN Trunk • LAN Access. <p>See Figure 3.6 LAN Type.</p>
		<p>If the LAN Type is 'LAN Access', user must further specify the 'Sub I/F id'.</p> <p>See Figure 3.7 LAN Type Sub I/F ID .</p>
		<p>If Interface Type is VSAT Management, user can also additionally configure:</p> <ul style="list-style-type: none"> • VSAT Mgmt IP/Subnet • Alias • VSAT WAN • Modem IP • Modem Username

		<ul style="list-style-type: none"> • Modem Password • ACU IP <p>See Figure 3.8 VSAT Management .</p> <p>Click 'Save' when done, or 'X' to cancel.</p>
--	--	--

Table 3-3 Interface Name

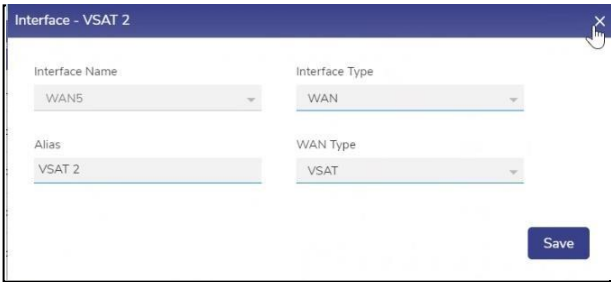


Figure 3.4 Interface Dialogue Box

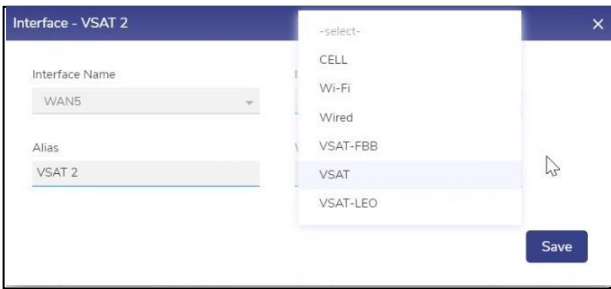


Figure 3.5 WAN Configuration

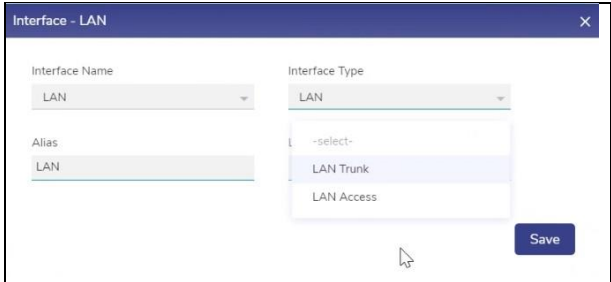


Figure 3.6 LAN Type

Interface - LAN

Interface Name: LAN

Interface Type: LAN

Alias: LAN

LAN Type: LAN Access

Sub I/F ID: eg. 10

Save

Figure 3.7 LAN Type Sub I/F ID

Interface - MGMT

Interface Name: FP/MGMT

Interface Type: VSAT Mgmt

VSAT Mgmt IP / Subnet: 10.0.1.3/24

Alias: MGMT

VSAT WAN: -select-

Modem IP: 10.0.1.1

Modem Username: eg. admin

Modem Password: eg. iDirect

ACU IP: eg. 10.0.3.2




Save

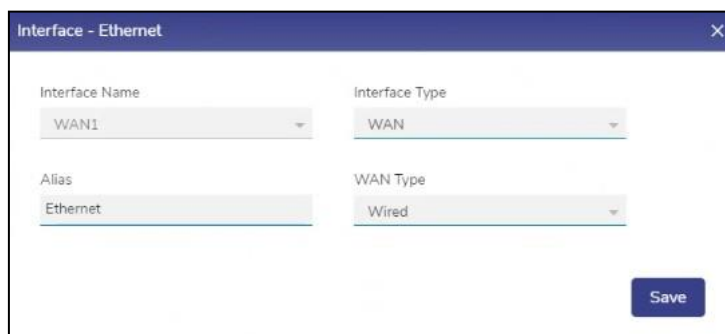
Figure 3.8 VSAT Management

3.1.2.1 Updating a WAN Interface

To update a WAN Interface, perform the following steps.

Steps

- Remove the WAN Interface to be updated from all WAN Profiles.
- Click on the  icon and disable the WAN Interface.
- Click the  icon next to the Interface. A popup appears, see [Figure 3.9 Update WAN Interface](#).
- Enter the Alias Name.
- Select the desired WAN type from the drop down, see [Figure 3.10 Select WAN](#).
- Click **Save**.
- Click on the  icon and enable the WAN Interface.
- The Interface is updated as required.



Field	Value
Interface Name	WAN1
Interface Type	WAN
Alias	Ethernet
WAN Type	Wired

Save

Figure 3.9 Update WAN Interface

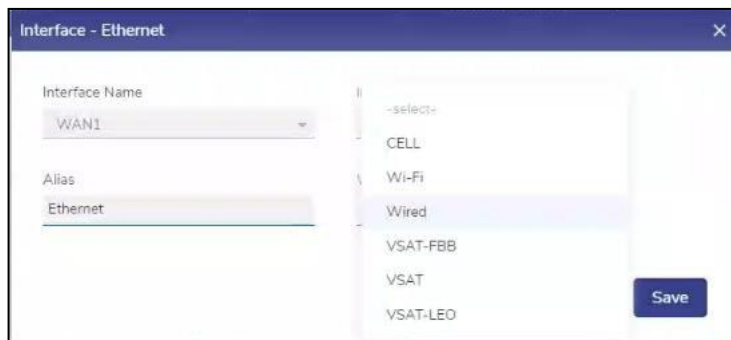





Figure 3.10 Select WAN Type

3.1.2.2 Configuring a WAN Interface as Starlink

To configure a WAN Interface as Starlink, perform the following steps.

Steps

- Remove the WAN Interface to be updated from all WAN Profiles.
- Click on the  icon and disable the WAN Interface.
- Click the  icon next to the Interface. A popup appears, see [Figure 3.9 Update WAN Interface](#).
- Select the WAN type as VSAT-LEO from the drop down, see [Figure 3.11 WAN Interface VSAT-LEO](#).
- Enter the Alias Name for the Interface.
- Click **Save**.
- Click on the  icon and enable the WAN Interface.
- The Starlink Interface is configured.

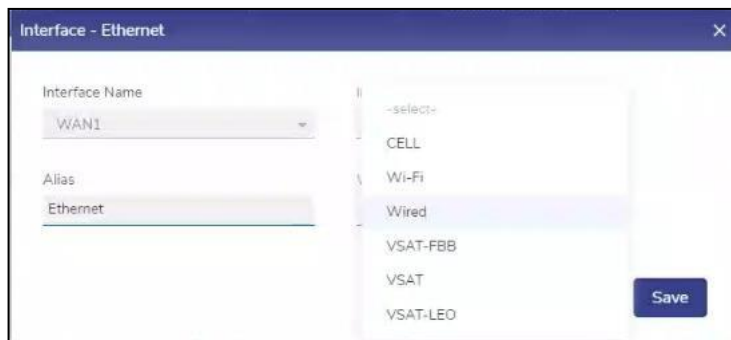





Figure 3.11 WAN Interface VSAT-LEO

3.1.2.3 Configuring a WAN Interface as L-Band

To update a WAN Interface, perform the following steps.

Steps

- Remove the WAN Interface to be updated from all WAN Profiles.
- Click on the  icon and disable the WAN Interface.
- Click the  icon next to the Interface. A popup appears, see [Figure 3.9 Update WAN Interface](#).
- Select the WAN type as VSAT-FBB from the drop down, see [Figure 3.12 Interface VSAT-FBB](#).
- Enter the Alias Name for the Interface.
- Click **Save**.
- Click on the  icon and enable the WAN Interface.
- The L-Band Interface is configured.

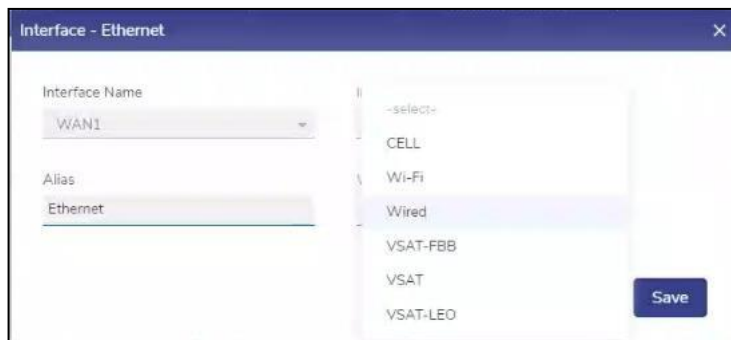




Figure 3.12 Interface VSAT-FBB

3.1.2.4 Configuring UWAN1 Interface as Ext5G

EdgeOS System variants having Ext5G modem connected, need to be configured on the Interfaces Screen. Make sure that the Ext5G modem (Peplink 5G Adaptor) is connected to the EdgeServer uWAN1 USB3 port.

To configure the UWAN1 Interface as Ext5G, perform the following steps.

Steps

- Click on the  icon and disable the UWAN1 Interface.
- Click the  icon next to the Interface. A popup appears.
- Select the Interface Type as WAN from the drop down, see [Figure 3.13 Interface Type Selection](#).

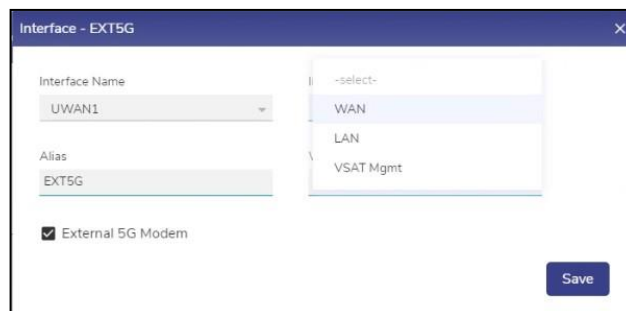


Figure 3.13 Interface Type Selection

- Select the WAN type as CELL from the drop down, see [Figure 3.14 WAN Type Selection](#).

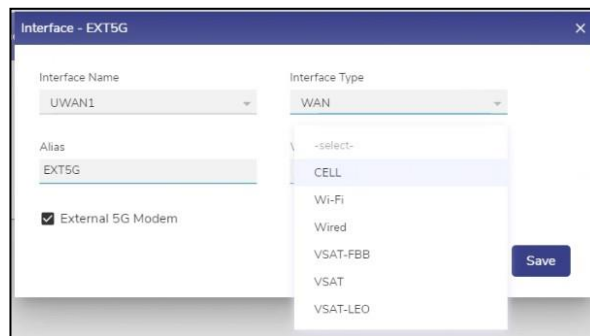


Figure 3.14 WAN Type Selection

- Enter the Alias Name for the Interface.
- Check the External 5G Modem checkbox, see [Figure 3.15 Interface EXT5G](#).

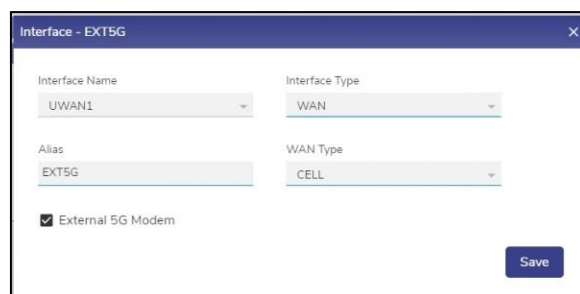






Figure 3.15 Interface EXT5G

- Click **Save**.
- Click on the  icon and enable the WAN Interface.
- The Ext5G Interface is successfully configured.

3.1.2.5 Updating a LAN Interface

To update a LAN Interface, perform the following steps.

Steps

- Click on the  icon and disable the LAN Interface.
- Click the  icon next to the Interface. A popup appears, see [Figure 3.16 LAN Type](#).
- Enter the Alias Name.
- Select the LAN type from the drop down, see [Figure 3.16 LAN Type](#).. If the LAN Type is 'LAN Access', then additionally enter the Sub I/F ID, see [Figure 3.17 LAN Type Sub I/F ID](#)
- Click **Save**.
- Click on the  icon and enable the LAN Interface.
- The LAN Interface is updated as required.

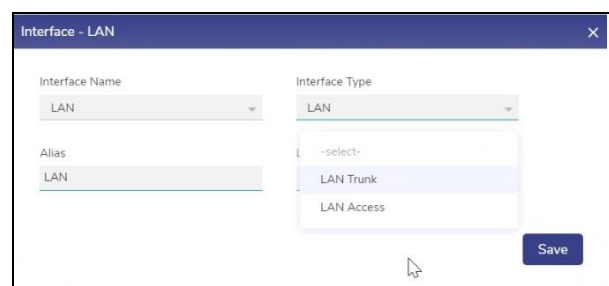





Figure 3.16 LAN Type

Figure 3.17 LAN Type Sub I/F ID

3.1.2.6 Updating a VSAT Mgmt Interface

To update a VSAT Mgmt Interface, perform the following steps.

Steps

- Click on the  icon and disable the Interface.
- Click the  icon next to the Interface. A popup appears, see [Figure 3.18 Select VSAT Mgmt Interface.](#)
- Enter the respective fields
- Click **Save**.
- Click on the  icon and enable the VSAT Mgmt Interface.
- The Interface is updated as required.

Interface - MGMT

Interface Name

FP/MGMT

Interface Type

VSAT Mgmt

VSAT Mgmt IP / Subnet

10.0.1.3/24

Alias

MGMT

VSAT WAN

-select-

Modem IP

10.0.1.1

Modem Username

eg. admin

Modem Password

eg. iDirect

ACU IP

eg. 10.0.3.2


Save

Figure 3.18 Select VSAT Mgmt Interface

3.1.3 Adding a New Sub Interface

To Add New Sub Interface, perform the following steps.

Steps

- Click on the Add Icon  on the top right of the Interfaces screen.
- The user is prompted with add new interface dialogue box. See figure below.

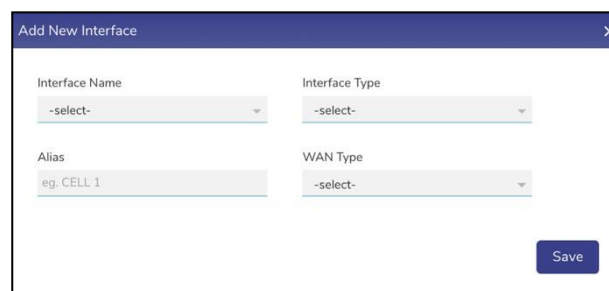
A dialog box titled "Add New Interface" with a close button (X) in the top right corner. It contains four input fields: "Interface Name" with a dropdown menu showing "-select-", "Interface Type" with a dropdown menu showing "-select-", "Alias" with a text input field containing "eg. CELL 1", and "WAN Type" with a dropdown menu showing "-select-". A "Save" button is located at the bottom right.

Figure 3.19 Add New Interface

- Select the parent **Interface Name** from the Interface Drop-Down Menu. See figure below.

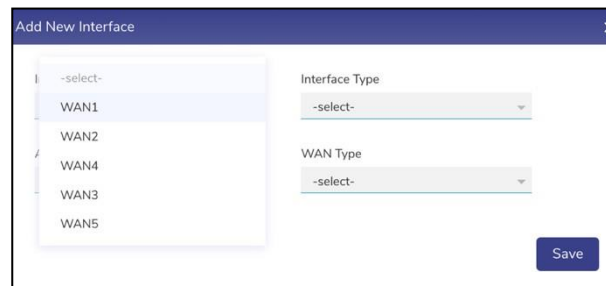
The same "Add New Interface" dialog box as in Figure 3.19, but with the "Interface Name" dropdown menu open. The menu shows a list of options: "-select-", "WAN1", "WAN2", "WAN4", "WAN3", and "WAN5". The "Save" button remains at the bottom right.

Figure 3.20 Interface Name

- Select the **Interface Type** of the new Interface (WAN Sub I/F option is available) See figure below.

Interface Name: -select-

Interface Type: -select- (dropdown open, showing WAN Sub I/F)

Alias: eg. CELL 1

Save

Figure 3.21 Interface Type

- Type the **Alias Name**.

Interface Name: -select-

Interface Type: -select-

Alias: TYPE NAME HERE

WAN Type: -select-

Save

Figure 3.22 Type Alias Name

- Select **WAN Type** of the new Interface from the drop-down menu.

Interface Name: WAN1

Interface Type: WAN Sub I/F

Alias: TYPE NAME HERE

Sub I/F ID: eg. 10

WAN Type: -select- (dropdown open, showing CELL, Wi-Fi, Wired, VSAT-FBB, VSAT, VSAT-LEO)

Save

Figure 3.23 Select WAN Type

- Type the **Sub Interface ID** (Sub I/F ID). See figure below.

Figure 3.24 Sub Interface ID

- Click on **Save**.

The interface is successfully created, and the related interfaces appear together in a common color background, see figure below. The original WAN Interface (WANx) under which the new Interface is created appears disabled and a new native Interface is created with the name WANx_0 (here WANx is WAN2). The new Sub Interface is disabled by default and must be enabled after creation.

Enable / Disable	Interface Name	WAN / LAN Type	Alias	Internet State	ETH State / Reset	IP Address / Subnet Mask	Gateway Address	Probe / Latency (ms)	DNS Servers	Public IP Address / Service Provider	Speed Test	US Internet
<input checked="" type="checkbox"/>	WAN1	Wired	Ethernet	<input checked="" type="checkbox"/>	UP	192.168.112.20/24	192.168.112.1	54.320	8.8.8.8	99.76 24.203 / AT&T Internet Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2	CELL	Cell 1	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2_0	CELL	Cell 1	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2_10	VSAT	VSAT2	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN3	VSAT	VSAT 1	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN4	CELL	Cell 2	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN5	VSAT-FBB	VSAT 2	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	LAN	LAN Trunk	LAN	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	FRHIGHT	---	MGMT	<input checked="" type="checkbox"/>	UP	10.255.240.1/28	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	VSATMIGHT	---	VSAT M...	<input checked="" type="checkbox"/>	Down	---	---	<input checked="" type="checkbox"/>	---	---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 3.25 Configuration Wizard – Sub Interface Created

- Uncheck the All Interfaces check box to view only enabled interfaces. The new Interface creation is complete.

Enable / Disable	Interface Name	WAN / LAN Type	Alias	Internet State	Eth State / Reset	IP Address / Subnet Mask	Gateway Address	Probe / Latency (ms)	DNS Servers	Public IP Address / Service Provider	Speed Test	US Internet
<input checked="" type="checkbox"/>	WAN1	Wired	Ethernet	UP	1000Mbps Full	192.168.112.20/24	192.168.112.1	53.989	8.8.8.8	99.76.24.203 / AT&T Internet Services	Speed Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2_0	CELL	Cell 1	Down	--	--	--	--	--	--	Speed Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2_10	VSAT	VSAT2	Down	--	--	--	--	--	--	Speed Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN2	VSAT	VSAT 1	Down	--	--	--	--	--	--	Speed Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN4	CELL	Cell 2	Down	--	--	--	--	--	--	Speed Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WAN5	VSAT-FBB	VSAT 2	Down	--	--	--	--	--	--	Speed Test	<input checked="" type="checkbox"/>

Figure 3.26 Configuration Wizard – View Enabled Interfaces

Fields	Description	Configuration
Interface Name Hyperlinks	<p>User can configure the static IP address of an Interface as theStatic IP has advantages and the following are a few advantages.</p> <ul style="list-style-type: none"> • Easy to manage with DNS. • It would be easier to work remotely through a VPN or other remote services using the Interface. • It is reliable to access the geolocation-based services using the Interface. • It is reliable for audio and video communications through VoIP using the Interface. 	<p>To configure the static IP of an Interface, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click an Interface. The WAN Configuration pop-up window appears. • For Ethernet/Hardline, see Figure 3.27 Ethernet/ Hardline For CELL configuration, see Figure 3.28 CELL Configuration. For VSAT, see Figure 3.29 VSAT Configuration. • Click Yes in the Configure Static IP field. • Enter the IP address and subnet mask number in the IP Address/Subnet Mask field.

		<ul style="list-style-type: none"> • Enter the gateway address in the Gateway Address field. • Click Save.
--	--	---

Table 3-4 Interface Name Hyperlinks

Ethernet/Hardline Configuration

Configure Static IP

Yes

No

IP Address/Subnet Mask

Gateway Address

Save

Figure 3.27 Ethernet/ Hardline

Cell 1 Static IP Configuration

Configure Static IP

Yes

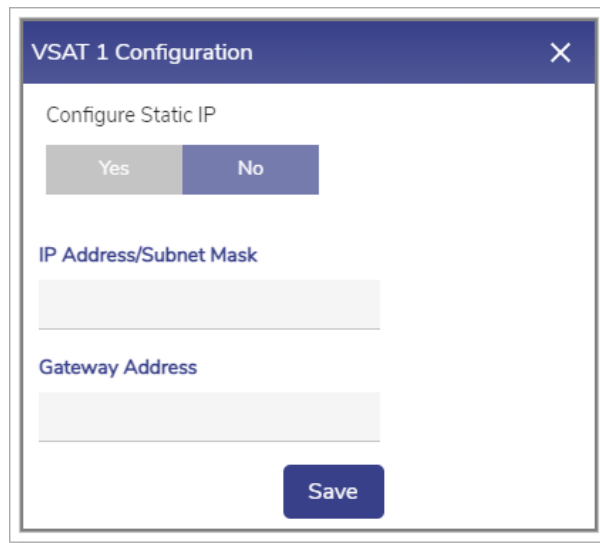
No

IP Address/Subnet Mask

Gateway Address

Save

Figure 3.28 CELL Configuration



The image shows a software dialog box titled "VSAT 1 Configuration" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Configure Static IP" with two buttons: "Yes" and "No". The "No" button is highlighted in blue. Below this, there are two text input fields. The first is labeled "IP Address/Subnet Mask" and the second is labeled "Gateway Address". At the bottom right of the dialog is a blue "Save" button.

Figure 3.29 VSAT Configuration

Field	Description	Configuration
WAN/LAN Type	This field shows the type of the interface.	<p>If the Interface type is. WAN, then this field can be one of:</p> <ul style="list-style-type: none"> • Cell • Wi-Fi • Wired • VSAT • VSAT-LEO (Starlink) • VSAT-FBB <p>If Interface Type is 'LAN', then, this field can be one of:</p> <ul style="list-style-type: none"> • LAN Trunk • LAN Access. <p>If Interface Type is VSAT Management, then this field is Blank.</p>

Table 3-5 LAN/WAN Type




Field	Description	Configuration
Alias	User can give an alias name to the entire Interface.	<p>To configure the alias name, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  next to the Interface. Enter a unique alias name of user choice. Click . <ol style="list-style-type: none"> Alias name of the WAN is saved. <p>Or,</p> <ol style="list-style-type: none"> To exit without giving an alias name, click .

Table 3-6 Alias

Fields	Description	Configuration
Internet State	<p>This indicates the status of the Interface. Following are the statuses of the Interface.</p> <ul style="list-style-type: none"> Up. This indicates that internet connectivity is available on the site. Down. This indicates that internet connectivity is not available on the site. 	N/A

Table 3-7 Internet State






Fields	Description	Configuration
Eth State/Reset	This indicates the maximum capacity of the respective Ethernet cable connected to the server.	<p>To view the Eth state details, hover on Info icon  .</p> <p>This shows the Eth state details.</p> <p> State Change Count indicates the number of times the Internet State of the Interface changed since the last reboot.</p> <p>Last State Change Timestamp</p> <p>See Figure 3.30 Eth State Hover.</p>
		<p>The info icon is blue  when the Internet State is consistent for last 15 minutes and amber  when Internet State changes in last 15 minutes. (Down to UP or UP to Down).</p>
		<p>To reset Interface</p> <p>Click on the reset icon  This bounces the Interface if it is a physical interface. If it is a sub interface, it restarts the DHCP client.</p>

Table 3-8 Eth State/Reset

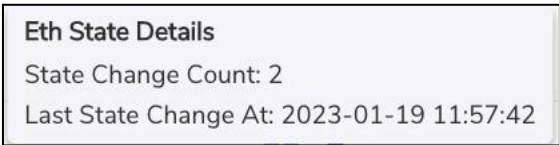




Figure 3.30 Eth State Hover

Fields	Description	Configuration
IP Address/Subnet Mask	This indicates the address of the network, host or device address, and subnet number.	N/A

Table 3-9 IP Address/ Subnet Mask

Fields	Description	Configuration
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.	<p>If WAN Type is CELL, then.</p> <p>To access the Cellular modem to procure details and services (data consumed by the Interface and signal strength etc.) offered by the respective company or vendor, click the IP address link. User will be routed to the URL of the company.</p>
	The boxes connect to the network of the companies or vendors to establish internet connectivity on the vessel.	<p>To procure details and services (data consumed by the CELL (LTE) and signal strength etc.) offered by the respective company or vendor.</p> <ul style="list-style-type: none"> Click  peplink. The Peplink Access Details pop-up window appears, see Figure 3.31 Peplink Access Details. Enter the required details in the respective fields and click Save. <p>The user will be routed to the URL of the company.</p>
	<ul style="list-style-type: none"> HTS services support along with the VSAT (SES/Intelsat). 	<p>If WAN Type is VSAT, then.</p> <ul style="list-style-type: none"> Click  . The VSAT Type pop-up window appears, Figure 3.32 VSAT. <p>If the VSAT modem is provisioned by K4, then</p>

	<ul style="list-style-type: none"> User can switch over from HTS to SES and SES to HTS. 	<ul style="list-style-type: none"> click Yes. The VSAT Type field becomes available. <hr/> <p>Note: By default, No is selected. This indicates that the VSAT is not provisioned by K4.</p> <p>In the VSAT Type list, select one of the available options.</p> <ul style="list-style-type: none"> Global VSAT- Non-K4 VSAT Provider Single Modem on VSAT1. With this option selected, VSAT controller will show up with all the available data. Beam Switch will not be supported with this configuration. K4 Global VSAT- Modem1 (SES) on VSAT1 K4 HTS VSAT- Modem1 (Hispasat) on VSAT1 K4 HTS/Global VSAT- Modem1 (SES) & Modem2 (Hispasat) on VSAT1 <hr/> <p>Note: SES and Hispasat are running two different iDirect platform firmware, hence the need for two modems.</p> <ul style="list-style-type: none"> K4 Global VSAT- Multiple ISPs- Modem1 (SES/Intelsat) on VSAT1 <hr/> <p>Note: SES and Intelsat configurations are saved in the EdgeOS System, and appropriate configuration is loaded on the modem.</p> <ul style="list-style-type: none"> K4 HTS/Global Coverage- Multiple ISPs- Modem1 (SES/Intelsat) and Modem2 (Hispasat) on VSAT1.
--	--	--



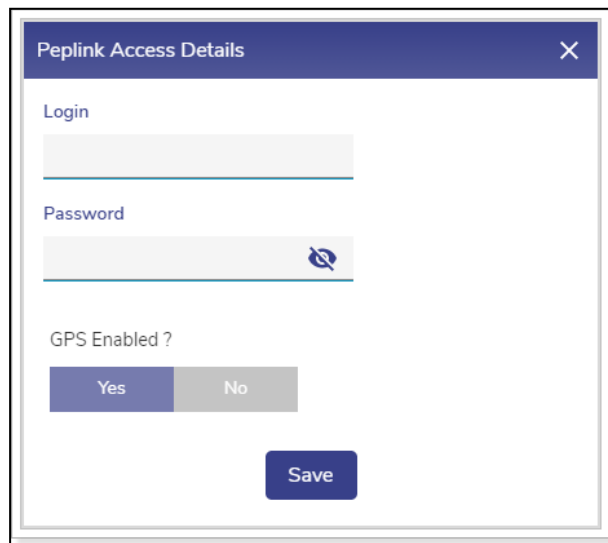
	<p>VSAT LEO (Starlink) service and support</p>	<p>If WAN Type is VSAT-LEO, then</p> <ul style="list-style-type: none"> Click . The VSAT-LEO Type pop-up window appears. <p>If the VSAT-LEO modem is managed by K4, then click Yes. Then Management IP field is editable.</p> <div data-bbox="842 600 1353 622" style="background-color: #008000; height: 10px; margin: 10px 0;"></div> <p>By default, NO is selected. This indicates that the VSAT-LEO is not managed by K4.</p> <p>See Figure 3.34 VSAT-LEO.</p> <p>Click on YES and enter the Management IP of the VSAT LEO Management Interface.</p>
	<p>If the WAN modem is available, then the user can add the WAN modem to the Konnect.</p>	<p>To add the WAN modem to the Konnect, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click . The Add to Konnect pop-up window appears, see Figure 3.35 Add to Konnect. Click Confirm. <p>The WAN modem connects to the Konnect.</p>

Table 3-10 Gateway Address



Peplink Access Details

Login

Password

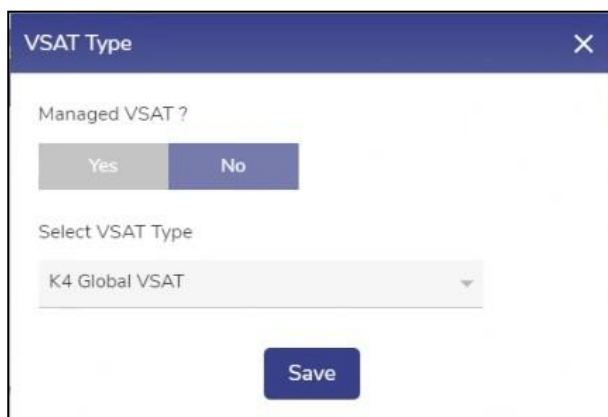
GPS Enabled ?

Yes No

Save

This is a screenshot of a 'Peplink Access Details' pop-up window. It features a dark blue header with the title and a close button. The form contains three main sections: a 'Login' section with a text input field, a 'Password' section with a text input field and a toggle icon, and a 'GPS Enabled ?' section with two radio buttons labeled 'Yes' and 'No'. A 'Save' button is located at the bottom right.

Figure 3.31 Peplink Access Details



VSAT Type

Managed VSAT ?

Yes No

Select VSAT Type

K4 Global VSAT

Save

This is a screenshot of a 'VSAT Type' pop-up window. It has a dark blue header with the title and a close button. The form includes a 'Managed VSAT ?' section with two radio buttons labeled 'Yes' and 'No', a 'Select VSAT Type' section with a dropdown menu currently showing 'K4 Global VSAT', and a 'Save' button at the bottom right.

Figure 3.32 VSAT Type default pop-up

VSAT Type [X]

Managed VSAT ?

Yes No

- Global VSAT
- K4 Global VSAT
- K4 HTS VSAT
- K4 HTS / Global VSAT
- K4 Global VSAT - Multiple ISPs
- K4 HTS / Global Coverage - Multiple ISPs

Figure 3.33 VSAT Type Selection

VSAT-LEO Type [X]

Managed VSAT-LEO ?

Yes No

Management IP

eg. 192.168.100.1

Save



Figure 3.34 VSAT-LEO

Add to Konnect [X]

Are you sure you want to add WAN Modem to Konnect?

Confirm

Figure 3.35 Add to Konnect

Fields	Description	Configuration
Probe/Latency (msec)	<p>Latency indicates the delay between the action and response in milliseconds.</p> <p>Latency is available for the Interface whose status is Up.</p> <p>The user can configure the probe settings for the Interface.</p>	<p>Each WAN type has a specific default probe setting. This is however configurable.</p> <p>To configure the probe settings, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  next to the Interface. The Configure Probe Settings pop-up window appears, see Figure 3.37 Configure Probe. Click a probing profile in the Probing Profiles field. <p>To understand the various probing profile, hover on the  icon. See Figure 3.36 Probe Profiles Information.</p> <p>To disable the probes, select the Always Up profile of the profile.</p> <p>Disabling the Interface probe will expose the following threats.</p> <ul style="list-style-type: none"> Reduce the probe rate to a few times an hour. The speed test will be disabled. It will also impact the Interface usage and reliability. <p>Therefore, it is highly recommended not to disable the probe. However,</p>

		<p>the Interface can be disabled for high costs low priority links.</p> <p>Configure the following probe settings in the Probe Settings field.</p> <ul style="list-style-type: none"> • 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. <p>If the user selects 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.</p> <p>To define the probe frequency, the user must select the Custom Probing profile of the probe and enter the probe frequency within the range of 1 to 3600.</p> <ul style="list-style-type: none"> • Link Up Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the Interface is up. <p>If the user selects the Default Probing, Slow Probing, and Fast Probing profile of the probe, then the probe</p>
--	--	--


		<p>frequency, link up down values will become available.</p> <hr/> <p>Note: For VSAT FBB WAN type, the default Probe Profile is High Cost.</p> <p>To define the link up counter, the user must select the Custom Probing profile of the probe and enter the linkup counts within range of 1 to 100.</p> <ul style="list-style-type: none"> Link Down Counter. Enter the count of the probe to be observed at the configured probe frequency to deem that the Interface is down. <p>If the user selects 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.</p> <p>To define the probe frequency, the user must select the Custom Probing profile of the probe and enter the linkdown counts within the range of 1 to 100.</p> <ul style="list-style-type: none"> Click Save.
	User can view the Probe/Latency chart of the Interface.	<p>To view the Probe/Latency chart of the Interface, click  corresponding to the Interface. The Link Status section appears on the Performance Chart.</p>

Table 3-11 Probe/Latency (msec)

Default Probing	–	Default settings for link health check.
Slow Probing	–	The system will check the link health slowly, thus will identify the link is down/up slowly (hourly).
Fast Probing	–	The system will check the link health rapidly, thus will identify the link is down/up quickly (few seconds).
Custom Probing	–	Ability to set the values as needed.
High Cost	–	The system will view the link as always being up and available (No Probing will be done). Only konnect traffic will be allowed as operational traffic.
Always Up	–	The system will view the link as always being up and available (No Probing will be done).

Figure 3.36 Probe Profiles Information

Figure 3.37 Configure Probe

Fields	Description	Configuration
DNS Server	<p>This indicates the initial DNS used by the device to convert the name of the host to an IP address.</p> <p>However, a maximum of three DNSs' can be configured.</p>	N/A

Table 3-12 DNS Server

Fields	Description	Configuration
Public IP Address/Service Provider	<p>Public IP Address 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).</p> <p>Service Provider indicates the name of ISP.</p>	<p>This information is available once speed test is run successfully on this interface, either manually or periodically.</p> <p>For speed test, see Table 3-14 Speed Test.</p>

Table 3-13 Public IP Address/Service Provider

Fields	Description	Configuration
Speed Test	The user can measure the performance of a specificInterface in real-time.	<p>Click Speed Test. The Speed Test Results pop-up window appears, see Figure 3.30 Speed Test.</p> <p>The speed test result includes the upload and download speed in Mbps and time stamp i.e., date and time when the speed test was performed.</p> <p>The speed test can be performed for the Interface whose state is Up.</p> <p>Default Speed Test settings per WAN type are:</p> <ul style="list-style-type: none"> • CELL– Enabled, every 24 Hours • VSAT- Enabled, every 6 Hours • VSAT-LEO – Enabled, every 1 Hour • VSAT-FBB - Disabled


		<ul style="list-style-type: none">• Wired – Enabled, every 1 Hour• Wi-Fi – Enabled, every 1 Hour <p>To configure the periodic speed test, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none">• Click  next to the Interface. The Interface Speed Test pop-up window appears, see Figure 3.38 Speed Test.• Click Yes under the Enable periodic Speed Tests. <p>To select a different periodicity value (other than default), Click the Speed Test Periodicity list, select the desired value, see Figure 3.39 Speed Test List. Click Save.</p>
--	--	---

Table 3-14 Speed Test

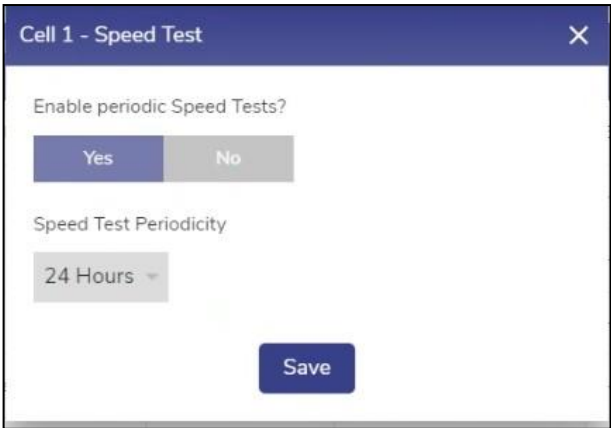


Figure 3.38 Speed Test

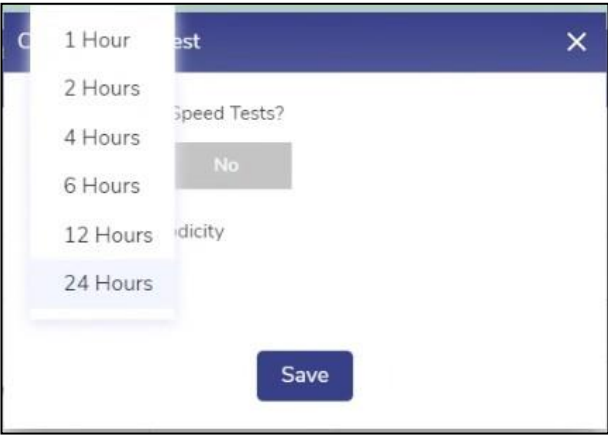


Figure 3.39 Speed Test List

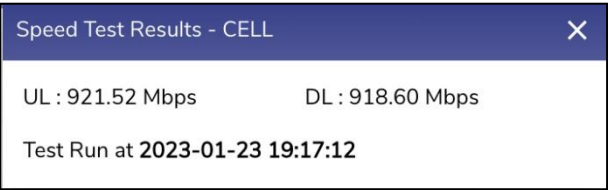


Figure 3.30 Speed Test





Fields	Description	Configuration
US Internet	To allow access to the US internet.	Use the toggle  to turn ON-OFF US Internet.

Table 3-15 US Internet

3.2 Access Network


The user can configure the following three types of networks supported.

-  Connected Networks
-  Managed Connected Networks (Traditional VLAN-s)
-  Managed Routed Networks

3.2.1 Adding New Connected Network

To configure the connected network, perform the following steps.

Steps

- Click  on the **Interfaces** page or click **Access Networks**. The **Access Networks** page appears, see below.

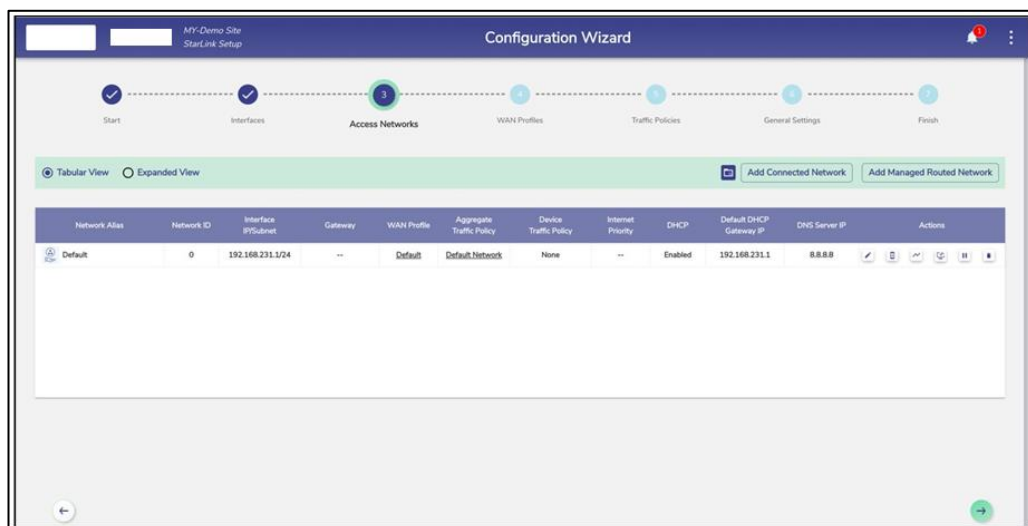


Figure 3.40 Access Networks

Initially, the **Default** network is available. The user can configure multiple networks. Once, the networks are configured, the networks become available on the **Access Networks** page.

This section has two view, Tabular View, and Expanded View. The default view is Tabular View. Click **Expanded View** to see the details of the networks in expanded form, see below.

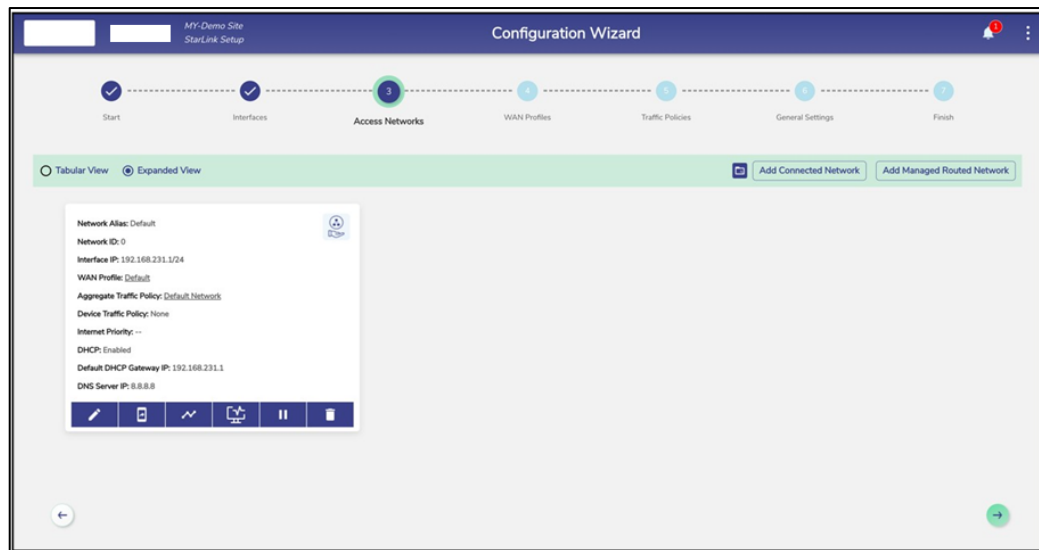


Figure 3.41 Expanded View

To add a Connected Access Network, perform the following steps.

Steps

- Click **Add Connected Network** button present on the top right of the screen. The **Add Connected Network** page appears, see below.

By default, Connected Networks are unmanaged, i.e., 'Managed Connected Network?' is set to 'No'. See **Figure 3.42 Add Connected Network**. To create a Managed Connected Network, set 'Managed Connected Network?' to **Yes**. See **Figure 3.43 Add Managed Connected Network**.

MY-DemoSite
Starlink Setup

Configuration Wizard

29

Start

Interfaces

Access Networks

WAN Profiles

Traffic Policies

General Settings

Finish

Add Connected Network

Network ID

eg. 100

Network Alias

eg. Owner

Interface IP

eg. 192.168.100.1/24

Managed Connected Network?

☒ No ☐ Yes

Captive Access Network?

☒ No ☐ Yes

Save

Figure 3.42 Add Connected Network

MY-DemoSite
Starlink Setup

Configuration Wizard

Start

Interfaces

Access Networks

WAN Profiles

Traffic Policies

General Settings

Finish

Add Connected Network

Network ID

eg. 100

Network Alias

eg. Owner

Interface IP

eg. 192.168.100.1/24

Managed Connected Network?

☐ No ☒ Yes

Captive Access Network?

☐ No ☒ Yes

WAN Profile and Traffic Policies

WAN Profile

--select--

Aggregate Traffic Policy

--select--

Device Traffic Policy

None

Internet Priority

Standard

Connect VPN

None

DHCP Settings

DHCP

Enabled

Default DHCP Gateway IP

eg. 192.168.100.1

DNS Server IP

eg. 192.168.30.1

IP Pools

eg. 192.168.100.2 - 192.168.100.100, 192.168.100.101 - 192.168.100.150

IP Reservations

New IP Reservation

Bulk Upload

Select devices from the table and assign a Traffic Policy

0 Device selected

Select Traffic Policy

✓


	MAC Address	IP Address	Name	Traffic Policy	Actions
--	-------------	------------	------	----------------	---------

Save


Figure 3.43 Add Managed Connected Network

Note: The user can configure multiple local networks to be used based on the hierarchy. They 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.










- To enter data in the respective fields, see table below.




Fields	Description
Network ID	<p>Enter a unique numeric ID from 2 to 4090.</p> <p>For details about the network ID, click  next to the network ID.</p> <hr/> <p>Network ID is known as a VLAN ID. Once the network ID is configured, user cannot modify or update the VLAN ID or network ID in the future.</p>
Network Alias	Enter a unique alias of the network.
Interface IP	Enter an interface IP address and subnet mask.
Managed Connected Network	<p>Click one of the following options.</p> <ul style="list-style-type: none"> • No. This indicates that by default, unmanaged connected network is configured. • Yes. To manage and configure the connected network, click Yes. The network configuration section becomes available, see Figure 3.44 Configure Managed Connected Network. <hr/> <p>The Managed Connected Network is the traditional VLANs’.</p>
Captive Access Network	<p>Captive Portal allows for each crew member/client to have a provisioned account with an associated Service Plan. The Account’s “service plan” is customized to match corporate policy (Quota, Duration, Traffic Policy – e.g., 10GB/month with defined traffic policies).</p> <p>Click one of the following options.</p> <hr/> <p>No, Default option if Captive functionality is disabled on the Access Network.</p>

	Yes. To enable Captive functionality on the Access Network.
WAN Profile and Traffic Policies	
WAN Profile	<p>Select a WAN Profile.</p> <p>A single WAN Profile, I.e., Default Profile will be created in the system after the EdgeOS System installation, and this profile will be assigned by default to any newly created Access Network. However, user can configure the distinct WAN profiles and assign to the Network. For details about configuring the WAN profiles, see 3.3 WAN Profiles.</p>
Aggregate Traffic Policy	<p>Select a Network Traffic Policy.</p> <p>A single Traffic Policy, I.e., Default Network will be created in the system after the EdgeOS System installation, and this policy will be assigned by default to any newly created Access Network. However, user can configure the distinct policies and assign to the Network. For details about configuring the network traffic policies, see 3.4 Traffic Policies.</p>
Device Traffic Policy	<p>Select a Device Traffic Policy.</p> <p>Initially, on Network creation, no Device Traffic Policy is assigned to the network. However, user can configure the distinct device traffic policy and assign to the network. For details about configuring the device traffic policies, see 3.5.1 Device Traffic Policies.</p> <p>The user can assign the traffic policy to a device from also General Settings For details, see 3.5 General Settings However, the traffic policy assigned to a device from this step will override the traffic policy of that device.</p> <div>Shaping Policy as per Device Policy, Application Policy same as Aggregate Policy for Network</div>
Konnect VPN	Select a configured Konnect VPN.

	<ul style="list-style-type: none"> To route the Access Network traffic through the VPN, edit the Access Network configuration to pick the configured VPN end point to route. This allows the EdgeOS System to VPN access networks to a Konnect VPN Server; this is most utilized between EdgeOS Systems. For details of VPN Configuration, see 3.5.6 Konnect VPN.
Internet Priority	<p>Select an Internet Priority. For details, click  next to the Internet Priority, see below.</p> <div data-bbox="652 808 1256 1108"> <p>Default – No Internet Priority</p> <p>High – Highest Priority</p> <p>Standard – Standard Priority</p> <p>Low – Lowest Priority</p> <p>Realtime – Voice/Video Communication</p> <p>Realtime Priority is suited for Apps such as Zoom and Teams, and is limited to a few Mbps.</p> </div>
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	<p>The default IP address becomes available.</p> <p>User can assign a new IP address. For this, click and delete the IP address and then assign a new IP address.</p>
DNS Server IP	<p>The default IP address becomes available.</p> <p>User can assign a new IP address. For this, click and delete the IP address and then assign a new IP address. They can assign a maximum of three DNS IP addresses.</p> <p>To configure the DNS proxy, perform the following steps.</p> <p>Steps</p>

	<ul style="list-style-type: none"> • Enter the DHCP Gateway IP address in the DNS Server IP field under the DHCP Settings section. • Click Save. The network is updated, and a successful message is displayed, see Figure 3.45 Network Updated Successfully. • Click OK. • The status In Use is displayed. • By default, the status Not In Use is displayed.
	<p>To remove the DNS proxy, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Delete the DHCP Gateway IP address in the DNS Server IP field under the DHCP Settings section. • Or, • Enter 8.8.8.8 in the DNS Server IP field under the DHCP Settings section. • Click Save. The network is updated, and a successful message is displayed, see Figure 3.45 Network Updated Successfully. • Click OK. • The status Not in Use is displayed, see Figure 3.46 Configure DNS Policy (Not in Use).
IP Pools	<p>The default sequential range of the IP addresses becomes available.</p> <p>User 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.</p> <p>User can assign multiple sequential IP address range excluding the specific IP addresses of that range. This is an example.</p> <p>192.168.10.2-192.168.10.100, 192.168.10.151-192.168.10.200, 192.168.10.220-192.168.10.254</p> <p>The following IP addresses will not be assigned to the device in the network.</p> <ul style="list-style-type: none"> • 192.168.10.101-192.168.10.150

	<ul style="list-style-type: none"> 192.168.10.2-201.168.10.219 <p>DHCP will assign the IP address to a device on the specified network based on the IP address range.</p>										
IP Reservations											
New IP Reservation	<p>To reserve an IP address for a device, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click New IP Reservation. <p>Configure the MAC Address, IP Address, Name, Traffic Policy, and Actions fields. •</p> <table> <tr> <td>MAC Address</td><td>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> <p>Click a traffic policy to be assigned to the device.</p> <p></p> <p>Inherit indicates that the device will inherit the device policy of the network.</p> </td></tr> <tr> <td>Actions</td><td> <p>To save the IP reservation configuration, click .</p> <p>Or,</p> <p>To cancel the IP reservation configuration, click .</p> </td></tr> </table>	MAC Address	Enter the MAC address of a device.	IP Address	Enter IP address from the sequential IP address range specified in the IP Pools field.	Name	Enter a name for the device.	Traffic Policy	<p>Click a traffic policy to be assigned to the device.</p> <p></p> <p>Inherit indicates that the device will inherit the device policy of the network.</p>	Actions	<p>To save the IP reservation configuration, click .</p> <p>Or,</p> <p>To cancel the IP reservation configuration, click .</p>
MAC Address	Enter the MAC address of a device.										
IP Address	Enter IP address from the sequential IP address range specified in the IP Pools field.										
Name	Enter a name for the device.										
Traffic Policy	<p>Click a traffic policy to be assigned to the device.</p> <p></p> <p>Inherit indicates that the device will inherit the device policy of the network.</p>										
Actions	<p>To save the IP reservation configuration, click .</p> <p>Or,</p> <p>To cancel the IP reservation configuration, click .</p>										
Bulk Upload	<p>To upload details of the IP reservation, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click Bulk Upload. The Bulk upload IP Reservations pop-up window appears, see Figure 3.47 Bulk Upload. 										

	<p>To download the bulk IP reservation template, click Download Reservations. The IP reservation template downloads in CSV format, see Figure 3.48 IP Reservations Template in CSV Format.</p> <p>Fill in the required details in the file. For an example, see Figure 3.49 Example of IP Reservations Template in CSV Format.</p> <div data-bbox="517 600 1428 616" style="background-color: #008000; height: 10px; margin: 10px 0;"></div> <p>The first row is referred to as the header row.</p> <p>Save the file.</p> <ul style="list-style-type: none"> Click Upload Reservations and browse the IP reservations CSV file. Click Open. The IP reservations are displayed under the IP Reservations section, see Figure 3.50 IP Reservations Details. Click Save.
	<p>User can modify the details of the IP reservation.</p> <p>To modify the details of the IP reservation, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click . 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. The MAC Address field is read-only. Click . <p>Or,</p> <p>To cancel the IP reservation, click .</p> <ul style="list-style-type: none"> Click Save. <p>Details of the IP reservation are modified.</p>
	<p>To delete the details of the IP reservation, perform the following steps.</p> <p>Steps</p>


-
- Click . The IP reservation details are deleted.
 - Click **Save**.

Table 3-16 Connected Network Information

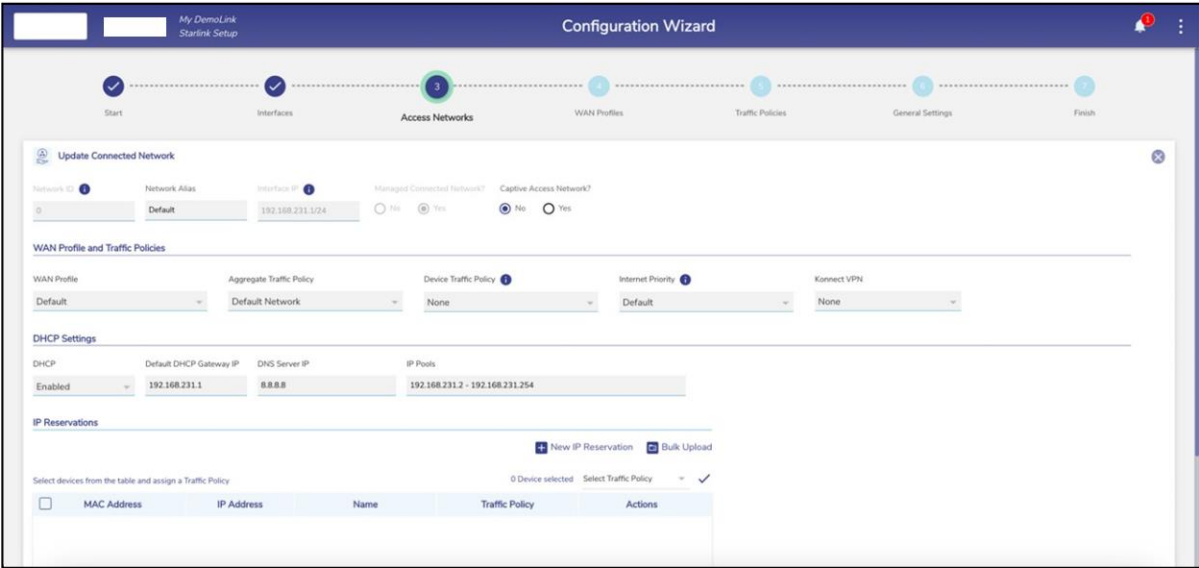


Figure 3.44 Configure Managed Connected Network

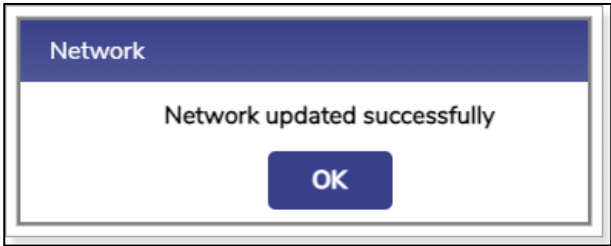


Figure 3.45 Network Updated Successfully

Configuration Wizard

Start Interfaces Access Networks WAN Profiles Traffic Policies **General Settings** Finish

+ Device Traffic Policies

+ Static Routes Configuration

+ Firewall Settings

- DNS Proxy Settings

DNS Server Status: **Not in Use**

Domain/Host Mapping

Enter one IP Address/Domain per line

For eg: IP/URL/Domain Name

You can enter the Host name entries OR Upload list of entries in CSV format

Cancel Save

DNS Forwarder

Enter one DNS Forwarder per line

8.8.8.8
8.8.4.4

Cancel Save

DNS Cache

Enable Disable

Enable/Disable of DNS Cache will modify the storage of DNS Lookups.

Figure 3.46 Configure DNS Policy (Not in Use)

Bulk upload IP Reservations

Upload Reservations

Download Reservations

Figure 3.47 Bulk Upload

DHCP_Reservations - Notepad

File Edit Format View Help

"DEVICE MAC","DEVICE IP","DEVICE Name"

Figure 3.48 IP Reservations Template in CSV Format

DHCP_Reservations - Notepad

File Edit Format View Help

"DEVICE MAC","DEVICE IP","DEVICE Name"

"19:A5:A6:73:BA:48","192.168.231.23","Karolann"

"FC:76:63:C3:69:06","192.168.231.45","Neva"

"E1:F1:20:5F:AA:CA","192.168.231.77","Jackie"

"88:D8:E7:96:F3:90","192.168.231.88","Lucio"

Figure 3.49 Example of IP Reservations Template in CSV Format

Select devices from the table and assign a Traffic Policy

0 Device selected Select Traffic Policy  

<input type="checkbox"/>	MAC Address	IP Address	Name	Traffic Policy	Actions
<input type="checkbox"/>	00:1B:44:11:3A:B7	192.168.231.23	Karolann	Inherit	 

Figure 3.50 IP Reservations Details

3.2.2 Adding a Managed Routed Network

To add a Managed Routed Network, perform the following steps.

Steps

The pre-requisite to add a Managed Routed Network is to first create an Unmanaged Connected Network. See [figure 2.3.1](#).

- Click the **Add Managed Routed Network** button. The **Add Managed Routed Network** page appears, see figure below.

The screenshot shows the 'Add Connected Network' configuration page in a 'Configuration Wizard'. The wizard progress bar indicates steps: Start, Interfaces, Access Networks (current), WAN Profiles, Traffic Policies, General Settings, and Finish. The 'Add Connected Network' section includes fields for Network ID, Network Alias (Default), Interface IP (192.168.231.1/24), Managed Connected Network? (radio buttons for No/Yes), and Captive Access Network? (radio buttons for No/Yes). Below this is the 'WAN Profile and Traffic Policies' section with dropdowns for WAN Profile (Default), Aggregate Traffic Policy (Default Network), Device Traffic Policy (None), Internet Priority (Default), and Connect VPN (None). The 'DHCP Settings' section includes a DHCP status dropdown (Enabled), Default DHCP Gateway IP (192.168.231.1), DNS Server IP (8.8.8.8), and IP Pools (192.168.231.2 - 192.168.231.254). The 'IP Reservations' section has buttons for 'New IP Reservation' and 'Bulk Upload', and a table header for selecting devices from a table and assigning a Traffic Policy.

Figure 3.51 Add Managed Routed Network

- To enter data in the respective fields, see table below.

Fields	Description
Network Alias	Enter a unique alias of the network.
Subnet	Enter the subnet based on the interface IP address and mask that was configured while configuring the connected network.

Gateway	<p>Enter the IP address of the device managing the communication with the external network.</p> <p>User must assign the IP address based on the interface IP address that was configured while configuring the connected network.</p>
Captive Access Network	<p>Captive Portal allows for each crew member/client to have a provisioned account with an associated Service Plan. The Account's "service plan" is customized to match corporate policy (Quota, Duration, Traffic Policy – e.g., 10GB/month with defined traffic policies).</p> <p>Click one of the following options.</p> <p>No, Default option if Captive functionality is disabled on the Access Network.</p> <p>Yes. To enable Captive functionality on the Access Network.</p>
WAN Profile and Traffic Policies	
Same as corresponding fields in Table 3-16 Connected Network Information .	
DHCP Settings	
Same as corresponding fields in Table 3-16 Connected Network Information .	
IP Reservations	
For details of each section, see Table 3-16 Connected Network Information .	

Table 3-17 Managed Routed Network Information

- The Connected Network and associated Managed Routed Networks are grouped and appear in the same background color in the Access Networks table. See example table below.

MY Demo Site
StarLink Setup

Configuration Wizard

Start Interfaces **Access Networks** WAN Profiles Traffic Policies General Settings Finish

Tabular View Expanded View

Add Connected Network Add Managed Routed Network


Network Alias	Network ID	Interface IP/Subnet	Gateway	WAN Profile	Aggregate Traffic Policy	Device Traffic Policy	Internet Priority	DHCP	Default DHCP Gateway IP	DNS Server IP	Actions
Default	0	192.168.231.1/24	---	Default	Default Network	None	---	Enabled	192.168.231.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network10	10	192.168.10.1/24	---	starlink_wan_profile_8	Default Network	None	Standard	Enabled	192.168.10.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network20	20	192.168.20.1/24	---	starlink_ordinary_bonded	Default Network	None	Standard	Enabled	192.168.20.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network30	30	192.168.30.1/24	---	wan_profile	Default Network	None	Standard	Enabled	192.168.30.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network40	40	192.168.40.1/24	---	Default	Default Network	None	Standard	Enabled	192.168.40.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network50	50	192.168.50.1/24	---	---	---	---	---	Disabled	---	---	[Edit] [Delete] [Refresh] [Reset] [Help]
Subnet511	---	10.30.1.1/24	192.168.50.4	starlink_wan_profile_8	Default Network	None	Standard	Enabled	10.30.1.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Subnet512	---	10.30.2.1/24	192.168.50.4	starlink_ordinary_bonded	Default Network	None	Standard	Enabled	10.30.2.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Network60	60	192.168.60.1/24	---	---	---	---	---	Disabled	---	---	[Edit] [Delete] [Refresh] [Reset] [Help]
Subnet611	---	10.50.0.1/24	192.168.60.2	Default	Default Network	None	Standard	Enabled	10.50.0.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Subnet612	---	10.50.1.1/24	192.168.60.3	wan_profile	Default Network	None	Standard	Enabled	10.50.1.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]
Subnet613	---	10.50.2.1/24	192.168.60.3	wan_profile	Default Network	None	Standard	Enabled	10.50.2.1	8.8.8.8	[Edit] [Delete] [Refresh] [Reset] [Help]

Figure 3.52 Grouped Networks

3.2.3 Modifying Network

To modify a network, perform the following steps.

Steps

- Click  next to the network under the **Action** section on the **Access Networks** page. The **Updated Connected Network** page appears, see **Figure 3.53 Update Connected Network**. To enter data in the respective fields, see **Table 3-16 Connected Network Information**.

Note: All fields except Network ID, Interface IP, and Managed Connected Network? are editable.

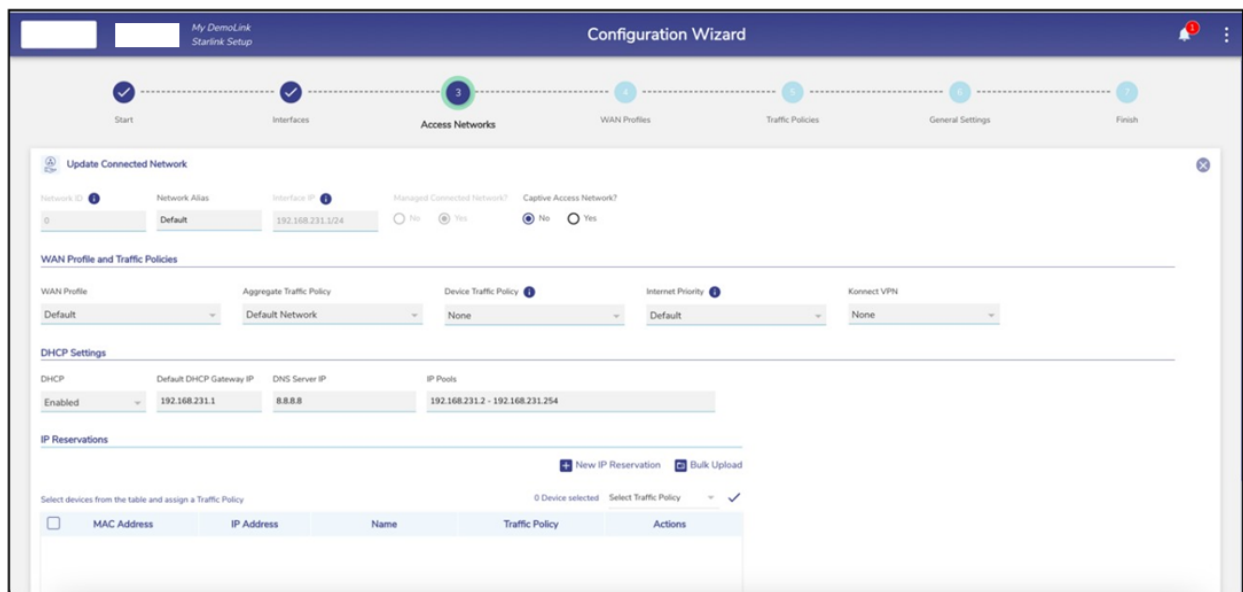



Figure 3.53 Update Connected Network

- Click **Save**.

3.2.4 Modifying Device Profile

To modify the device profile, perform the following steps.

Steps

- Click  next to the network under the **Action** section on the **Access Networks** page. The **Device Profile** page appears, see figure below.

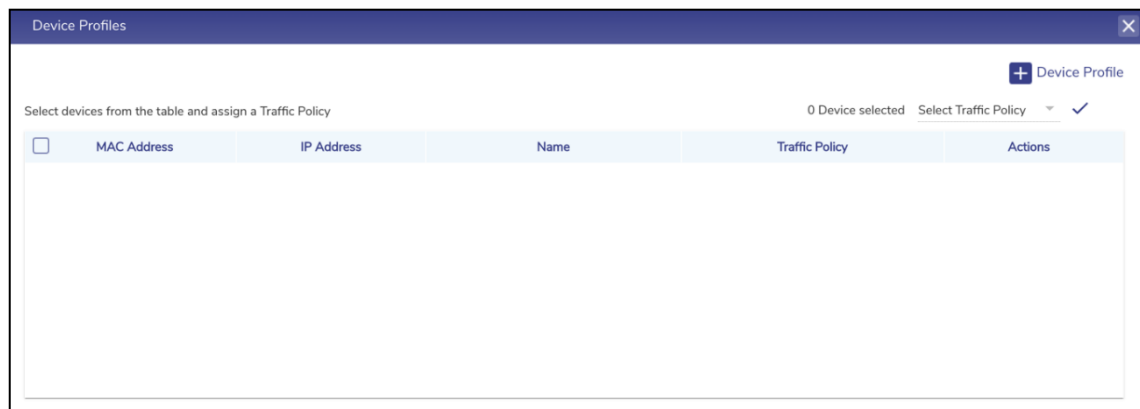


Figure 3.54 Device Profile

- Click **Device Profile** on top right to add a new device profile.
- To enter data in the respective fields, see **Table 3-16 Connected Network Information**.
- Click **Save**.

The user cannot modify the device profiles of the connected network.

3.2.5 Viewing Network Usage Data

To view network usage data, perform the following steps.

Steps

- Click  next to the network under the **Action** section on the **Access Networks** page. The **Network Usage** page appears, see figure below.

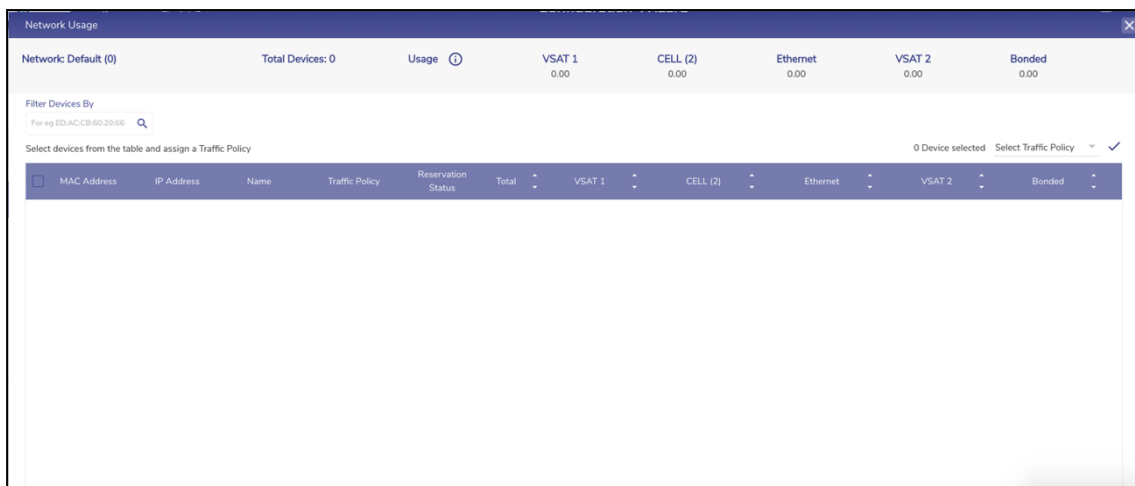








Figure 3.55 Network Usage

- For details about the fields, see table below.

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 3.56 Quota Details .
VSAT	This indicates the total data consumed by the VSAT.

VSAT-LEO	This indicates the total data consumed by the Starlink.
VSAT-FBB	This indicates the total data consumed by the L-Band.
CELL (LTE)	This indicates the total data consumed by the CELL (LTE).
Ext5G	This indicates the total data consumed by Ext5G.
Wi-Fi	This indicates the total data consumed by the Wi-Fi.
Ethernet	This indicates the total data consumed by the ETHERNET.
Bonded	This indicates the total data consumed by the Bonded.
Filter Devices By	Enter the MAC address of the specific device. Details about the device become available.
MAC Address	<p>This indicates the MAC address of the device connected to the network.</p> <p>To pause the device, click . The Pause Device Profile confirmation message pop-up window appears, see Figure 3.57 Pause Device Confirmation Message.</p> <p>Click Pause. The  (resume button) becomes available and the row of the device is highlighted by a color.</p> <p>Or,</p> <p>To resume the device, click . The Resume Device Profile confirmation message pop-up window appears, see Figure 3.58 Resume Device Confirmation Message.</p> <p>Click Resume.</p>
IP Address	This indicates the IP address assigned to the device.
Name	<p>This indicates the alias name of the device.</p> <p>To modify the alias name, click  and modify the alias name.</p>

Traffic Policy	<p>This indicates the traffic policy assigned to the device.</p> <p>To modify the traffic policy, click  and modify the traffic policy. For details, see 3.4 Traffic Policies.</p> <p>To assign the traffic policy to multiple devices, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Select the check box next to the device. The count of the devices selected is displayed in the Devices Selected field. • Click Select Traffic Policy. • Click the traffic policy to be assigned the devices selected. <p>Or,</p> <p>To assign the traffic policy to the devices in bulk, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Select the check box next to the MAC Address field. The count of the devices selected is displayed in the Devices Selected field. • Click Select Traffic Policy. • Click the traffic policy to be assigned the devices selected.
Reservation Status	<p>This indicates that whether the IP address assigned to the device is reserved.</p> <p>To reserve the IP address of the device, select the corresponding check box.</p> <p>Or,</p> <p>To un-reserve the IP address of the device, clear the check box.</p>
Total	<p>This indicates the sum of the data consumed by the device on the following WAN links.</p> <ul style="list-style-type: none"> • VSAT • VSAT-LEO • VSAT-FBB

	<ul style="list-style-type: none"> • CELL (LTE) • Ext5G • Wi-Fi • Ethernet • Bonded
VSAT	This indicates the quantum of the data consumed by the device on the VSAT.
CELL (LTE)	This indicates the quantum of the data consumed by the device on the CELL (LTE).
Wi-Fi	This indicates the quantum of the data consumed by the device connected through Wi-Fi.
Ethernet	This indicates the quantum of the data consumed by the device on the Ethernet.
Bonded	This indicates the quantum of the data consumed by the device on the Bonded.

Table 3-18 Network Usage

Remaining	VSAT	CELL	Ethernet	Bonded
UL Quota	Unlimited	Unlimited	Unlimited	Unlimited
DL Quota	Unlimited	Unlimited	Unlimited	Unlimited

Figure 3.56 Quota Details

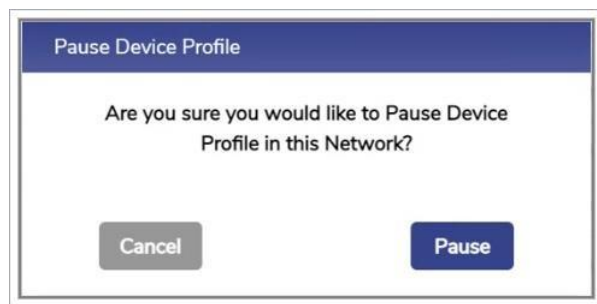


Figure 3.57 Pause Device Confirmation Message



Figure 3.58 Resume Device Confirmation Message

3.2.6 Configuring Captive Access Network

Captive Portal allows for each crew member/client to have a provisioned account with an associated Service Plan. The Account's "service plan" is customized to match corporate policy (Quota, Duration, Traffic Policy – e.g., 10GB/month with defined traffic policies).

To configure an Access Network as Captive, perform the following steps.

Steps

- Click icon of the Access Network that the user wants to make Captive.
- Set the 'Captive Access Network?' field to Yes to enable the Captive Access Network, see [Figure 3.59 Captive Access Network](#).
- Set the Aggregate Network Policy such that all applications but *.k4mobility.com is denied, see [Figure 3.60 Aggregate Network Policy](#).
- Set the Device Traffic Policy to None.
- Click **Save**. The Captive Access Network will be created. This will show up

with  icon next to it, see [Figure 3.61 Captive Access Network](#).

- Create one or more Device Traffic Policies in the Traffic Policy Section which will apply to devices connecting via Captive Access Network, see [Figure 3.62 Device Traffic Policy](#). These policies will be associated with the plans assigned to users of these devices.

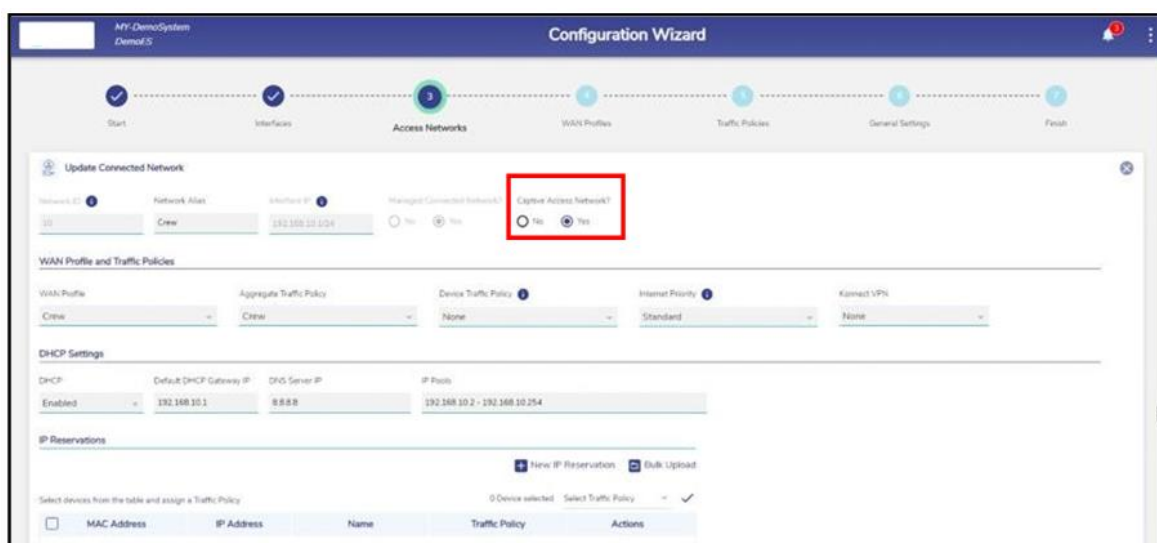


Figure 3.59 Captive Access Network Configuration

Application Policy Profile

New Rule

Below rules will be applied in the order stated.

Allow Domain (*x4mobility.com)

Implicit Deny

Figure 3.60 Aggregate Network Policy

MY-Demo Site
StarLink Setup

Configuration Wizard

Start Interfaces **Access Networks** WAN Profiles Traffic Policies General Settings Finish

☒ Tabular View ☐ Expanded View

[Add Connected Network](#) [Add Managed Routed Network](#)































Network Alias	Network ID	Interface IP/Subnet	Gateway	WAN Profile	Aggregate Traffic Policy	Device Traffic Policy	Internet Priority	DHCP	Default DHCP Gateway IP	DNS Server IP	Actions
Default	0	10.91.1.1/24	--	Default	Default	None	High	Enabled	10.91.1.1	8.8.8.8	    
Crew	10	192.168.10.1/24	--	Crew	Crew	None	Standard	Enabled	192.168.10.1	8.8.8.8	    
Guest	20	192.168.20.1/24	--	Guest	Guest	None	Standard	Enabled	192.168.20.1	8.8.8.8	    
Operational	50	192.168.50.1/24	--	--	--	--	--	Disabled	--	--	    
Subnet-1	--	10.30.1.1/24	192.168.50.4	Operational	Operational	None	High	Enabled	10.30.1.1	8.8.8.8	    
Subnet-2	--	10.30.2.1/24	192.168.50.4	Operational	Operational	None	Standard	Enabled	10.30.2.1	8.8.8.8	    

Figure 3.61 Captive Access Network

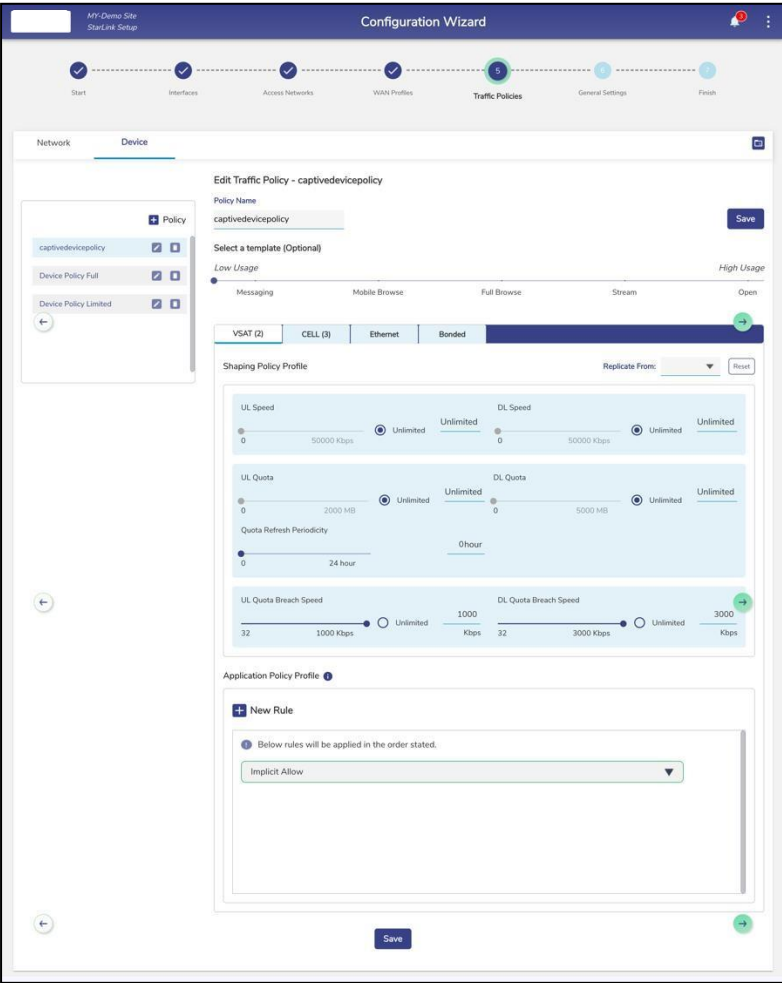



Figure 3.62 Device Traffic Policy

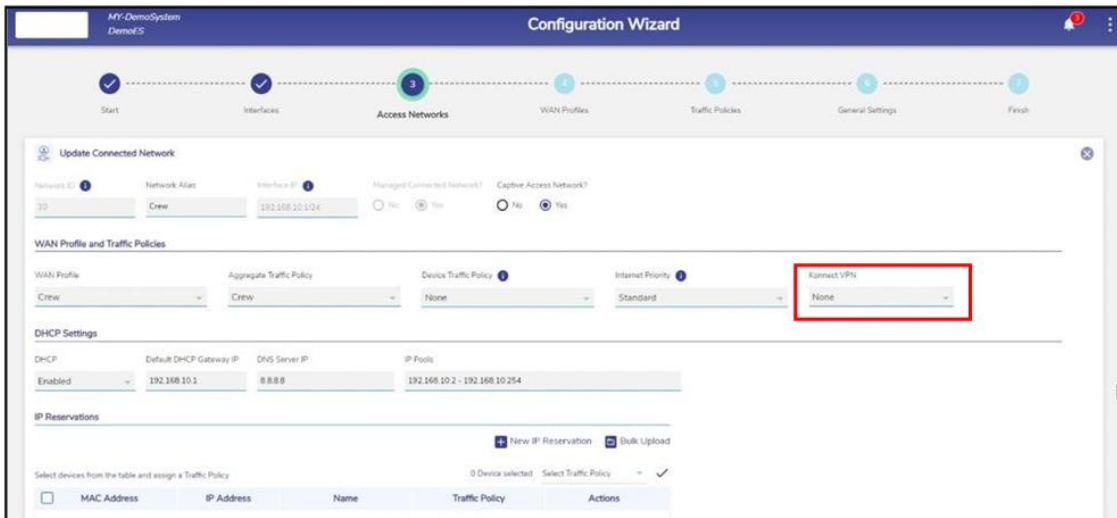
3.2.7 Configuring Konnect VPN

To route the Access Network traffic through the VPN, edit the Access Network configuration to pick the configured VPN end point to route. This allows the EdgeOS System to VPN access networks to a Konnect VPN Server; this is most utilized between EdgeOS Systems. For details of VPN Configuration, see [3.5.6 Konnect VPN](#).

To configure Konnect VPN, perform the following steps.

Steps

- Click  icon of the Access Network that the user wants to configure Konnect VPN for.
- Under the Konnect VPN field, select from one of the configured VPNs, see [Figure 3.63 Konnect VPN Configuration](#).



The screenshot displays the 'Configuration Wizard' interface for 'MY-DemoSystem Demo-5'. The wizard is at the 'Access Networks' step, indicated by a green circle with the number 3. The progress bar shows steps: Start, Interfaces, Access Networks, WAN Profiles, Traffic Policies, General Settings, and Finish.

The 'Update Connected Network' section includes fields for 'Network ID' (10), 'Network Alias' (Crew), 'Interface ID' (192.168.10.1/24), and checkboxes for 'Managed Connected Network?' (No) and 'Captive Access Network?' (Yes).

The 'WAN Profile and Traffic Policies' section contains dropdown menus for 'WAN Profile' (Crew), 'Aggregate Traffic Policy' (Crew), 'Device Traffic Policy' (None), 'Internet Priority' (Standard), and 'Konnect VPN' (None). The 'Konnect VPN' dropdown is highlighted with a red rectangle.

The 'DHCP Settings' section shows 'DHCP' (Enabled), 'Default DHCP Gateway IP' (192.168.10.1), 'DNS Server IP' (8.8.8.8), and 'IP Pools' (192.168.10.2 - 192.168.10.254).


The 'IP Reservations' section has buttons for 'New IP Reservation' and 'Bulk Upload', and a table with columns: MAC Address, IP Address, Name, Traffic Policy, and Actions.

Figure 3.63 Konnect VPN Configuration

3.2.8 LAN Monitoring

To monitor a device connected to the network, perform the following steps.

Steps

- Click  corresponding to the network under the **Action** section on the **Access Networks** page. The **LAN Monitoring** pop-up window appears, see figure below.

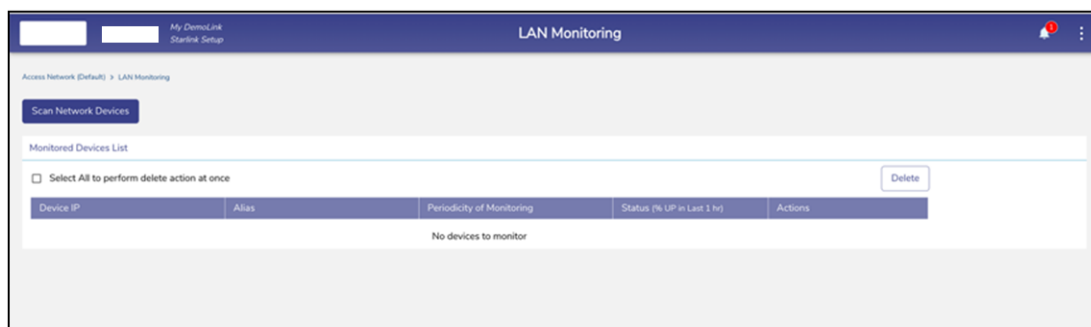


Figure 3.64 LAN Monitoring

- Click **Scan Network Devices**. The scan is in progress, see figure below.

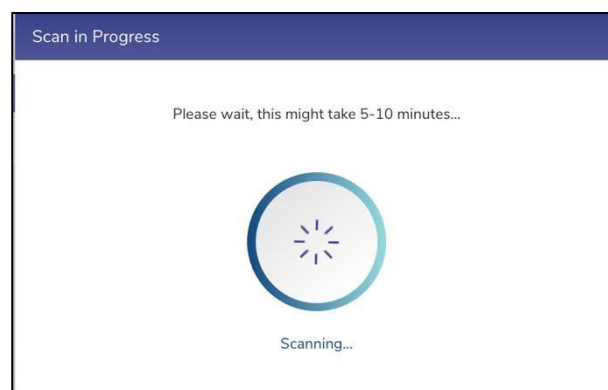


Figure 3.65 Network Design Scan Progress

The scanned network devices list is displayed, see figure below.

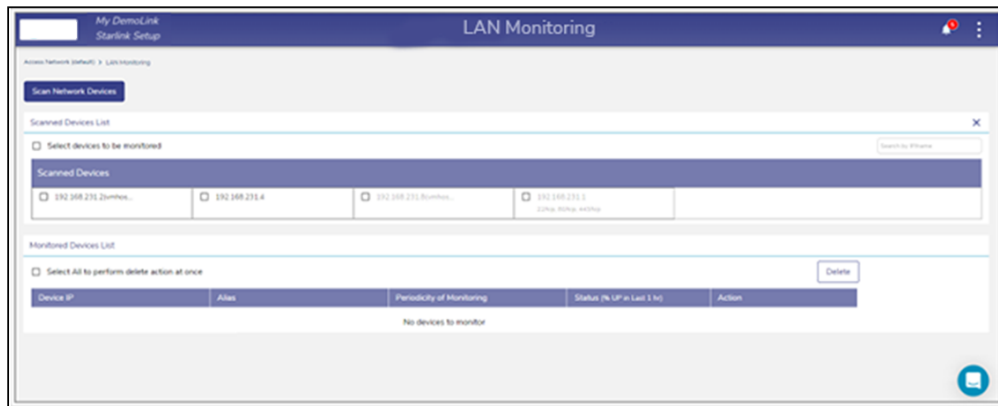


Figure 3.66 LAN Monitoring

- Select the IP address check box of the devices under the **Scanned Devices List** section.
- Or,
- To select the entire device, select the **Select devices to be monitored** check box under the **Scanned Devices List** section.
- The IP address of the device becomes available under the **Monitored Devices List**, see figure below.

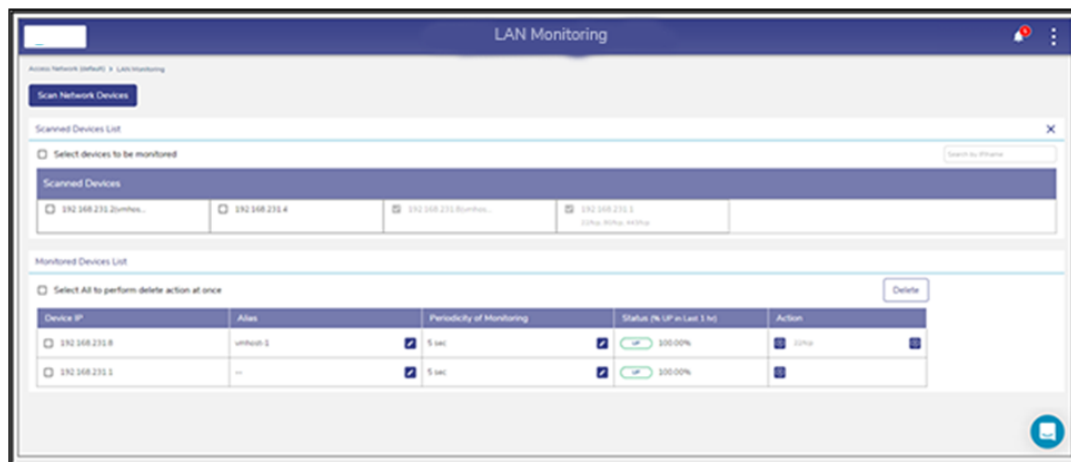




Figure 3.67 Monitored Devices

If the device is up, then the status  is displayed under the **Status (% UP in Last 1 hr.)** section.


If the device is down, then the status  is displayed under the **Status (% UP in Last 1 hr.)** section.

Additionally, the duration of the device being up in the last 1 hour is displayed next to the status under the **Status (% UP in Last 1 hr.)** section.

3.2.8.1 Configuring Periodicity of Monitoring

To configure the periodicity of monitoring, perform the following steps.

Steps

- Click  under the **Periodicity of Monitoring** section on the **LAN Monitoring** page. The periodicity list becomes available, see figure below.

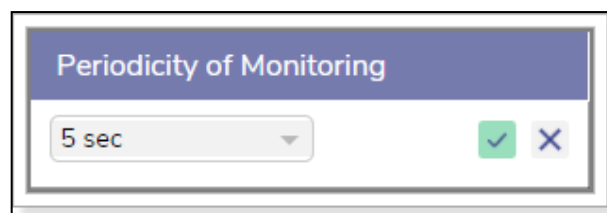



Figure 3.68 Periodicity of Monitoring

- In the periodicity list, click the periodicity.
- Click .

The device is monitored based on the configured periodicity.


Or,

To exit without configuring the periodicity of monitoring, click .

3.2.8.2 Adding to Konnect

To add to the Konnect, perform the following steps.

Steps

- Click  under the **Action** section on the **LAN Monitoring** page. The **Add to Konnect** pop-up window appears, see figure below.

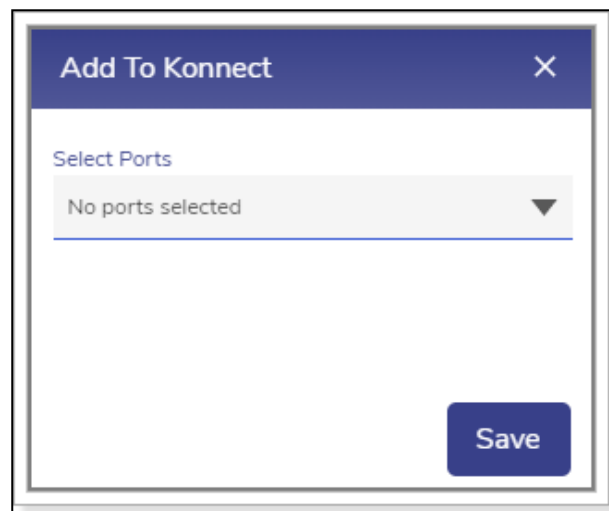


Figure 3.69 Add to Konnect

- Click the port list and then select the port number check box.

User can select multiple port numbers.

- Click **Save**. The port numbers are displayed under the **Action** section, see figure below.



Figure 3.70 Port Added to the Konnect

In addition to this, the **Remove from Konnect** icon becomes available under the **Action** section, see figure below.

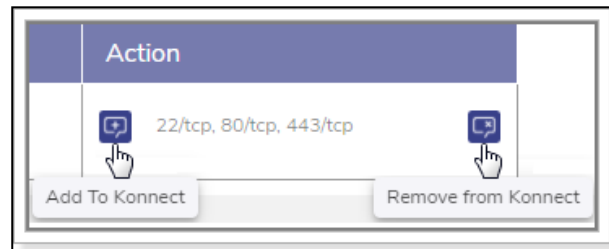


Figure 3.71 Add/Remove from Konnect

3.2.8.3 Removing from Konnect

To remove from Konnect, perform the following steps.

Steps

- Click the Remove from Konnect icon, see **Figure 3.71 Add/Remove from Konnect**. The Remove From Konnect pop-up window appears, see **Figure 3.72 Remove from Konnect Pop-up**.

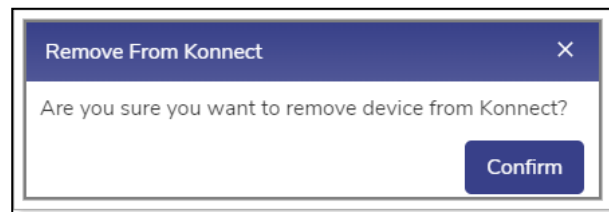


Figure 3.72 Remove from Konnect Pop-up

- Click **Confirm**.

The device is removed from the Konnect.

3.2.8.4 Deleting the Monitored Devices

To delete the monitored devices, perform the following steps.

Steps

- Select the IP address check box.

User can select multiple

devices. Or,

To select all devices, select the **Select All** to perform delete action at once.

check box under the **Monitored Devices List** section.

- Click Delete. The Stop Monitoring pop-up window appears, see [Figure 3.73 Stop Monitoring](#).

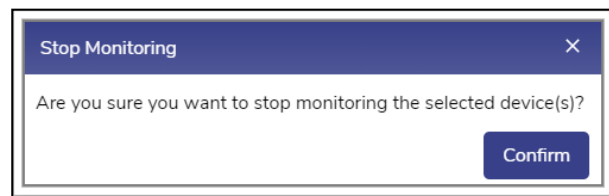


Figure 3.73 Stop Monitoring

- Click **Confirm**.

The device is deleted. Therefore, it is not monitored.

3.2.9 Pausing or Resuming Network Traffic

To pause the network traffic, perform the following steps.

Steps


- 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 below.




Figure 3.74 Pause Network Pop-up

- Click **Pause**. The Resume Network Traffic  button becomes available, and the row of the network is highlighted by color. In addition to this,  icon becomes available corresponding to the network under the Network Alias field.

User cannot pause the network traffic of the connected network.

To resume the network traffic, perform the following steps.

Steps

- 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 below.

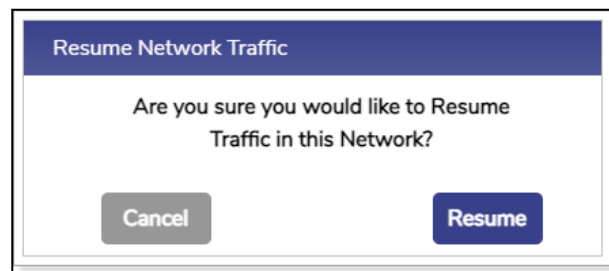



Figure 3.75 Resume Traffic Pop-up

- Click **Resume**. The network traffic on the network resumes.

3.2.10 Deleting Network

To delete the network, perform the following steps.

Steps

- 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 below.

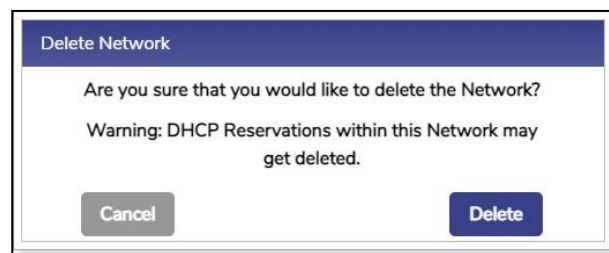


Figure 3.76 Delete Network Pop-up

- Click **Delete**.
- The network is successfully deleted. This will impact the DHCP reservations. Therefore, it is highly recommended to verify the network details before deleting the network.

3.3 WAN Profiles

While the EdgeOS System is installed on the vessel, a default WAN Profile is created with the priority of the enabled WANs configured in this WAN Profile and assigned to the default Access Network. However, user can create multiple WAN profiles of their choice.

3.3.1 WAN Profile Types

There are multiple profile options available, such as Strict Priority, Bonding and Advanced Bonding.

3.3.1.1 Strict Priority

This is a configuration where WAN links are arranged in a priority order where there is never more than one WAN link for a given priority.

3.3.1.2 Bonding

It is possible to configure any individual VLAN, subnet or even device in a way that the Internet traffic that entity is carried by more than one WAN link, based on conditions. This feature is called bonding, and the set of WAN links is called the 'bonded set'. Within WAN profiles, if any priority levels contain more than one WAN link, then those links in that priority level form a bonded set. It should be noted that, should any one link in a bonded set fail, while new TCP or UDP sessions would be assigned to one of the surviving links of the bonded set, any sessions currently using that failed link will be lost.

3.3.1.3 Advanced Bonding

This is a special case of bonding where, if one of the links in a bonded set fails, any existing TCP or UDP sessions over it will be seamlessly diverted to another link in the same set. This type implements link bonding of WAN links based on advanced proprietary algorithm. The implementation considers link speed estimates, which is also determined using an advanced proprietary algorithm. It also uses latency measurements to augment or even replace re-weighting based on speed estimates.

3.3.2 Enabling Advanced Bonding

On top left of the WAN Profile screen, Advanced Bonding Enable/Disable buttons are available, see figure below. By default, Advanced Bonding is disabled. **Advanced Bonding** is a licensed feature and is available with only US Internet features.

Therefore, to enable this, user must ensure that the license of the Advanced Bonding is available for the vessel.

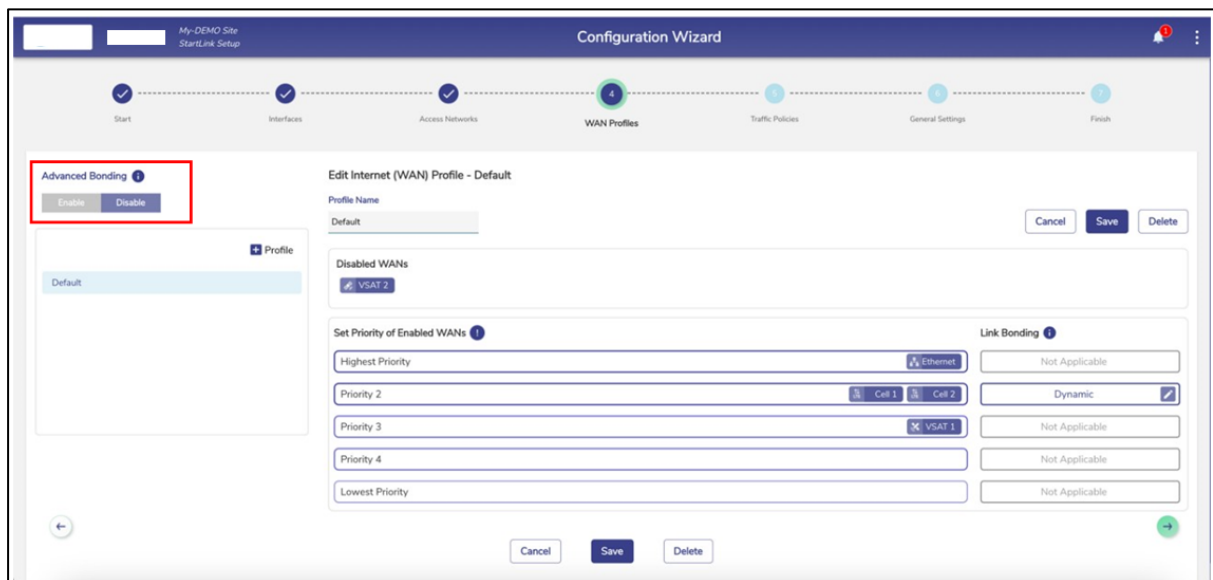



Figure 3.77 Advance Bonding

3.3.3 Creating a new WAN Profile

To create a WAN profile, perform the following steps.

- Click  on the **Access Networks** page or click **WAN Profiles**. The **WAN Profiles** page appears, see figure below.

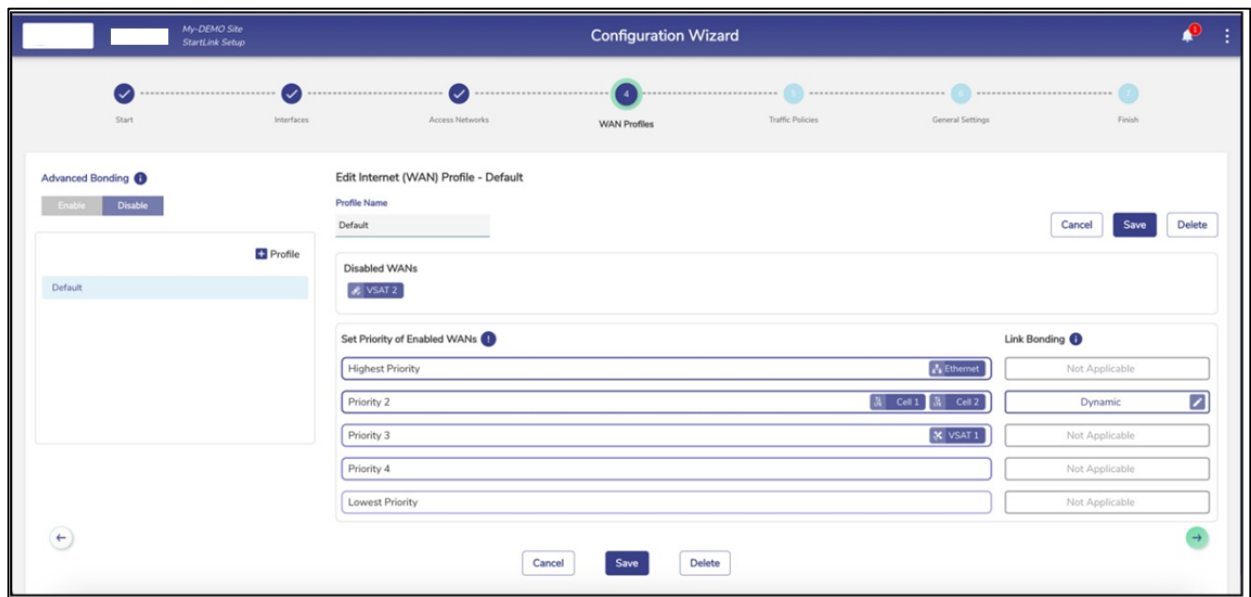



Figure 3.78 WAN Profile

Initially, the **Default** WAN profile is available. User can create multiple profiles. Once, the profiles are configured, the profiles become available on the **WAN Profiles** page. They can associate the WAN profile with Access Networks.

- To create a WAN Profile, click **+ Profile**. The Profile Name field becomes available under the **Create Internet (WAN) Profile** section. To enter data in the respective fields, see table below.

Fields	Description
Profile Name	Enter the name of the profile.
Disabled WANs	Disabled WAN sources are displayed.
Set Priority of Enabled WANs	
Highest Priority	<p>To assign WAN links/Interfaces to a priority level, perform the following steps.</p> <p>Note: Only Interfaces enabled on the Interfaces tab will be visible on the WAN Profile screen.</p> <p>Steps</p> <p>Drag and drop the WANs available from the Disabled WANs section to the respective priority section. More than one WAN (similar or dissimilar type) can be associated with a single priority. In this case, these WANs will be bonded.</p> <hr/> <p>Note: Interfaces/WANs for which Probe Configuration Profile is set to Always Up or High Cost cannot be bonded with other Interfaces/WANs.</p> <p>Link Bonding can be set to Static or Dynamic. By default, the link bonding type is Dynamic, in which case the system distributes the traffic on each WAN link based on performance. In Static Setting, a configured % of traffic is set for each WAN link. For details of the types of link bonding, point to  next to the Link Bonding. The user can configure the weighting % of the WAN link.</p> <p>To configure the weighting %, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click Dynamic under the link bonding section. The Bonding Mechanism pop-up window appears, see Figure 3.79 Bonding Mechanism. Click Static. The Weighting % (applicable for Static Bonding) section becomes available. The Bonding Mechanism pop-up window appears, see Figure 3.80 Static Bonding Mechanism.

	<ul style="list-style-type: none"> Enter the weighting % for the WAN links. User must ensure that the sum of the weighting % for all WAN links must be 100%. Below is an example of the like WAN links bonding. <p>User can configure 40 as the weighting % for the Cell 1 and 60 as the weighting % for the Cell 2. As, sum of both weighting % (40 + 60) = 100.</p> <p>Below is an example of the unlike WAN links bonding.</p> <p>User can configure 40 as the weighting % for the VSAT1, 30 as the weighting % for the Cell 1, and 30 as the weighting % for the Cell 2, hence the sum of weighting % (40 + 30 + 30) = 100.</p> <ul style="list-style-type: none"> Click Done. The WAN Profile is created and updated in the left table. <p>In case of trying to bond WANs with probe configuration profile set to 'Always Up' or 'High Cost', an error message is displayed, see Figure 3.81 Error Message.</p>
Priority 2	Refer to Highest Priority .
Priority 3	Refer to Highest Priority .
Priority 4	Refer to Highest Priority .
Lowest Priority	Refer to Highest Priority .

Table 3-19 WAN Profile

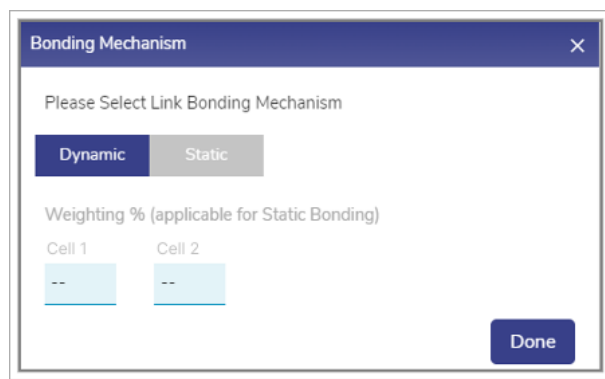


Figure 3.79 Bonding Mechanism

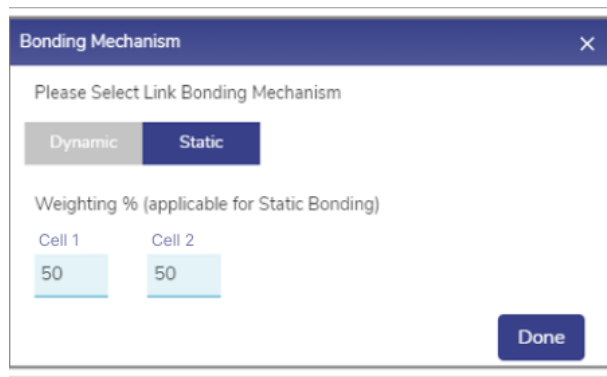


Figure 3.80 Static Bonding Mechanism



Figure 3.81 Error Message

Once the WAN link is assigned to the priority levels, the server will verify the network based on the priority levels. As an example, the user can set the following priority levels of enabled WANs for Owner Profile.

Highest Priority – Ethernet

Priority 2 – Cell1 and Cell2.

Priority 3 – VSAT 1 and VSAT 2.

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

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

- Click **Save**.

WAN profile is configured successfully and visible on the table listing on the left. The WAN profile will become available while configuring the networks, see figure below.

The screenshot displays the 'Configuration Wizard' interface for 'MY-DEMO Site StartLink Setup'. The wizard progress bar at the top shows steps: Start, Interfaces, Access Networks, WAN Profiles (current step, highlighted with a green circle), Traffic Policies, General Settings, and Finish. The main content area is titled 'Edit Internet (WAN) Profile - Owner Profile'. On the left, under 'Advanced Bonding', there is a table listing profiles: 'Default' and 'Owner Profile'. The 'Owner Profile' is highlighted with a red rectangle. The main configuration area for the 'Owner Profile' includes a 'Profile Name' field, 'Owner Profile' label, and buttons for 'Cancel', 'Save', and 'Delete'. Below this is a 'Disabled WANs' section. The 'Set Priority of Enabled WANs' section contains a table with five rows: 'Highest Priority', 'Priority 2', 'Priority 3', 'Priority 4', and 'Lowest Priority'. Each row has a dropdown menu for selecting a WAN link. The 'Highest Priority' row is set to 'Ethernet', 'Priority 2' to 'Cell 1', 'Priority 3' to 'VSAT 1', 'Priority 4' to 'VSAT 2', and 'Lowest Priority' is empty. To the right of this table is a 'Link Bonding' section with a dropdown menu set to 'Not Applicable'. At the bottom of the configuration area are 'Cancel', 'Save', and 'Delete' buttons. A green arrow button is located at the bottom right of the wizard.

Figure 3.82 WAN Profile Creation

3.3.4 Editing a WAN Profile

To edit a WAN profile, perform the following steps.

Steps

- Click on the **WAN Profile** to be edited.
- The WAN Profile appears on the right section.
- The user can edit the profile name or WAN priorities.
- Click **Save** to profile.
- The WAN Profile is successfully saved.

3.3.5 Deleting a WAN Profile

To delete a WAN profile, perform the following steps.

Steps

- Click on the **WAN Profile** to be deleted.
- Click **Delete** button on top right or bottom.
- Click OK to confirm the deletion operation, see **Figure 3.83 Delete Profile**.
- The WAN Profile will be deleted from the system.

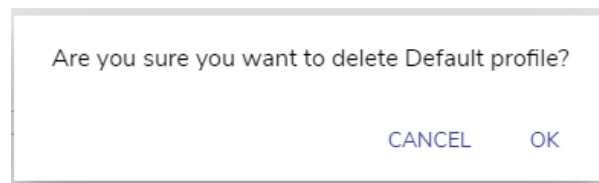


Figure 3.83 Delete Profile

3.4 Traffic Policies

When the EdgeOS System is installed on the vessel, by default, the network level policy named 'Default Network' is pre-created in the system, but no device level traffic policies are present. The network level policy will be applicable under the Aggregate Traffic Policy of the Access Network and the device level policy will be applicable under the Device Traffic Policy.

3.4.1 Creating a new Network Traffic Policy

To configure the Traffic Policies, perform the following steps.

Steps

- Click  on the **WAN Profiles** or click **Traffic Policies**. The **Traffic Profiles** page appears, see figure below.

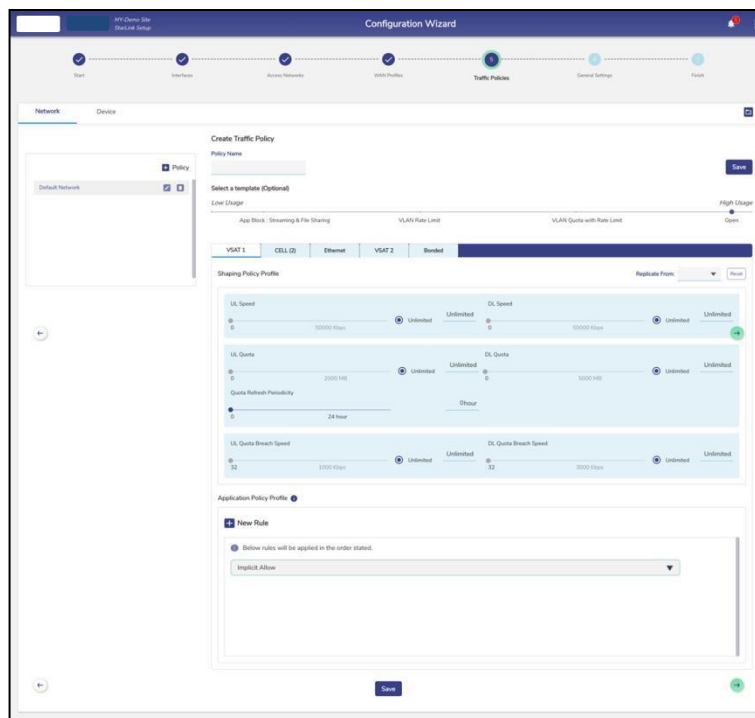


Figure 3.84 Traffic Policies

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

- Click **Network**.

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

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

Fields	Description
Policy Name	Enter the name of the policy.
Select a template (Optional)	<p>Click a template that is to be assigned to a WAN. 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, user can modify the template.</p> <p>The user 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 their requirement through the Open template. By default, the Open template is selected.</p>
Select WAN Type	<p>Aliases of the Interfaces/WANs that are enabled on the Interfaces screen will appear here.</p> <hr/> <p>Exception: If there are two or more Interfaces/WANs of the same technology, they will have common policy and will appear in a single tab with name same as the Interface/WAN type and the number of WAN in brackets (hover on the WAN will show the Interface Aliases of the Interfaces for which the policy is applicable). If there are Bonded Interfaces/WANs in any of the WAN profiles, there will be a Bonded tab. The policy under this tab will apply to traffic flowing through bonded links.</p>


	<p>By default, the first Interface Alias will be selected. The tab can be any/all the below WAN types, depending on the number of WANs enabled in the system.</p> <ul style="list-style-type: none"> • VSAT • VSAT-LEO • VSAT-FBB • CELL • Wi-Fi • Ethernet • Bonded
Shaping Policy Profile	
UL Speed	<p>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.</p> <p>To configure the upload speed, move the slider to the right or click the speed.</p> <p>The Unlimited is cleared and the upload speed configured is displayed corresponding to the UL Speed.</p>
DL Speed	<p>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.</p> <p>To configure the download speed, move the slider to the right or click the speed.</p> <p>The Unlimited is cleared and the download speed configured is displayed corresponding to the DL Speed.</p>
UL Quota	<p>This indicates the permissible quota up to which the user can upload the data.</p> <p>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.</p>


	<p>To configure the upload quota, move the slider to the right or click the quota.</p> <p>The Unlimited is cleared and the upload quota configured is displayed corresponding to the UL Quota.</p>
DL Quota	<p>This indicates the permissible quota up to which the user can download the data.</p>
	<p>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.</p> <p>To configure the download quota, move the slider to the right or click the quota.</p> <p>The Unlimited is cleared and the download quota configured is displayed corresponding to the DL Quota.</p>
Quota Refresh Periodicity	<p>This indicates the expiry in hours after which the upload quota and download quota will be refilled or reset to the pre-configured upload quota and download quota respectively.</p>
	<p>To configure the quota refresh periodicity, move the slider to the right or click the refresh periodicity.</p> <p>The refresh periodicity configured is displayed corresponding to the Quota Refresh Periodicity.</p>
UL Quota Breach Speed	<p>This indicates the upload speed that will be applicable after the UL quota is exhausted.</p>
	<p>By default, Unlimited is selected and the Unlimited UL quota breach speed is displayed corresponding to the UL Quota Breach Speed.</p> <p>This indicates that the UL quota breach speed will continue until the UL quota is refilled based on the quota refresh periodicity.</p> <p>To configure the UL quota breach speed, move the slider to the right or click the breach speed.</p>


	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.
	<p>By default, the Unlimited is selected and the Unlimited DL quota breach speed is displayed corresponding to the DL Quota Breach Speed.</p> <p>This indicates that the DL quota breach speed will continue until the DL quota is refilled based on the quota refresh periodicity.</p> <p>To configure the DL quota breach speed, move the slider to the right or click the breach speed.</p> <p>The DL quota breach speed configured is displayed corresponding to the DL Quota Breach Speed.</p>
Replicate From	<p>To replicate the traffic policy of a WAN, perform the following steps.</p> <p>Steps</p> <p>Click Replicate From.</p> <p>Click a WAN whose traffic policy is to be applied to the WAN. •</p> <p>The user can re-configure the replicated traffic policy.</p>
Application Policy Profile	
New Rule	To create a new rule, click New Rule . The Category, Application and Internet Priority fields become available.
Select Category	<p>Click a category, see Figure 3.85 Category list.</p> <p>By default, the Application category is selected. Therefore, the Application Rules field becomes available, see Figure 3.86 Applications List.</p> <p>Or,</p>

	<p>If the user selects the Domain category, then the Domain Rules field becomes available, see Figure 3.87 Domain Rules.</p> <p>Or,</p> <p>If user selects the IP & Port category, then the IP & Port field becomes available.</p> <p>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. User cannot modify the Implicit Allow rule.</p>
Application Rules	<p>To apply or deny application rules, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click under the Application Rules section. The list becomes available, see Figure 3.86 Applications List. Click Category or Subcategory. List based on the selected Category or Subcategory becomes available. Click a category or subcategory. To allow the application, click Allow. <p>Or,</p> <ul style="list-style-type: none"> To block the application, click Deny. <hr/> <p>By default, Allow is selected.</p> <p>Click Save.</p> <p>The allowed and blocked application becomes available, see Figure 3.88 Application Allow or Deny.</p> <hr/> <p>There can be a single deny and single allow rule per category or an implicit allow or an implicit deny rule.</p> <p>If user selects the Application Rule in the Select Category field, then the Application Rules field becomes available.</p>

Domain Rules	<p>To apply or deny domain rules, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click under the Domain Rules section. <p>Enter the name of the domain in one of the following formats.</p> <ul style="list-style-type: none"> domain.com domain1.domain2.com *.domain.com, <p>where,</p> <p>* Can be any value.</p> <hr/> <p>The user can enter multiple domain names.</p> <ul style="list-style-type: none"> To allow the domain, click Allow. <p>Or,</p> <ul style="list-style-type: none"> To block the domain, click Deny. <hr/> <p>By default, Allow is selected.</p> <ul style="list-style-type: none"> Click Save. <p>The allowed and blocked domain becomes available.</p> <hr/> <p>If user selects the Domain Rule in the Select Category field, then the Domain Rules field becomes available.</p>
	<p>The user can also upload the rule list in CSV format.</p> <p>To upload the rule list in CSV format, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Open the Notepad. <hr/> <p>The user can create the CSV file in various text editors such as - Notepad, Microsoft Excel, and Google Docs.</p>

	<ul style="list-style-type: none"> Enter the Domain in the first row, see Figure 3.89 Domain Rule CSV Format. <hr/> <p>The first row is referred to as the header row.</p> <ul style="list-style-type: none"> Enter the name of the domain in the subsequent rows, see. Figure 3.90 Example of Domain Rule Save the file with the .csv extension. Click  and browse the CSV file of the domain rule list. Click Open. The domain rules are displayed under the Domain Rules section, see Figure 3.91 Domain Rule Section. Click Save. <hr/> <p>If user selects the Domain Rule in the Select Category field, then the DomainRules field becomes available.</p>
IP & Port	<p>To apply or deny IP and port rules, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click under the IP & Port section, see Figure 3.92 IP & Port Section. <p>Enter IP and port in one of the following formats.</p> <ul style="list-style-type: none"> 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 <p>Where,</p> <p>x is a subnet, and its value can be from 0 (zero) to 32.</p> <p>y and z are port numbers, and its value can be from 0 (zero) to 65535.</p>

	<p>a/b/c/d are IP, and its value can be from 0 (zero) to 255.</p> <hr/> <p>User can enter multiple IP and ports.</p> <ul style="list-style-type: none"> To allow the IP, click Allow. <p>Or,</p> <ul style="list-style-type: none"> To block the IP, click Deny. <hr/> <p>By default, Allow is selected.</p> <ul style="list-style-type: none"> Click Save. <p>The allowed and blocked IP and the port become available.</p> <hr/> <p>If user selects IP & Port in the Select Category field, then the IP & Port field becomes available.</p>
	<p>The user can also upload the rule list in CSV format.</p> <p>To upload the rule list in CSV format, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Open the Notepad. <hr/> <p>The user can create the CSV file in various text editors such as - Notepad, Microsoft Excel, and Google Docs.</p> <ul style="list-style-type: none"> Enter the IP & Port in the first row, see Figure 3.93 IP & Port Rule. <hr/> <p>The first row is referred to as the header row.</p> <ul style="list-style-type: none"> Enter the IP and port in the subsequent rows, see Figure 3.94 IP & Port Rule Example CSV Rule. Save the file with the .csv extension. Click  and browse the CSV file of the IP & Port rule list. Click Open. Only the valid IP & Port rules are displayed under the IP & Port Rules section, see Figure 3.95 Valid IP & Ports.

	<p>If an invalid IP & Ports are available, then an error is displayed.</p> <ul style="list-style-type: none"> Click Save. <p>If user selects IP & Port in the Select Category field, then the IP & Port field becomes available.</p>
Internet Priority	<p>To view the details of the internet priority, point the mouse to .</p> <p>And,</p> <p>In the Internet Priority list, click the internet priority.</p> <div> <p>Default – No Internet Priority</p> <p>High – Highest Priority</p> <p>Standard – Standard Priority</p> <p>Low – Lowest Priority</p> <p>Realtime – Voice/Video Communication</p> <p>Realtime Priority is suited for Apps such as Zoom and Teams, and is limited to a few Mbps.</p> </div>
UL Speed	<p>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.</p> <p>To configure the upload speed, move the slider to the right or click the speed.</p> <p>The Unlimited is cleared and the upload speed configured is displayed corresponding to the UL Speed.</p>
DL Speed	<p>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.</p> <p>To configure the download speed, move the slider to the right or click the speed.</p> <p>The Unlimited is cleared and the download speed configured is displayed corresponding to the DL Speed.</p> <p>After configuring the new rule, click Save.</p>


Implicit Allow/Deny Rules	<p>To implicitly allow the final policy, click Implicit Allow/Deny Rules, and then click Allow,</p> <p>Or,</p> <p>To implicitly Deny the final policy, click Implicit Allow/Deny Rules, and then click Deny, see Figure 3.96 Application Allow or Deny.</p>	
	Internet Priority	<p>To view the details of the internet priority, point the mouse to  . And,</p> <p>In the Internet Priority list, click the internet priority.</p>
	After configuring the implicit allow or deny rule, click Save .	

Table 3-20 Traffic Policy

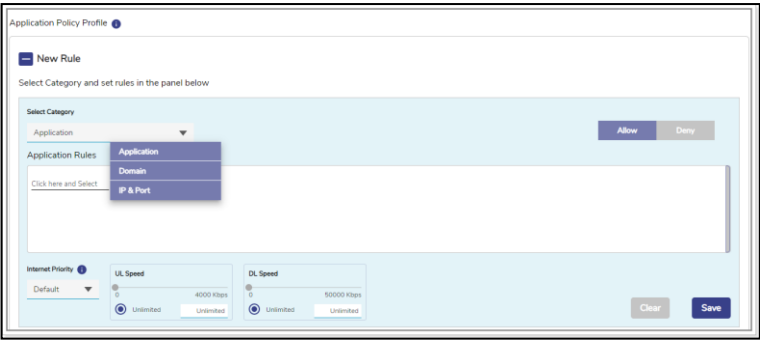


Figure 3.85 Category list

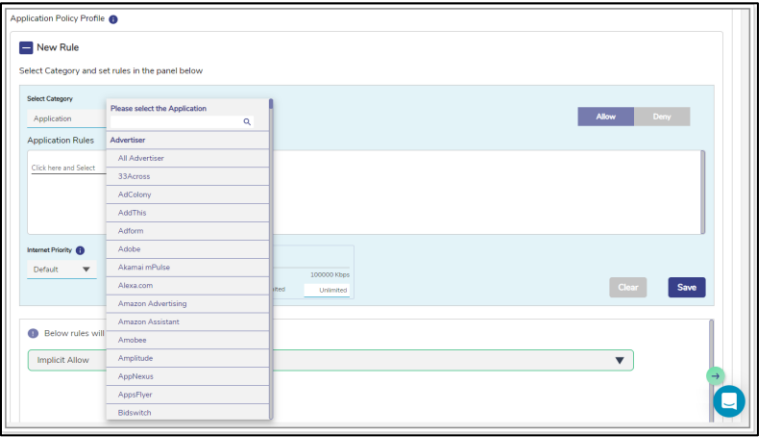


Figure 3.86 Applications List

Application Policy Profile

New Rule

Select Category and set rules in the panel below

Select Category

Domain

Allow Deny

Domain Rules

Type and Enter

You can enter the Policy Rules OR Upload list of Rules in CSV format

Internet Priority

Default

UL Speed

0 50000 kbps

Unlimited Unlimited

DL Speed

0 100000 kbps

Unlimited Unlimited

Clear Save

Figure 3.87 Domain Rules

Application Policy Profile

New Rule

Below rules will be applied in the order stated.

Implicit Allow

Implicit Allow/Deny Rules

This will be the final Policy Rule for all remaining unmatched data.

Allow Deny

Internet Priority

Default

Save

Figure 3.88 Application Allow or Deny

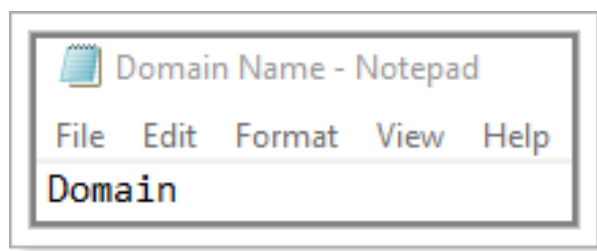


Figure 3.89 Domain Rule CSV Format

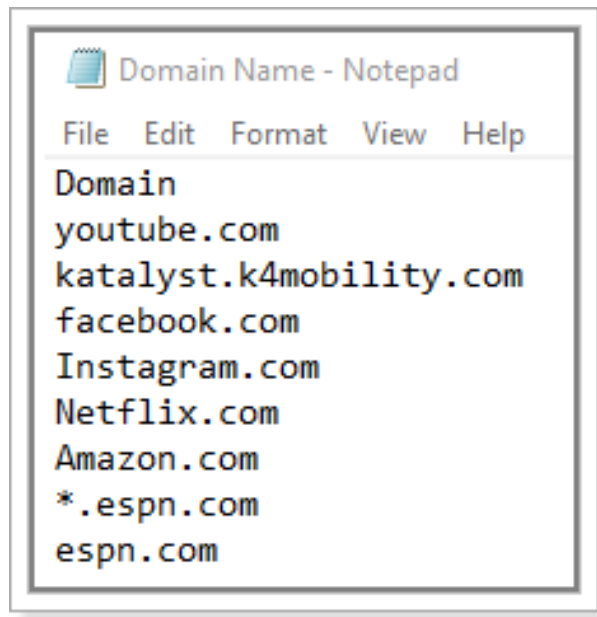


Figure 3.90 Example of Domain Rule

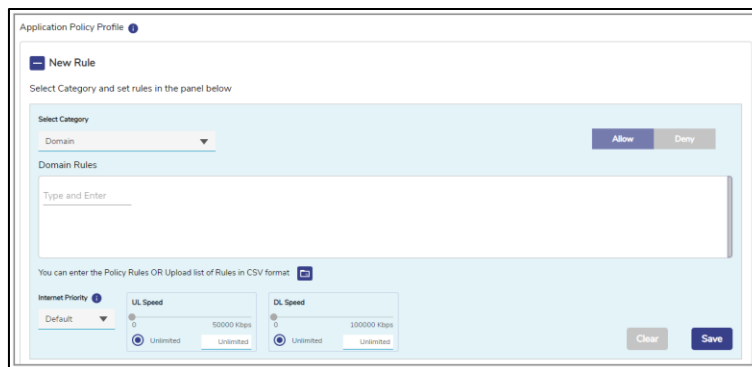


Figure 3.91 Domain Rule Section

Application Policy Profile 1

New Rule

Select Category and set rules in the panel below

Select Category: IP & Port Allow Deny

IP & Port Rules

Type and Enter

You can enter the Policy Rules OR Upload list of Rules in CSV format

Internet Priority: Default

UL Speed: 4000 Kbps Unlimited

DL Speed: 50000 Kbps Unlimited

Clear Save

Below rules will be applied in the order stated.

Implicit Allow

Save

Figure 3.92 IP & Port Section

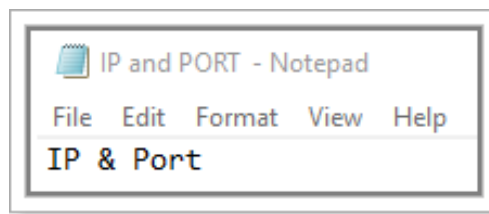


Figure 3.93 IP & Port Rule

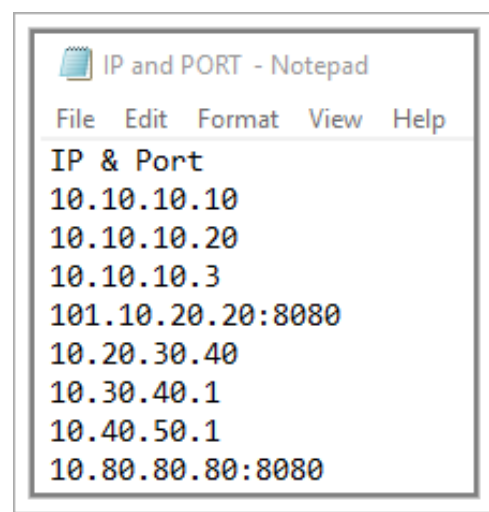


Figure 3.94 IP & Port Rule Example CSV Rule

Application Policy Profile

New Rule

Select Category and set rules in the panel below

Select Category: IP & Port

IP & Port Rules

10.10.10.10 10.10.10.20 10.10.10.3 101.10.20.20.8080 10.20.30.40 10.30.40.1 10.40.50.1 10.80.80.80.8080 10.10.10.10/32

10.10.10.10 255.255.255.255 Type and Enter

You can enter the Policy Rules OR Upload list of Rules in CSV format

Internet Priority: Default

UL Speed: 40000 Kbps

DL Speed: 100000 Kbps

Buttons: Clear, Save

Figure 3.95 Valid IP & Ports

Application Policy Profile

New Rule

Below rules will be applied in the order stated.

Implicit Allow

Implicit Allow/Deny Rules

This will be the final Policy Rule for all remaining unmatched data.

Internet Priority: Default

Buttons: Allow, Deny, Save

Figure 3.96 Application Allow or Deny

- Click **Save**. This will create the Network Traffic Policy.

3.4.2 Creating a new Device Policy

- Click Device tab to create Device Traffic Policy.
- Initially, no traffic policy is not available for the Device.
- Follow the same steps as Network Policy to create Device Traffic Policy.

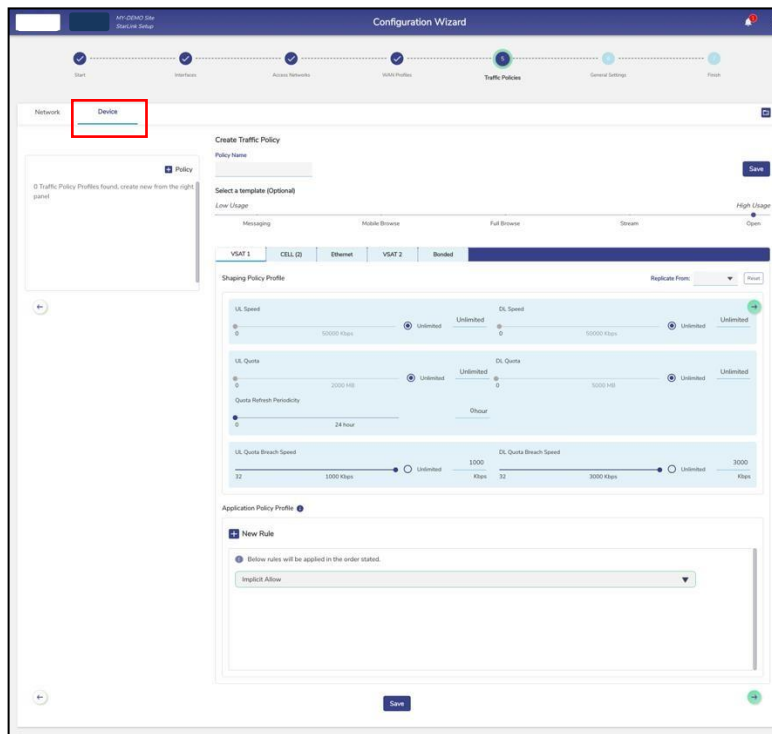


Figure 3.97 Create Device Policy


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 **Access Networks**.

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

3.4.3 Editing an existing Traffic Policy

To edit Traffic Policies, perform the following steps.


Steps

- Click on the edit icon  next to the policy.
- Update the fields that need to be changed.
- Click on **Save**.
- The policy will be successfully edited.

3.4.4 Deleting a Traffic Policy

To delete a Traffic Policies, perform the following steps.

Steps

- Click on the delete icon  next to the policy.
- Click **OK** to confirm or **Cancel** to cancel the deletion.
- On clicking OK, the policy will be successfully deleted.
- Note: If the policy to be deleted is assigned to an Access Network, then its deletion will result in an error message, see figure below.

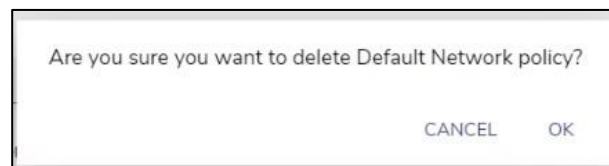


Figure 3.98 Delete Network Policy

3.5 General Settings

The user can configure the global Device Traffic policies, Static Routes, Firewall Rules, DNS proxy, Multicast settings, Konnect VPN, Quality of Service (QoS) settings, Configuration Backups, and uploads, see figure below.

Note: QoS Enable/Disable section is visible to users with administrative rights only.

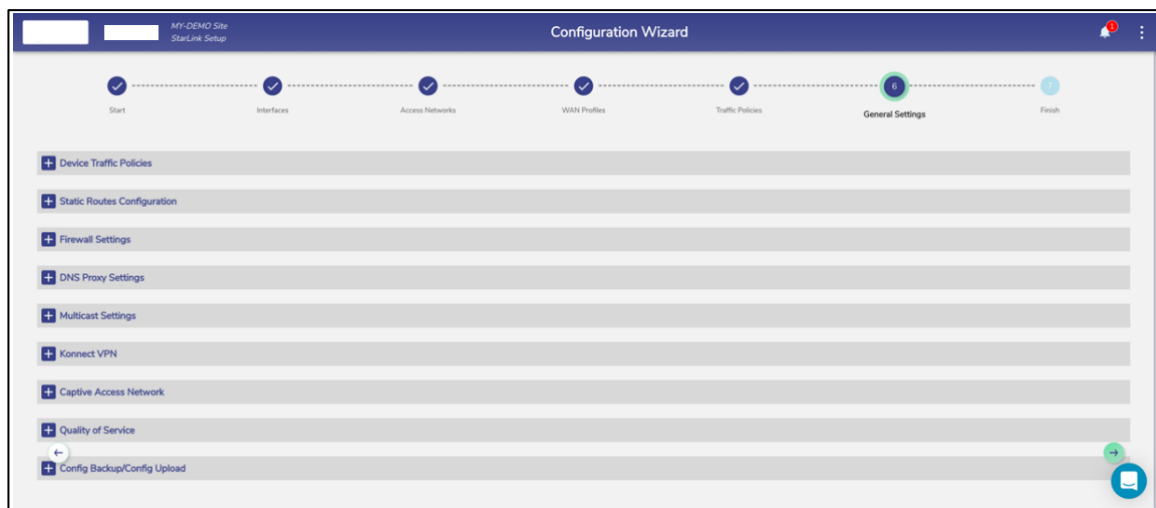


Figure 3.99 General Settings Configuration Wizard


3.5.1 Device Traffic Policies

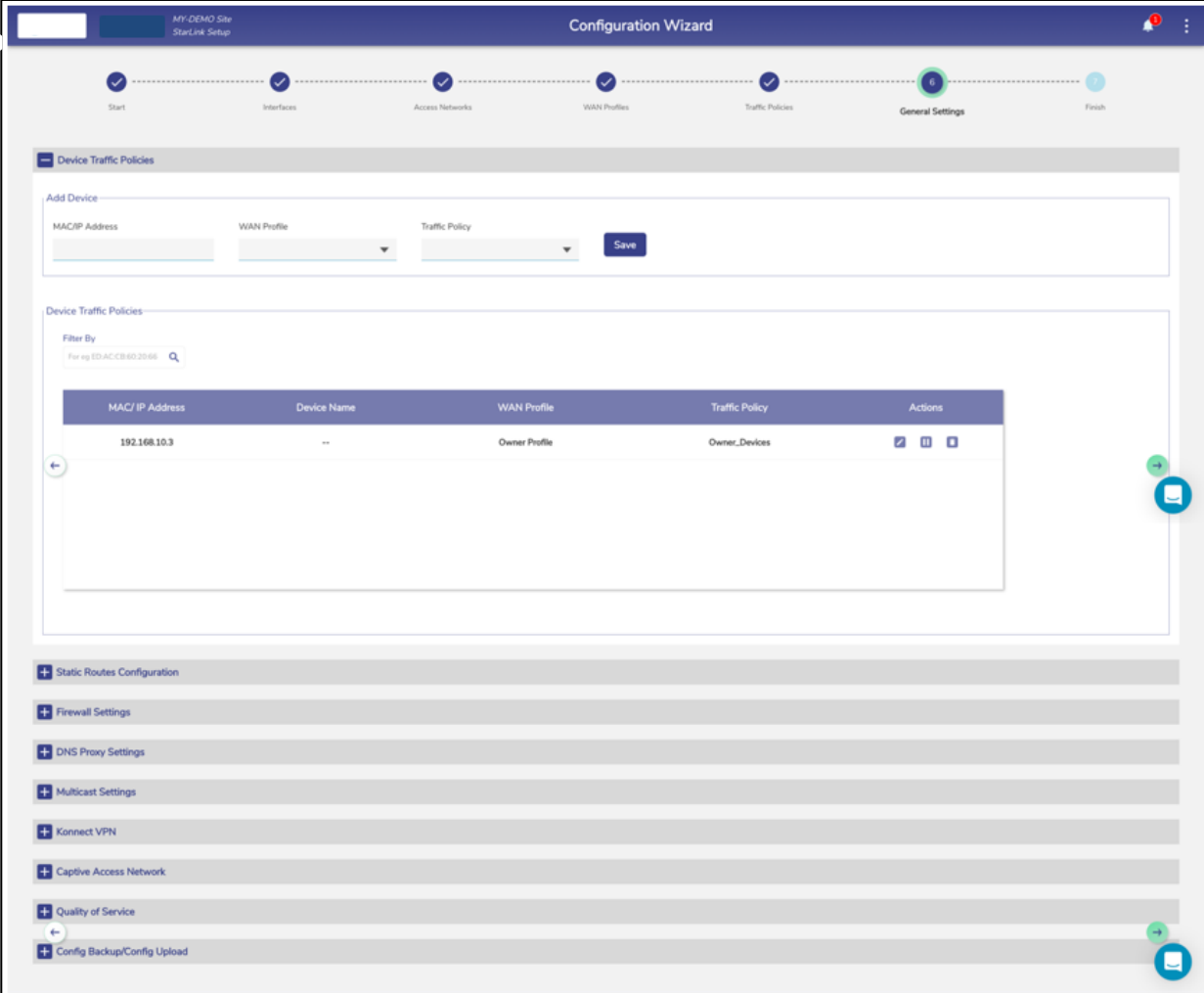
- It is possible to assign unique Traffic Policy and WAN Profile to a device through Device Traffic Policies section. Hence, if a device is assigned a unique Device Traffic Policy and it connects to an Access Network, the Traffic Policy and WAN Profile assigned to the device will override the Device Traffic policy and WAN Profile of the Access Network.

3.5.1.1 Configuring Device Traffic Policies

To configure the device traffic policy, perform the following steps.

Steps

- Click  on the Traffic Profiles page or click General Settings. The General Settings page appears., see [Figure 3.99 General Settings Configuration Wizard](#).
- Click **Device Traffic Policies**. The **Add Device** and Device Traffic Policies section becomes available, see figure below.






The screenshot shows the 'Configuration Wizard' interface with the 'General Settings' step highlighted. The 'Device Traffic Policies' section is expanded, showing an 'Add Device' form and a table of existing policies.

Add Device Form:

- MAC/IP Address:
- WAN Profile:
- Traffic Policy:
- Save button

Device Traffic Policies Table:

MAC/ IP Address	Device Name	WAN Profile	Traffic Policy	Actions
192.168.10.3	--	Owner Profile	Owner_Devices	  

Other Configuration Options (bottom):

- + Static Routes Configuration
- + Firewall Settings
- + DNS Proxy Settings
- + Multicast Settings
- + Connect VPN
- + Captive Access Network
- + Quality of Service
- + Config Backup/Config Upload

Figure 3.100 Device Traffic Policies

- To enter data in the respective fields, see table below.

Fields		Description
Add Device	MAC/IP Address	<p>Enter the MAC or IP address of a device.</p> <p>Or,</p> <p>Click the box and select a MAC or IP address.</p> <hr/> <p>The devices connected to the entire network become available.</p>
	WAN Profile	<p>This field is applicable only for IP Address. If user enters MAC Address, then WAN Profile will be disabled.</p> <p>In the WAN Profile list, click a WAN profile to be assigned to the IP address specified in the MAC/IP Address field. For this device, this WAN Profile will over-ride the WAN Profile of the Network to which the device is connected.</p>
	Traffic Policy	<p>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, Figure 3.101 Device Traffic Policy.</p> <hr/> <p>The device traffic policy created while configuring the traffic policies will become available. For details about the traffic policy, see 3.4 Traffic Policies.</p> <p>The user can assign the traffic policy to a device from also Access Networks. For details, see 3.2 However, the traffic policy last assigned to a device from any step will override the traffic policy of that device. Following is an example.</p> <p>Previously, the traffic policy was assigned to a device from Access Networks. A new traffic policy is assigned to a device from General Settings Therefore, the traffic policy assigned to a device from General Settings will override the existing traffic policy of that device.</p>




Device Traffic Policies	<p>Details of the MAC or IP address become available under the Device Traffic Policies section.</p> <p>To assign a new traffic policy to a MAC or IP address, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  corresponding to the MAC/IP address. The box becomes available corresponding to the MAC/IP address. Click and select a new WAN profile or traffic policy to be assigned to the MAC/IP address. <p>Or,</p> <ul style="list-style-type: none"> To pause the traffic on a MAC/IP address, click  corresponding to the MAC/IP address. To resume the traffic policy, click Resume. <p>To delete the traffic policy of a MAC/IP address, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  corresponding to the MAC/IP address. The confirmation message box appears. Click OK.
--------------------------------	--

Table 3-21 Device Traffic Policies

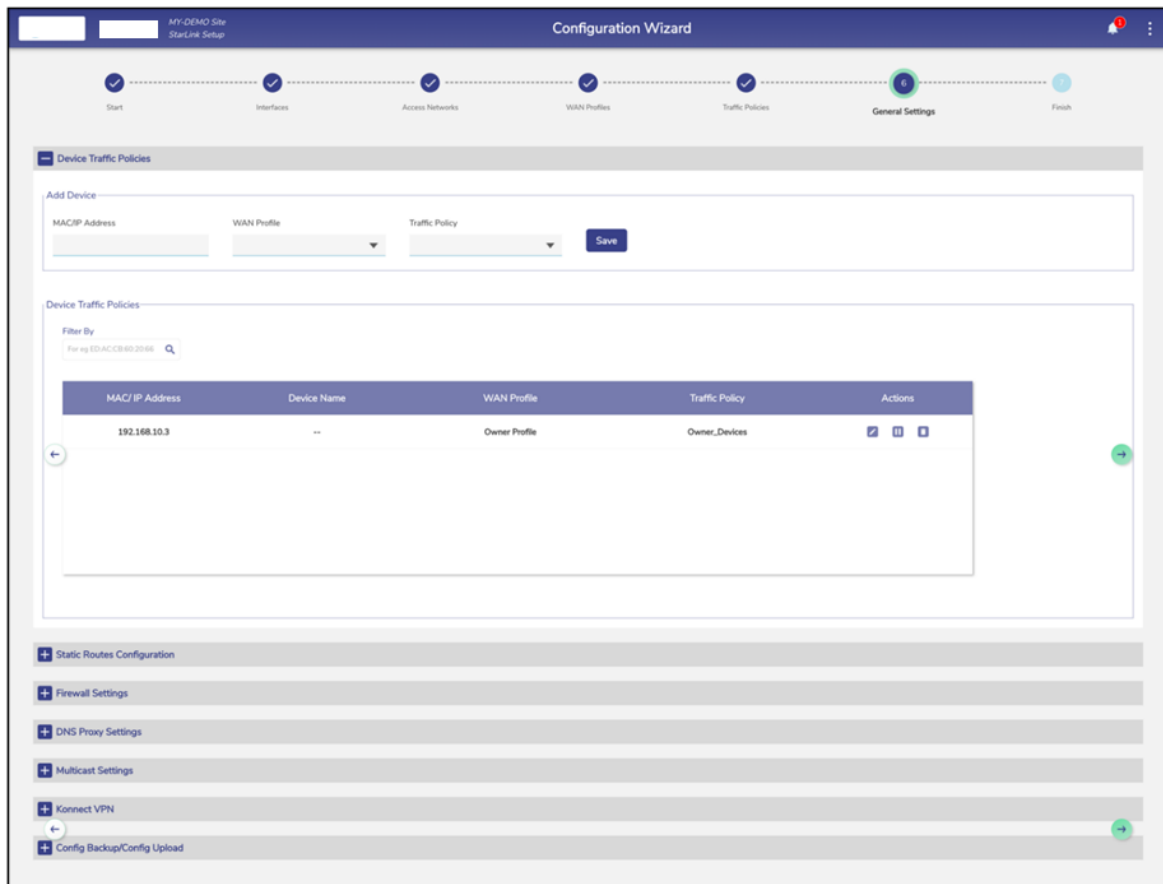


Figure 3.101 Device Traffic Policy Creation


3.5.2 Static Routes Configuration

This section has routes that need to be configured to access any device that can be reached through a router connected to the LAN interface of the EdgeOS System. As part of configuration, we need to specify the subnet we want to reach, and the 'gateway address', which is the address of the router.

3.5.2.1 Configuring Static Routes

To configure the static routes, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click **Static Route Configuration**. The **Add Static Routes** section becomes available. See figure below.

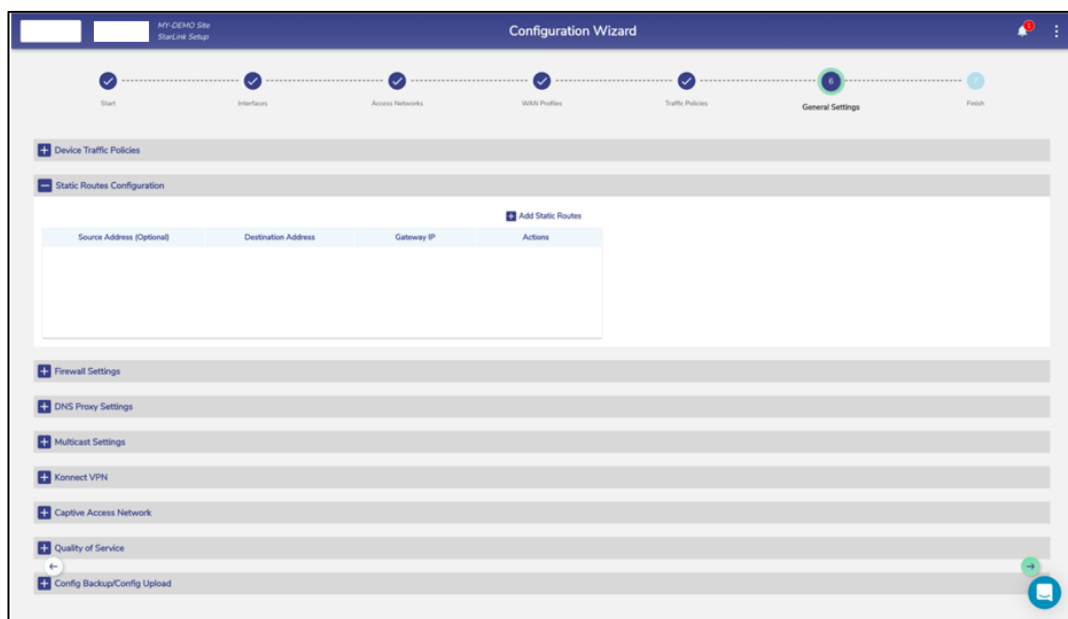


Figure 3.102 Static Route Configuration

- Click **Add Static Routes**. The route section becomes available, see figure below.

The screenshot shows a window titled "Static Routes Configuration". In the top right corner, there is a button labeled "Add Static Routes". Below this, there is a table with four columns: "Source Address (Optional)", "Destination Address", "Gateway IP", and "Actions". The first row of the table contains example values: "eg. 192.168.10.5/24" for Source Address, "eg. 192.168.30.10/24" for Destination Address, "eg. 192.168.10.1" for Gateway IP, and a green checkmark icon for Actions.

Figure 3.103 Add Static Route

- To enter data in the respective fields, see Table below.


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	<p>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.</p> <table> <tr> <td>Source Address (Optional)</td><td>92.168.10.5/24</td></tr> <tr> <td>Destination Address</td><td>192.168.10.5/24</td></tr> <tr> <td>Gateway IP</td><td>192.168.10.1</td></tr> </table> <p>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.</p>	Source Address (Optional)	92.168.10.5/24	Destination Address	192.168.10.5/24	Gateway IP	192.168.10.1
Source Address (Optional)	92.168.10.5/24						
Destination Address	192.168.10.5/24						
Gateway IP	192.168.10.1						
Action	Click  .						


Table 3-22 Static Route

The static route is configured.

3.5.3 Firewall Settings

To configure the firewall, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click **Firewall Settings**. The **Firewall Settings** section becomes available, see figure below.

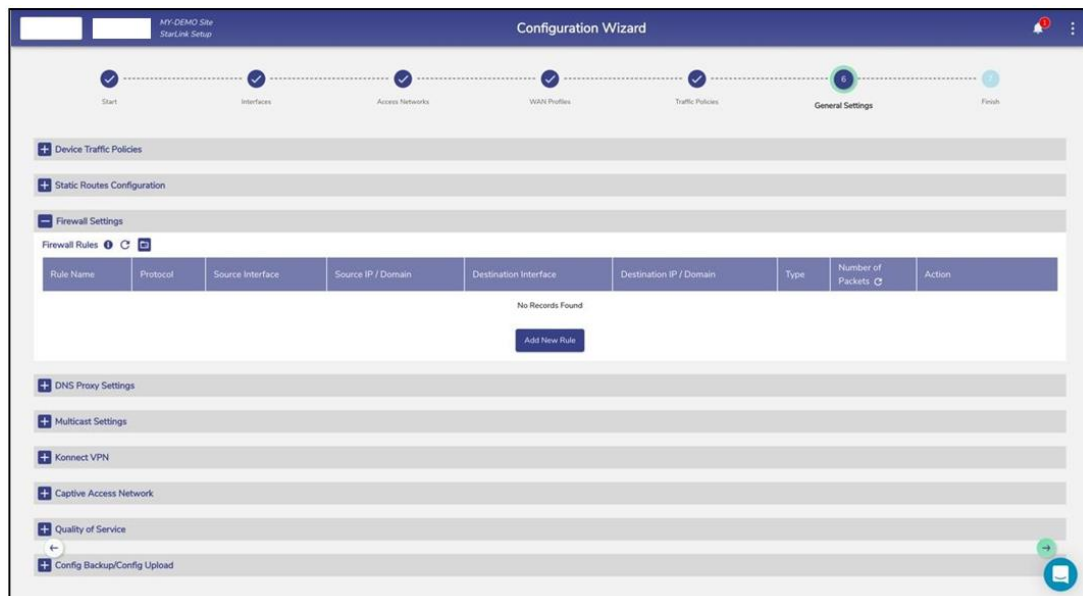


Figure 3.104 Firewall Settings

- Click **Add New Rule**. The **Add New Rule** section appears, see figure below.

The screenshot shows the 'Configuration Wizard' interface with the 'General Settings' step selected. Below the wizard steps, there are sections for 'Device Traffic Policies', 'Static Routes Configuration', and 'Firewall Settings'. The 'Firewall Settings' section is expanded, showing a table with columns: Rule Name, Protocol, Source Interface, Source IP / Domain, Destination Interface, Destination IP / Domain, Type, Number of Packets, and Action. A 'No Records Found' message is displayed below the table, with an 'Add New Rule' button. Below the table, the 'Add New Rule' form is visible, showing fields for Rule Name, Protocol (Any), Source (All), Destination (All), and Action (Allow/Deny). The 'Add New Rule' button is at the bottom right of the form.

Figure 3.105 Add New Rule Firewall Settings

The screenshot shows the 'Add New Rule' form for Firewall Settings. The form has a title bar 'Add New Rule' and a close button. Below the title bar, there is a section 'New Firewall Rule' with a blue header. The form contains the following fields: Rule Name (text input), Protocol (dropdown menu with 'Any' selected), Source (dropdown menu with 'All' selected, Type: Domain Name, Domain Name: eg. google.com, Port: From: 443, To: 443), Destination (dropdown menu with 'All' selected, Type: Domain Name, Domain Name: eg. google.com, Port: From: 443, To: 443), and Action (radio buttons for Allow and Deny). A 'Save' button is at the bottom right of the form.

Figure 3.106 Add New Firewall Domain Rule

- To enter data in the respective fields, see table below.

Fields	Configuration		
Rule Name	Enter the unique name of the rule. The name can include alphanumeric and special characters.		
Protocol	<p>In the Protocol list, click one of the following protocols that apply to the rule.</p> <ul style="list-style-type: none"> Any. This indicates that any protocol will apply to the firewall rule. By default, Any protocol is available. If user selects Any protocol, then they cannot specify the port number range. TCP. This is a reliable and connection-centric communication protocol. UDP. This is the transport layer protocol. The UDP is unreliable and does not establish a connection before the data transfer. 		
Source	<p>In the WANs and networks list, click the source device to which the rule is applicable.</p> <p>To apply the rule to entire WANs and networks, click All.</p>		
	Type	Select the type, IP Address or Domain Name .	
		If the Type selected is 'IP Address', then the following fields will be available for update.	
		IP	Enter the IP address of the device for which the rule is applied.
		Mask	In the Mask list, click the mask.
		Port From	Enter the port number.
		To	Enter the port number.
		If the Type selected is 'Domain Name', then the following fields will be available for update.	
		Domain Name	Enter the Domain Name of the device for which the rule is applied.

		Port From	Enter the port number.
		To	Enter the port number.
Destination	In the WANs and networks list, click the destination device to which the rule is applicable.		
	To apply the rule to entire WANs and networks, click All .		
	Type	Same as fields in Source field.	
Action	Click one to the following action.		
	<ul style="list-style-type: none">• Allow. To allow the firewall settings, click Allow.• Deny. To deny the firewall settings, click Deny.		


Table 3-23 Add New Rule

- Click **Save**.

The rules are displayed under the **Firewall Rules** section, see figure below.

Firewall Rules ⓘ									
Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets	Action	
Rule 1	TCP	VSWT-1	10.168.201.6	VSWT-2	10.168.201.25	Allow	6601	<input checked="" type="checkbox"/>	T1
Rule 2	TCP	VSWT-1	10.168.201.65	VSWT-2	10.168.201.87	Allow	0	<input checked="" type="checkbox"/>	T1


Figure 3.107 Firewall New Rules


If multiple rules are added, then the drag icon  is displayed. By default, highest priority is assigned to the top rule and the priority decreases down the rule list. However, user can prioritize the rule by using the drag icon.

If the user allows the firewall rule, then **Allow** is displayed under the **Type** section.

If user deny the firewall rule, then **Deny** is displayed under the **Type** section.

For details about the firewall rules, point the mouse to ⓘ next to the **Firewall Rules**. The **Firewall Rules** pop-up window appears, see **Figure 3.108 Firewall Rules**

Info To refresh the firewall rules, click on the  icon, see **Figure 3.109 Firewall**

Refresh To copy the firewall rules from a Configuration Backup, click on , see **Figure 3.110 Firewall Upload Config from Backup**. This will take the user to the Configuration Upload section where they can select the configuration to be uploaded.

Once this is done, the Firewall Configuration will automatically reflect in the Firewall Rules table.

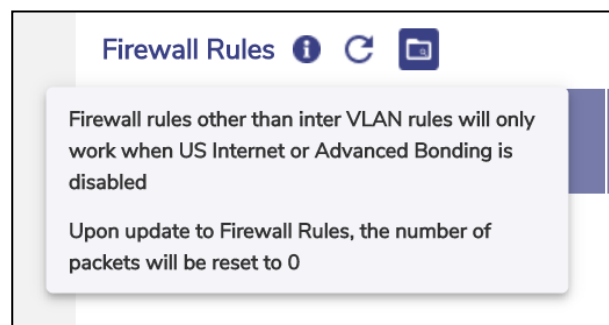


Figure 3.108 Firewall Rules Info

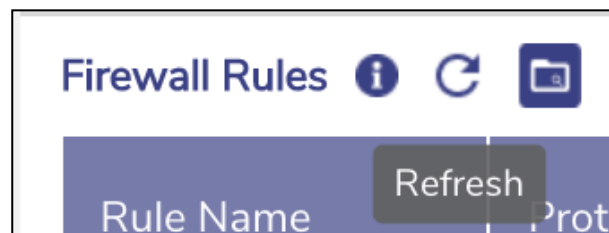


Figure 3.109 Firewall Refresh

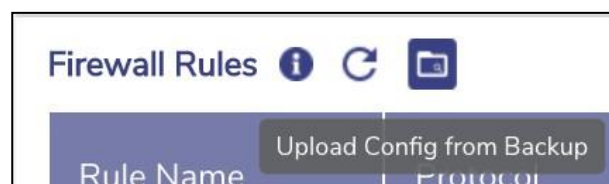




Figure 3.110 Firewall Upload Config from Backup

3.5.3.1 Modifying Firewall Rule

To modify the firewall rule, perform the following steps.

Steps

- Click  corresponding to the firewall rule is to be modified, see figure below.







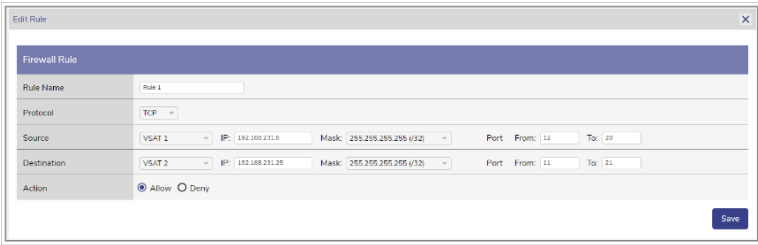
Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets	Action
Rule 1	TCP	VSIAT 1	192.168.231.6	VSIAT 2	192.168.231.25	Allow	6691	  T1
Rule 2	TCP	VSIAT 1	192.168.231.65	VSIAT 2	192.168.231.87	Allow	0	  T1

Figure 3.111 Firewall Rules List

- The **Edit Rule** section appears, see figure below.



Firewall Rule

Rule Name: Rule 1

Protocol: TCP

Source: VSIAT 1 IP: 192.168.231.6 Mask: 255.255.255.255 (/32) Port: From: 11 To: 20

Destination: VSIAT 2 IP: 192.168.231.25 Mask: 255.255.255.255 (/32) Port: From: 11 To: 21

Action: ☒ Allow ☐ Deny

Save

Figure 3.112 Edit Firewall Rules

- To enter data in the respective fields, see [Table 3-23 Add New Rule](#).
- Click **Save**.


The rules are displayed under the Firewall Rules section, see [Figure 3.111 Firewall Rules List](#).

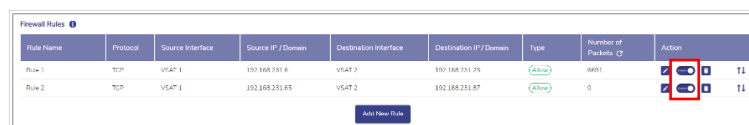
3.5.3.2 Disabling Firewall Rule

By default, the firewall rule is enabled.

To disable the firewall rule, perform the following steps.

Steps

- Click  corresponding to the firewall rule is to be modified, see figure below.



Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets	Action
Rule 1	TCP	VSWT 1	192.168.231.8	VSWT 2	192.168.231.25	Allow	8881	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Rule 2	TCP	VSWT 1	192.168.231.85	VSWT 2	192.168.231.87	Allow	0	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable

Figure 3.113 Enable/Disable Toggle Firewall Rules

- The **Disable Firewall Rule** pop-up window appears, see figure below.

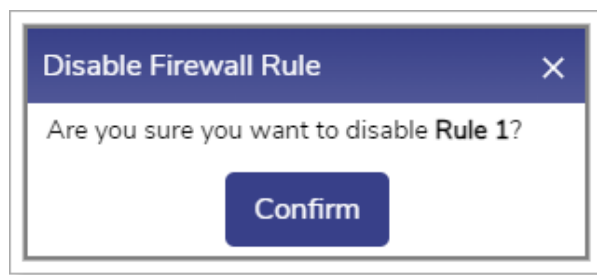


Figure 3.114 Disable Firewall Rule Pop-up

- Click **Confirm**.

The firewall rule is disabled.

3.5.3.3 Enabling Firewall Rule

The user can enable the disabled firewall rule.

To enable the firewall rule, perform the following steps.

Steps


- Click  corresponding to the disabled firewall rule. The **Enable Firewall Rule** pop-up window appears, see figure below.



Figure 3.115 Enable Firewall Pop-up

- Click Confirm.



The firewall rule is enabled and implemented.

3.5.3.4 Deleting Firewall Rule

To delete the firewall rule, perform the following steps.

Steps

- Click  corresponding to the firewall rule is to be deleted, see figure below.

Firewall Rules 0									
Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets (2)	Action	
Rule 1	TCP	VSAT 1	102.168.231.6	VSAT 2	102.168.231.25	Allow	6681		T1
Rule 2	TCP	VSAT 1	102.168.231.65	VSAT 2	102.168.231.97	Allow	0		T1

[Add New Rule](#)

Figure 3.116 Delete Firewall Rule Icon

- The Delete Firewall Rule pop-up window appears, see figure below.

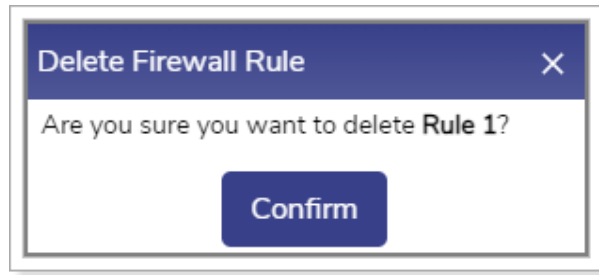


Figure 3.117 Delete Firewall Rule Pop-up


- Click **Confirm**.









The firewall rule is deleted.

3.5.3.5 Defining New Priority of the Firewall Rules

To define the new priority of the firewall rule, perform the following steps.


Steps

- Click  corresponding to the firewall rule whose priority is to be re-configured, see figure below.

Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets (s)	Action
Rule 1	TCP	VSWAN 1	100.168.231.6	VSWAN 2	100.168.231.25	Allow	6681	   
Rule 2	TCP	VSWAN 1	100.168.231.65	VSWAN 2	100.168.231.87	Allow	0	   

[Add New Rule](#)

Figure 3.118 Defining New Priority of the Firewall Rules Icon

- Hold the icon  and drag the firewall rule based on the priority is to be assigned.

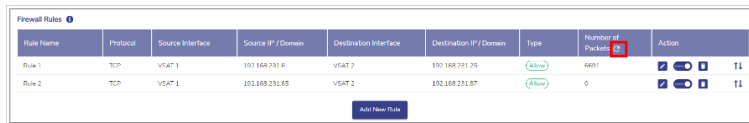
The new priority of the firewall rule is configured.







3.5.3.6 Resetting the Number of Packets

To reset the number of packets, perform the following steps.

Steps

- Click  in the **Number of Packets** section, see figure below.



Rule Name	Protocol	Source Interface	Source IP / Domain	Destination Interface	Destination IP / Domain	Type	Number of Packets	Action
Rule 1	TCP	VSWT 1	192.168.231.6	VSWT 2	192.168.231.25	(Allow)	6661	   T1
Rule 2	TCP	VSWT 1	192.168.231.65	VSWT 2	192.168.231.87	(Allow)	0	   T1

[Add New Rule](#)

Figure 3.119 Resetting the Number of Packets Icon

- The **Reset Counters** pop-up window appears, see figure below.

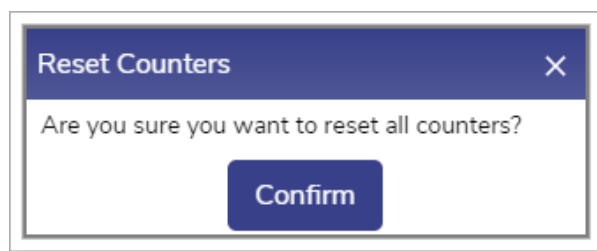


Figure 3.120 Reset Counter Pop-up

- Click **Confirm**.


The entire counter is reset.

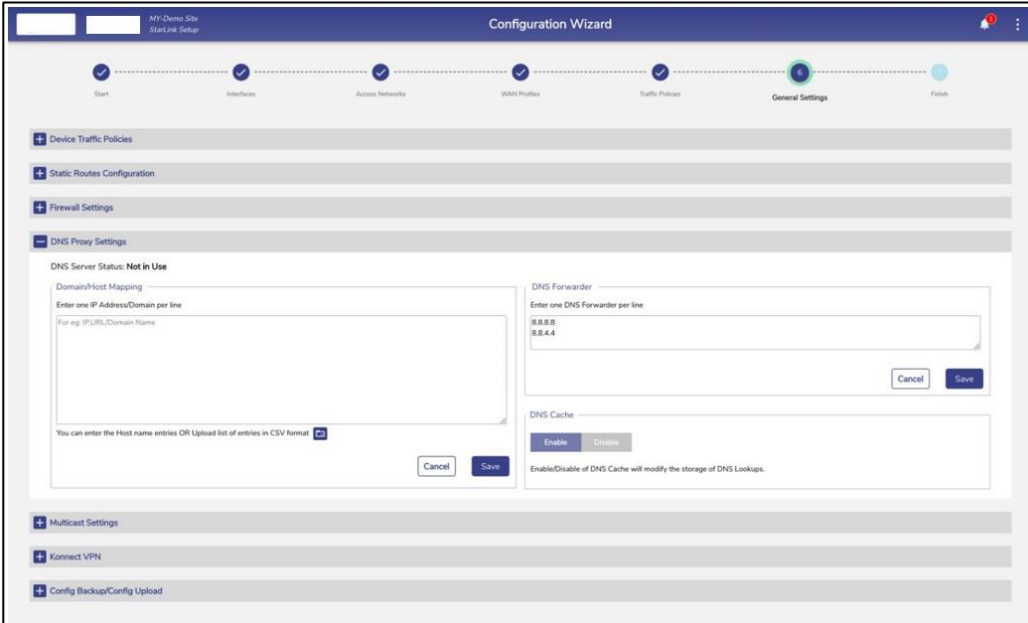
3.5.4 DNS Proxy Settings

3.5.4.1 Configuring DNS Proxy Settings

To configure the DNS proxy settings, perform the following steps.

Steps



- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click **DNS Proxy Settings**. The **Domain/Host Mapping**, **DNS Forwarder**, and **DNS Cache** sections become available, see figure below.



The screenshot shows the 'Configuration Wizard' interface with the 'General Settings' step highlighted. The 'DNS Proxy Settings' section is expanded, revealing three sub-sections: 'Domain/Host Mapping', 'DNS Forwarder', and 'DNS Cache'. The 'Domain/Host Mapping' section includes a text area for entering IP Address/Domain per line, with a hint 'For eg: IP/URL/Domain Name'. The 'DNS Forwarder' section has a text area for entering one DNS Forwarder per line, with a hint '8.8.8.8' and '8.8.4.4'. The 'DNS Cache' section has an 'Enable' button and a 'Disable' button, with a note 'Enable/Disable of DNS Cache will modify the storage of DNS Lookups.'.

Figure 3.121 DNS Proxy Settings

- To enter data in the respective fields, see table below.

Fields	Description	Configuration
DNS Server Status	If any Access Network is using the DNS proxy, then the status In Use is displayed.	<p>To configure the DNS proxy, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click Access Networks. The Access Networks page appears, see Figure 3.40 Access Networks. Click  corresponding to the network under the Action section on the Access Networks page. The Updated Connected Network page appears, see Figure 3.53 Update Connected Network. Enter the DHCP Gateway IP address in the DNS Server IP field under the DHCP Settings section. Click Save. The network is updated, and a successful message is displayed, see Figure 3.122 Network Updated Successfully. Click OK. The status In Use is displayed, see Figure 3.123 DNS Server In Use. By default, the status Not In Use is displayed.
	If the Access Network is not using the DNS proxy, then the status Not in Use is displayed.	<p>To remove the DNS proxy, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click Access Networks. The Access Networks page appears, see Figure 3.40 Access Networks. Click  corresponding to the network under the Action section on the Access Networks page. The Updated Connected Network page appears, see Figure 3.53 Update Connected Network. Delete the DHCP Gateway IP address in the DNS Server IP field under the DHCP Settings section.


		<ul style="list-style-type: none"> • Or, • Enter 8.8.8.8 in the DNS Server IP field under the DHCP Settings section. • Click Save. The network is updated, and a successful message is displayed, see Figure 3.122 Network Updated Successfully. • Click OK. <p>The status Not In Use is displayed, see Figure 3.124 DNS Server Not in Use.</p>
Domain/Host Mapping		<p>Enter an IP address and suffix domain on a single line.</p> <p>Click Save.</p> <p>Or,</p> <p>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,</p> <p>The user 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.</p> <p>Click Save.</p>
DNS Forwarder		<p>Enter only one DNS forwarder on every line.</p> <p>Click Save.</p>
DNS Cache		<p>To enhance the DNS lookups, click Enable.</p>

Table 3-24 DNS Proxy Settings

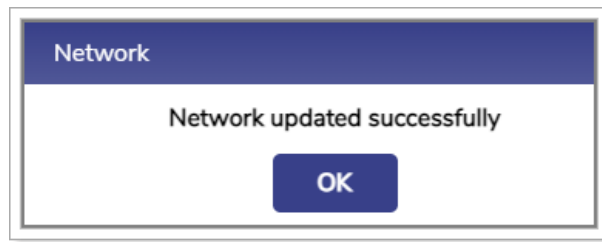


Figure 3.122 Network Updated Successfully

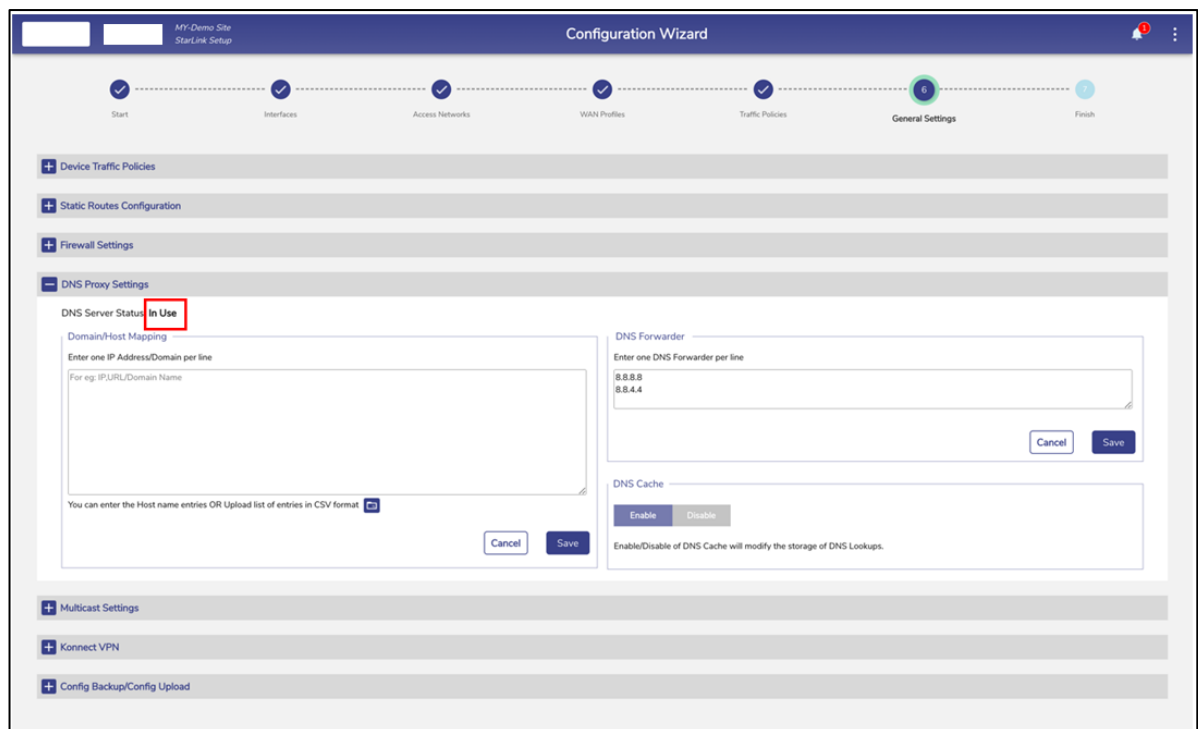


Figure 3.123 DNS Server In Use

The screenshot shows the 'Configuration Wizard' interface with a progress bar at the top indicating steps: Start, Interfaces, Access Networks, WAN Profiles, Traffic Policies, General Settings (current), and Finish. The 'General Settings' section is expanded, showing various configuration options. Under 'DNS Proxy Settings', the 'DNS Server Status' is set to 'Not in Use', which is highlighted with a red box. Below this, there are two main sections: 'Domain/Host Mapping' and 'DNS Forwarder'. The 'Domain/Host Mapping' section has a text area for entering IP Address/Domain per line, with a hint 'For eg: IP:URL/Domain Name'. The 'DNS Forwarder' section has a text area for entering one DNS Forwarder per line, with the example '8.8.8.8' and '8.8.4.4' entered. Below these sections, there is a 'DNS Cache' section with 'Enable' and 'Disable' buttons. At the bottom of the wizard, there are sections for 'Multicast Settings' and 'Config Backup/Config Upload'.

Configuration Wizard

Start Interfaces Access Networks WAN Profiles Traffic Policies General Settings Finish

+ Device Traffic Policies

+ Static Routes Configuration

+ Firewall Settings

- DNS Proxy Settings

DNS Server Status **Not in Use**

Domain/Host Mapping

Enter one IP Address/Domain per line

For eg: IP:URL/Domain Name

You can enter the Host name entries OR Upload list of entries in CSV format

Cancel Save

DNS Forwarder

Enter one DNS Forwarder per line

8.8.8.8
8.8.4.4

Cancel Save

DNS Cache

Enable Disable

Enable/Disable of DNS Cache will modify the storage of DNS Lookups.

+ Multicast Settings

+ Config Backup/Config Upload

Figure 3.124 DNS Server Not in Use

The DNS proxy is configured.

3.5.5 Multicast Settings


By default, multicast traffic is enabled on all networks available under the Access Networks. Multicast traffic is efficient as the server sends the data packets and the switches and routers only forward the data packets to the group of recipients. Therefore, the load over the server and the network traffic decreases.

The user can disable and enable the multicast traffic on one or multiple networks.

3.5.5.1 Disabling the Multicast Traffic

To disable multicast traffic on the Access Networks, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click **Multicast Settings**. The multicast traffic section becomes available, see figure below.

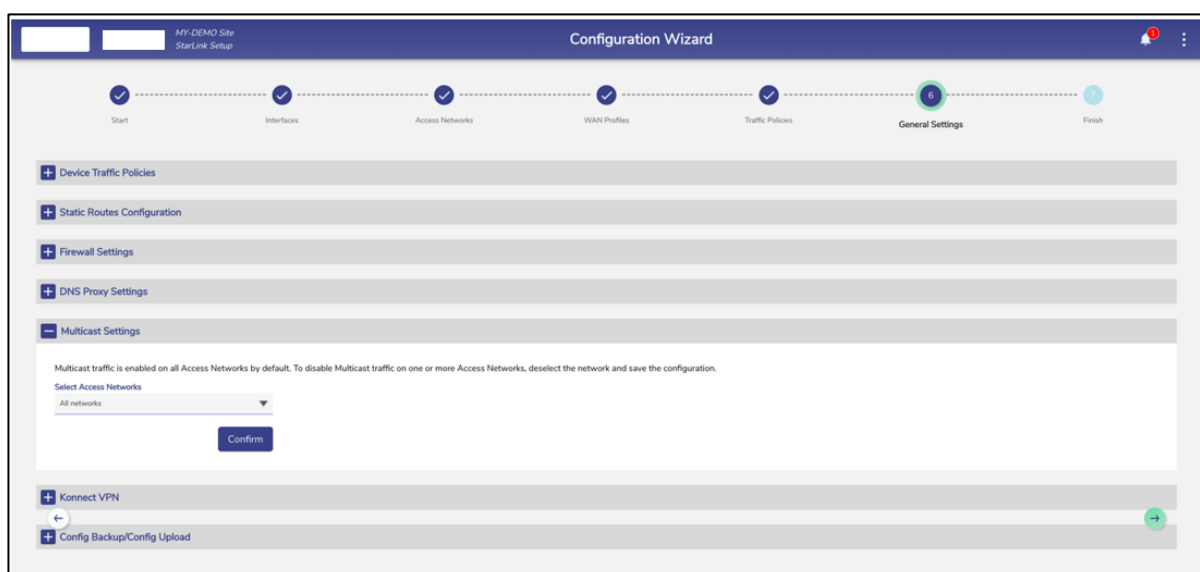


Figure 3.125 Multicast Settings

- In the **Access Networks** list, clear the network check boxes whose multicast traffic is to be disabled.

By default, all networks are selected, and the name of the selected networks is displayed under the **Select Access Networks** section, see figure below.

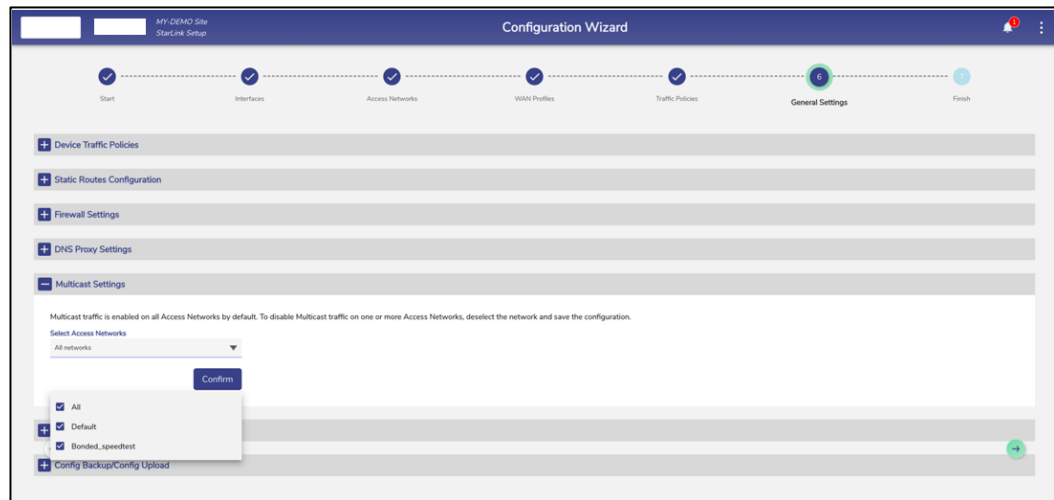


Figure 3.126 Select Access Network


- Click **Confirm**.

Multicast traffic on the deselected Access Network is disabled.

3.5.5.2 Enabling the Multicast Traffic

To enable multicast traffic on the Access Network, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click Multicast Settings. The multicast traffic section becomes available, see [Figure 3.125 Multicast Settings](#).
- In the **Access Networks** list, select the network check boxes whose multicast traffic is to be enabled.
- Click **Confirm**.

Multicast traffic on the Access Networks is enabled.

3.5.6 Konnect VPN


Konnect VPN allows the EdgeOS System to VPN access networks to a Konnect VPN Server; this is most utilized between EdgeOS Systems. The configuration involves the following steps.

- Creation of the VPN Client profile. The user needs to provide an Alias name for the Client and Access Network/subnet which is allowed from the client. Once the New client is created the Client configuration can be downloaded.
- Downloading of the client configuration from the server and applying the configuration by clicking the “New Connection” on the Konnect VPN Client end point.
- Configuring Konnect VPN on an Access Network, for details see [3.2.7 Configuring Konnect VPN](#).

Note: The above steps just create the Konnect VPN tunnel between the end points. To route the Access Network traffic through the VPN, edit the Access Network configuration to pick the configured VPN end point to route. See [Table 3-16 Connected Network Information](#).

To access the Konnect VPN section, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click Konnect VPN. The Konnect VPN section becomes available, see [Figure 3.127 Konnect VPN Settings](#).
- This section has two sub sections – **Konnect VPN Server** and **Konnect VPN Client**.

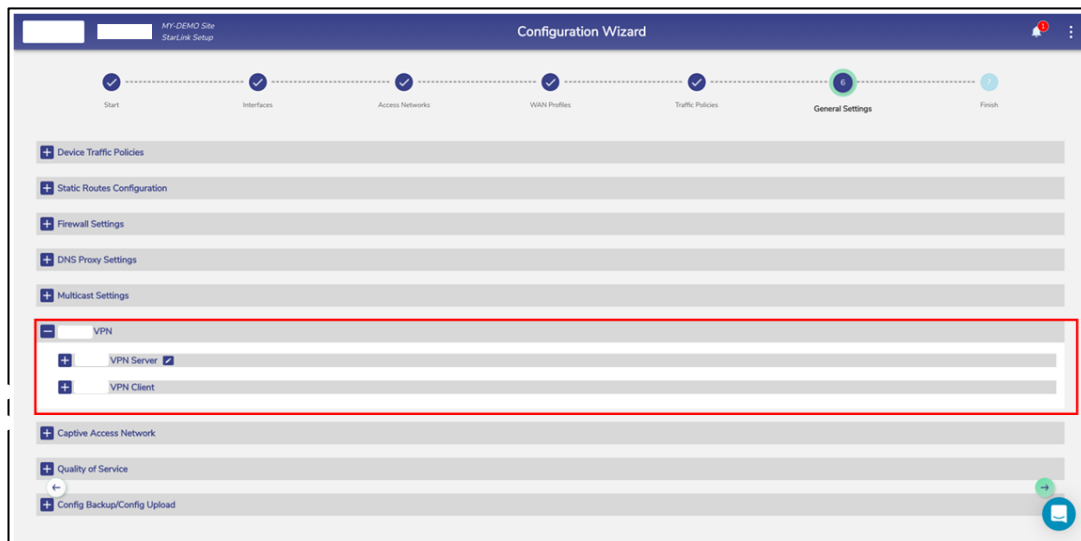



Figure 3.127 Konnect VPN Settings

Konnect VPN server needs the Public IP Address and the Listening Port to be configured. The Public IP Address must be fetched from the Internet gateway where the EdgeOS System is connected, and the port forwarding must be enabled on the gateway as well.

3.5.6.1 Konnect VPN Server Settings

To do Konnect VPN Server settings, perform the following steps.

Steps

- Click  next to Konnect VPN Server. Pop-up as seen [Figure 3.128 Konnect VPN Server Settings](#) in appears.
- Enter the Public IP Address or the Hostname of the Server.
- Enter the port for the Konnect VPN server.
- Click Save. See [Figure 3.129 Konnect VPN Server Settings Pop-up](#) as example VPN Server settings.

VPN Server Settings

Hostname / IP Address
eg. myoffice.com

Port
eg. 2022

Incase of any modifications to these settings, the client configurations will be regenerated.
These will need to be downloaded again on the client.

Cancel Save

Figure 3.128 Konnect VPN Server Settings

VPN Server Settings

Hostname / IP Address
108.232.84.254

Port
7000

Incase of any modifications to these settings, the client configurations will be regenerated.
These will need to be downloaded again on the client.

Cancel Save

Figure 3.129 Konnect VPN Server Settings Pop-up

3.5.6.2 Adding a new VPN Client


To add a new VPN client, perform the following steps.

Steps

- Click the Konnect VPN Server section.
- Click **+** New Client button on the top right, see [Figure 3.130 Konnect VPN Server Section](#) Add New Client Pop-up appears, see [Figure 3.131 Add New Client Pop-up](#).
- Enter Client Alias Name, i.e., a name for the new client.

- Enter the subnet(s) for the new client. The user can enter one or more subnets, which are comma separated but without spaces. Onboard networks should be used for this purpose.
- Click **Save**.

The client details appear in the table listing the currently configured clients, see **Figure 3.132 Configured Clients Table** with each row having details of the Client Name, Creation Timestamp, Subnet(s), and Status.

The user can click on  to download the Connection File of each client by clicking the icon.

The user can click on  to delete client.



Figure 3.130 Konnect VPN Server Section

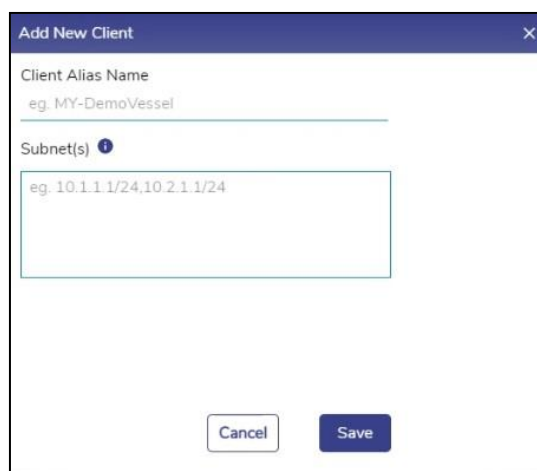


Figure 3.131 Add New Client Pop-up

Client Name	Timestamp	Subnet(s)	Status	Actions
Test123	2023-10-09 20:49:27	192.168.215/24	UP	

Figure 3.132 Configured Clients Table

3.5.6.3 Adding a New VPN Connection

To add New Connection, perform the following steps.

Steps

- Click the Konnect VPN Client section.
- Click New Connection button on the top right, see [Figure 3.133 Konnect VPN Client Section](#) Add New Connection Pop-up appears, see [Figure 3.134 Add New Connection](#)
- Enter Konnect VPN Server Alias Name, i.e., a client connection name.
- Select a WAN Profile to apply this connection to. Note that the selected WAN profile should not have any bonded set.
- Click the to upload the Connection File obtained from the server.
- Click **Save**.

The configured client connection details appear in the table listing the currently configured client connection table, see [Figure 3.135 Configured Connections Table](#) with each row having details of the Server Connection Name, Creation Timestamp, Subnet(s), Hostname/IP Address, Port, Server Public Key, WAN Profile and Status.

The user can click on to edit the client connection. Only Connection Name and WAN Profile are editable, see [Figure 3.136 Edit Client Connection](#). Click on to save the changes or to discard them.

The user can click on to delete client connection.

Server Connection Name	Timestamp	Subnet(s)	Hostname / IP Address	Port	Server Public Key	WAN Profile	Status	Actions
No Records Found								

Figure 3.133 Konnect VPN Client Section

Figure 3.134 Add New Connection

Server Connection Name	Timestamp	Subnet(s)	Hostname / IP Address	Port	Server Public Key	WAN Profile	Status	Actions
Edge-01	2022-12-27 20:29:11	192.168.252.	198.212.84.254	7000	19c79pyn5adls...	Default	UP	

Figure 3.135 Configured Connections Table

Server Connection Name	Timestamp	Subnet(s)	Hostname / IP Address	Port	Server Public Key	WAN Profile	Status	Actions
Edge-01	2022-12-27 20:29:11	192.168.252.	198.212.84.254	7000	19c79pyn5adls...	Default	UP	

Figure 3.136 Edit Client Connection

3.5.7 Quality of Service

Quality of Service (QoS) settings provide flexibility to enable or disable Traffic Policies (Shaping and DPI), Usage statistics in the system. With QoS disabled, the system will not provide Traffic Policies, Client and Access Network usage, and DPI services. When QoS is enabled, the system performance is approximately halved. It is recommended if the EdgeOS System is performing Cellular/Satellite GW services only, then it makes good sense to disable QoS to improve performance.

Note: During installation of EdgeOS System, QoS is enabled. Only users with administrative rights have access to this section and can disable QoS.

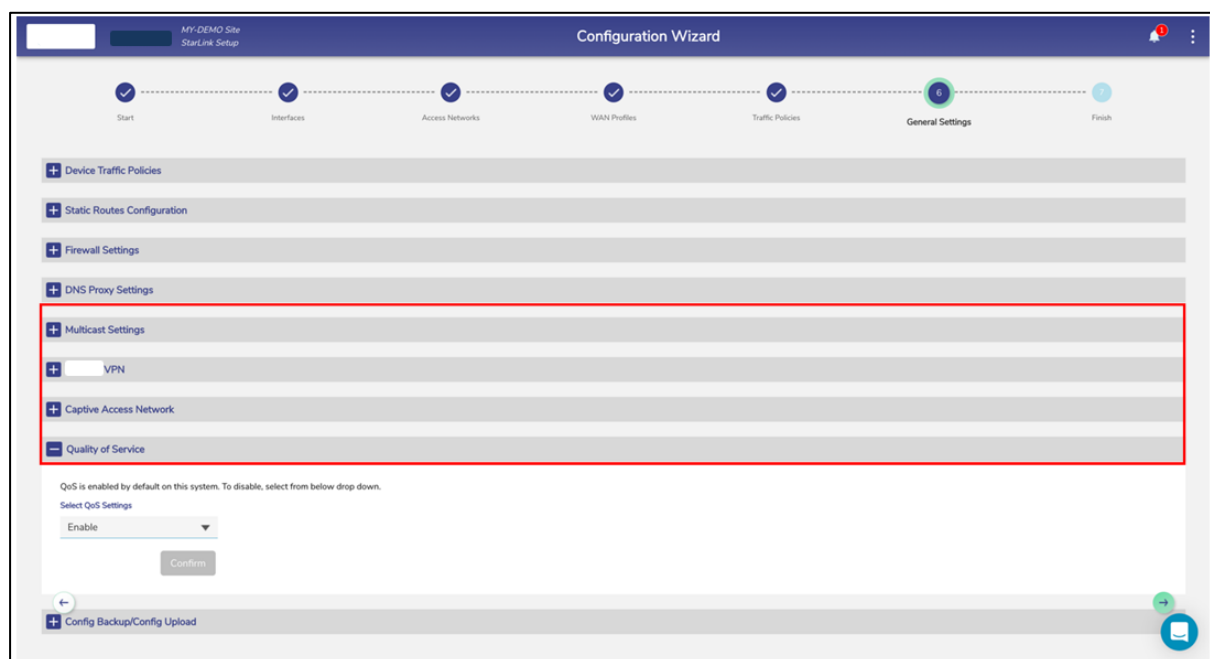



Figure 3.137 Quality of Service

3.5.7.1 Disabling QoS

To disable QoS, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click Quality of Service. The Quality-of-Service section becomes available, see [Figure 3.137 Quality of Service](#).
- From the drop down, select 'Disable' option. See [Figure 3.138 Quality of Service Disable](#).
- Click **Confirm**.

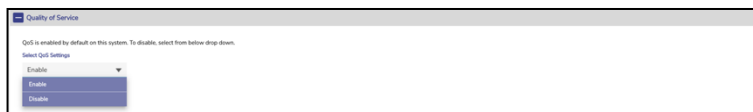


Figure 3.138 Quality of Service Disable

3.5.8 Config Backup/Config Upload

Running configuration of the EdgeOS System can be saved or applied/restored from the EdgeOS /Web portal from this section of the Configuration Wizard, see below.

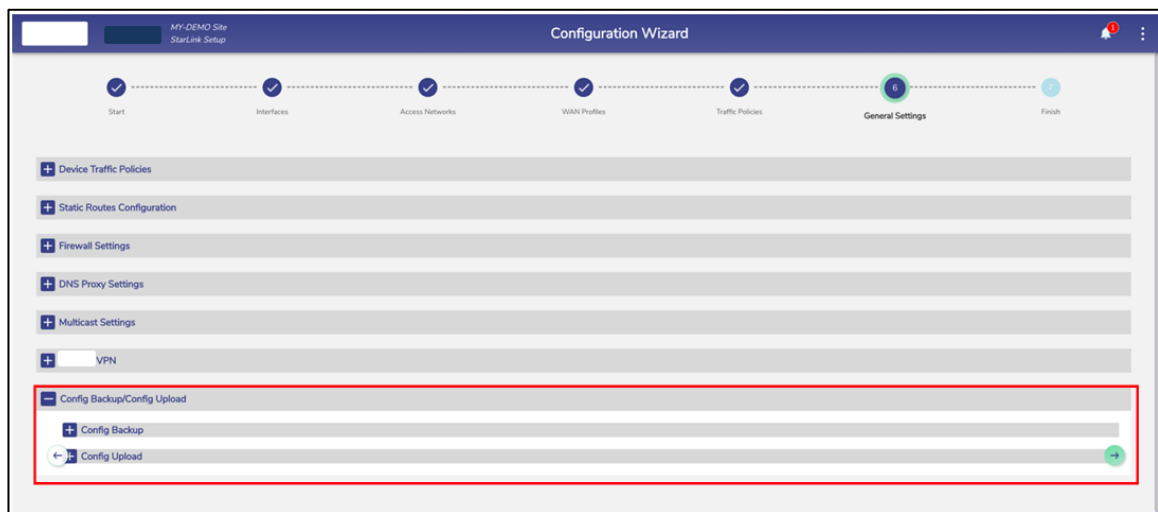



Figure 3.139 Config Backup/ Config Upload

3.5.8.1 Creating new Configuration Backup

To initiate a new Configuration backup, perform the following steps.

Steps

- Click  on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click Config Backup/Config Upload. The Config Backup/Config Upload section becomes available, see [Figure 3.139 Config Backup/ Config Upload](#).
- Click **Config Backup**. The Available Configuration Backups table becomes available. This table has listing of the prior backups that are available in the system. If there are no backups yet, this table will be empty. Below the table

there is a subsection, **Initiate New Configuration Backup**, see **Figure 3.140 Initiate New Configuration Backup**.

- Select Configuration Backup Type. Configurations are grouped as below. see **Figure 3.141 Select Configuration Backup Type**.
- All Configuration
- Interfaces - All the LAN/WAN interface configuration and WAN profiles
- Traffic Policies - All traffic policies, include Device policies.
- Networks - All Access Network configuration, including DHCP reservation.
- Firewall Rules
- After selecting the Configuration which needs to be backed up, user can add comments to identify the backup. This is an optional step.
- Click on **Start Backup** button.


Once the backup is ready, it will show in the available Configuration backups along with the backup type, user login through which the backup has been created and the time of backup creation, see **Figure 3.142** . By clicking the download icon  next to the Configuration back, the saved configuration can be transferred/saved to the local device.



Figure 3.140 Initiate New Configuration Backup



Figure 3.141 Select Configuration Backup Type

Available Configuration Backups				
Configuration Backup Name	Backup Type	User Name	Created On	Download
K8-03-999-a65554-2018279AAA...	All	edge	2022-11-23 17:49:22	
K8-03-999-a65554-2018279AAA...	All	edge	2022-11-23 17:49:05	
K8-03-999-a65554-2018279AAA...	All	edge	2022-11-23 17:28:39	
K8-03-999-a65554-2018279AAA...	Firewall Rules	edge	2022-11-23 17:28:28	
K8-03-999-a65554-2018279AAA...	Networks	edge	2022-11-23 17:28:25	
K8-03-999-a65554-2018279AAA...	Traffic Policies	edge	2022-11-23 17:28:20	
K8-03-999-a65554-2018279AAA...	Interfaces	edge	2022-11-23 17:28:15	
K8-03-999-a65554-2018279AAA...	All	edge	2022-11-23 17:27:47	

Figure 3.142 Available Config Backups


3.5.8.2 Uploading Configuration from Backup

To initiate a Configuration upload, perform the following steps.

Steps

- Click on the **Traffic Profiles** page or click **General Settings**. The **General Settings** page appears.
- Click Config Backup/Config Upload. The Config Backup/Config Upload section becomes available, see [Figure 3.139 Config Backup/ Config Upload](#).
- Click **Config Upload**. The Previous Configuration Uploads table becomes available. This table has listing of the prior uploads that have been done on the system. If there are no uploads, this table will be empty. Below the table there is a subsection, **Initiate New Configuration Upload**, see [Figure 3.143 Initiate New Configuration Upload](#).
- To initiate an upload, click on icon next to Initiate New Configuration Upload. Select a configuration from the list of backed up configurations. The selected configuration will appear next to the upload icon, see [Figure 3.144 Upload Configuration](#).
- Click **Apply Configuration** button. The configuration upload will be initiated and will take a few minutes, see [Figure 3.145 Apply Configuration](#) Once configuration is applied, the services will be restarted and corresponding message will be visible, see [Figure 3.146 Apply Configuration Intermediate Step](#). The uploaded configuration will also be visible in the Uploads table. The last

step will be to reboot the server to apply the configuration, see [Figure 3.147 Apply Configuration Reboot Server](#).

- Click Reboot icon . A confirmation Pop-up will be available, see [Figure 3.148 Reboot Confirmation](#). Click Confirm to reboot the server. Once the server comes up, the configuration will be uploaded on the system.

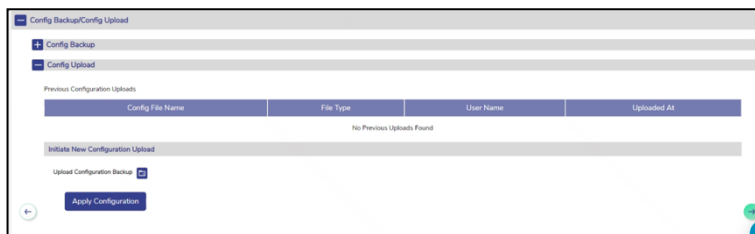


Figure 3.143 Initiate New Configuration Upload

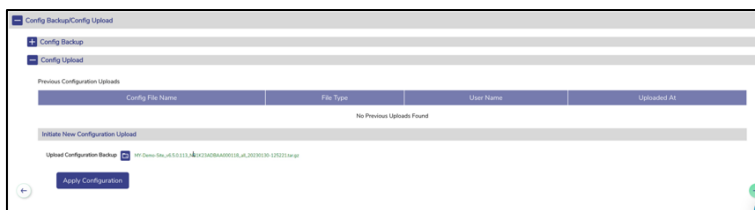


Figure 3.144 Upload Configuration

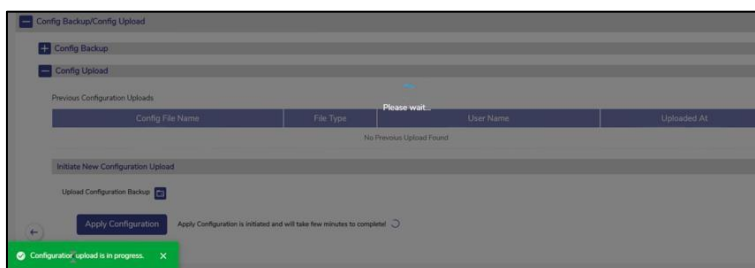


Figure 3.145 Apply Configuration

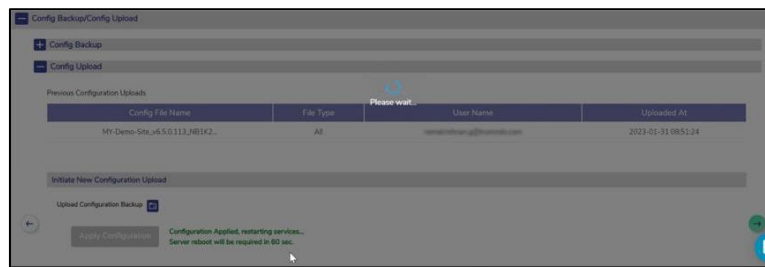


Figure 3.146 Apply Configuration Intermediate Step

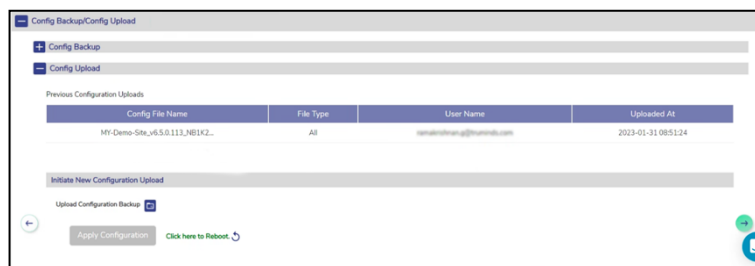


Figure 3.147 Apply Configuration Reboot Server

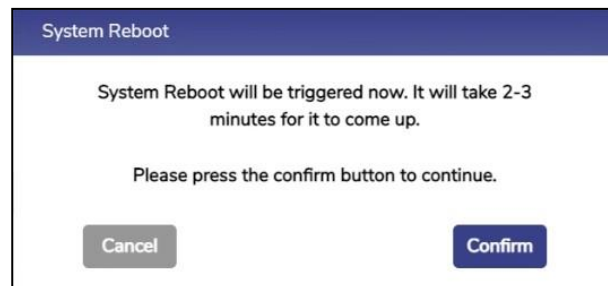


Figure 3.148 Reboot Confirmation

This completes the General Settings of the EdgeOS System.

4 Monitoring EdgeOS System

The user can monitor the Alerts, Internet Status, Performance, Network Usage, Speeds, and device location through the EdgeOS System Portal.

4.1 Monitoring Alerts

System alerts are raised in various scenarios. Some examples are:

- Active Internet Source becomes unavailable.
- Network/Device consumption exceeds thresholds.
- Traffic is pause on a Network/Device/Enterprise User.
- Any configuration is updated through the Configuration Wizard.


Following are the severity levels of the system alerts.

- Critical
- Major
- Minor
- Info
- Warning

4.1.1 Viewing Alerts

To view the alerts, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the bell icon .
- The **Notifications** pop-up window appears. See figure below.

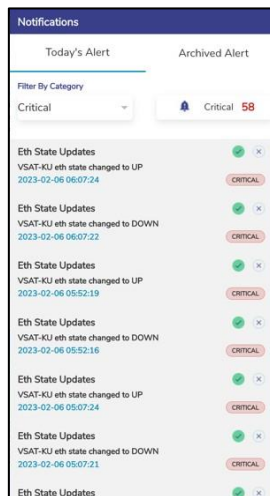


Figure 4.1 Notification Pop-up

- The count of alerts is displayed over the bell icon, see figure below.

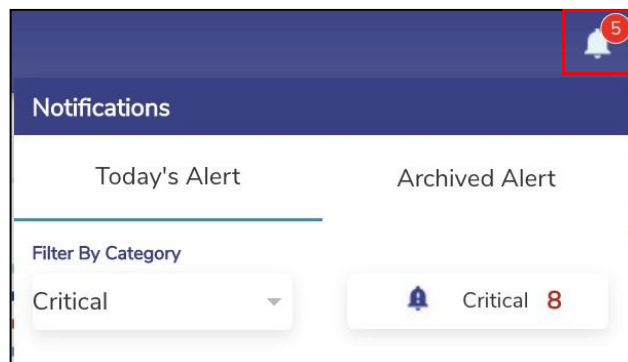


Figure 4.2 Notification Count

- Click **Today's Alert**. The current day alerts will become available under the **Today's Alert** tab.
- The user can filter the alerts based on the severity levels. For this, click the drop-down arrow under the **Filter By Category** section see **Figure 4.3 Filter by**

Category Drop-Down. Details of the alerts are displayed. In addition to this, the count of the alerts based on the severity level is displayed.

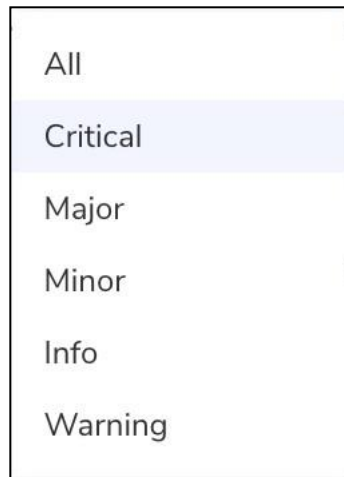




Figure 4.3 Filter by Category Drop-Down

- Click **Archived Alerts**. Alerts up to previous 30 days are available under this tab.

4.1.2 Clearing an Alert

To clear an alert, perform the following steps.



Steps

- Log on to the EdgeOS System. The home page appears.
- Click the bell icon .
- The **Notifications** pop-up window appears.
- Click on Today's Alerts.
- Click on  icon next to the alert that the user wants to clear or mark as fixed, see **Figure 4.1 Notification Pop-up**. This will still maintain the alert in the system.

4.1.3 Deleting an Alert

To delete an alert, perform the following steps.



Steps

- Log on to the EdgeOS System. The home page appears.
- Click the bell icon .
- The **Notifications** pop-up window appears.
- Click on Today's Alerts tab.
- Click on  icon next to the alert, see [Figure 4.1 Notification Pop-up](#). This will remove the alert from the system.

4.1.4 Clearing all Alerts

To clear archived alerts, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the bell icon .
- The **Notifications** pop-up window appears.
- Click on Archived Alerts tab.
- Click on  Clear All icon, see figure below. This will clear all previous day's alerts.

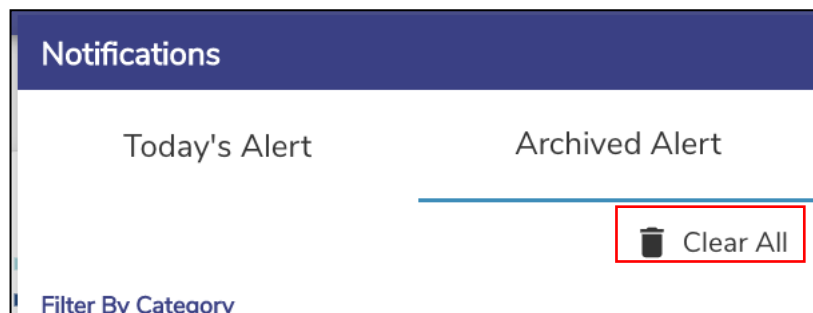


Figure 4.4 Clear All Notifications

4.2 System Information


The user can view and edit system details such as Site Name, Device details, Firmware details. Additionally, it is possible to upgrade the firmware through this Pop-up.

Note: Updating system information is possible only if the user has administrative rights.

4.2.1 Viewing System Information

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

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **System Info**. The **System Information** pop-up window appears, see figure below.









System Information	
Site Name	DemoSite 
Device Name	Starlink Setup 
Device Make	K4 Edge Server
Device Model	700-00040-000
Device S/N	ES1K27AAAAA000999
Firmware Version	6.5.0.119_67 
System Up Since	2023-01-25 20:29:44 

Figure 4.5 System Information

For details of the system information, see tables below.

Fields	Description	Configuration
Site Name	<p>This is the location name where the EdgeOS System is assigned to, this location is specified while registering the site.</p> <p>User can modify the Site Name.</p>	<p>A preinstalled server has a Location or Site Name assigned.</p> <p>To update Site Name of the server, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none">Click . The Update Site Name pop-up window appears, see Figure 4.6 Update Site Name.The current Site Name is displayed in the Current Site Name field.Enter the new Site Name in the New Site Name field.Click Save. <p>The system reboots automatically. Thereafter, the new Site Name is reflected.</p>
Device Name	<p>This name uniquely identifies the EdgeOS System.</p>	<p>A preinstalled server has a Device Name available.</p> <p>To update Device Name of the server, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none">Click . The Update Device Name pop-up window appears, see Figure 4.7 Update Device Name. <p>The current Device Name is displayed in the Current Device Name field.</p>

		<ul style="list-style-type: none"> Enter the new Device Name in the New Device Name field. Click Save. <p>Thereafter, the new Device Name is reflected within 60 seconds.</p>
Device Make	This identifies the hardware type of the Server.	N/A
Device Model	This identifies the part details of the EdgeOS System.	N/A
Device S/N	This identifies the serial number of the EdgeOS System.	N/A
Firmware Version	This identifies the firmware version currently installed on the server.	<p>The user can update the firmware installed on the server to the latest version if the current version is not latest. If the current version is same as latest version, then  icon is present next to the firmware version, see Figure 4.8 Updated Firmware Version. else  icon is present, see Figure 4.5 System Information.</p> <p>To update the firmware version, see section 4.2.2 Installing latest Firmware.</p>
System Up Since	<p>This identifies the date and time since the system is up.</p> <p>The user can modify the system up details.</p>	<p>To modify the system up details, perform the following steps.</p> <p>Steps</p>


		<ul style="list-style-type: none"> Click . The System Reboot pop-up window appears, see Figure 4.9 System Reboot. Click Confirm. <p>The system gets rebooted. Once the system is up, the new date and time are displayed.</p>
--	--	--

Table 4-1 System Information

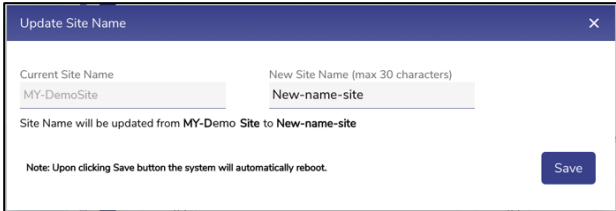


Figure 4.6 Update Site Name



Figure 4.7 Update Device Name

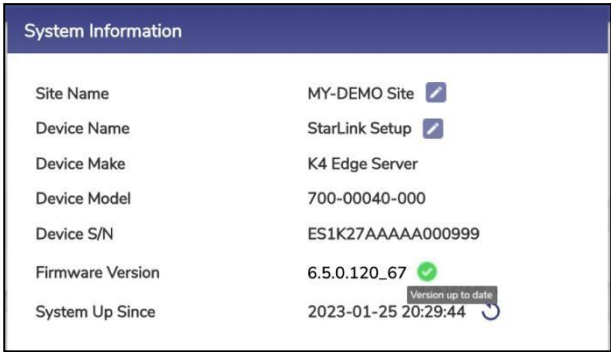


Figure 4.8 Updated Firmware Version

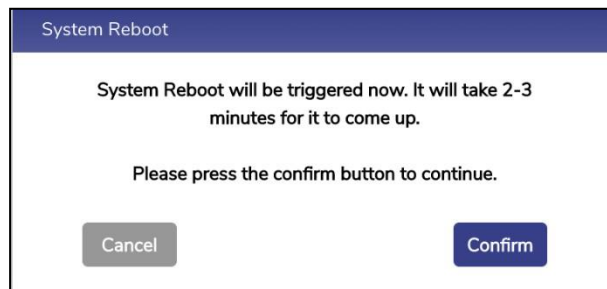


Figure 4.9 System Reboot

4.2.2 Installing latest Firmware

To download the latest firmware, perform the following steps.

Steps



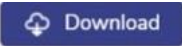
- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click the System Info. The System Info Pop-up appears.
- Click the  icon next to Firmware version.
- A new Pop-up with version details is available, see figure below.



Figure 4.10 New Update Available

- Click the  button to initiate the download. A Pop-up indicating that the download is in progress appears, this process may take few minutes to complete, see [Figure 4.11 Downloading latest version](#) . On successful completion of download, a new Pop-up with details of downloaded version appears, see [Figure 4.12 Download Successful](#).

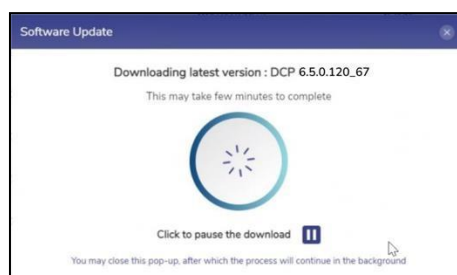


Figure 4.11 Downloading latest version

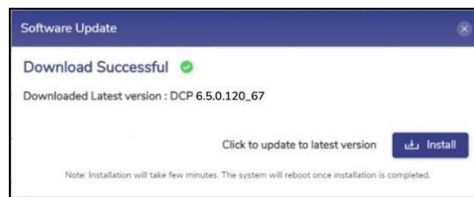


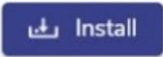


Figure 4.12 Download Successful

- To pause the process, click on  icon, see [Figure 4.11 Downloading latest version](#). To resume the process, click on  icon. The process resumes from where it was paused.
- Click the  button to initiate installation process, see [Figure 4.12 Download Successful](#). The installation process is initiated, see [Figure 4.13 Installation Initiation](#). Post installation completion, the server reboot is initiated automatically, see [Figure 4.14 Rebooting Server](#).
- Login to the server and check the firmware details on the System Info Pop-up. The version is now the latest available, see [Figure 4.16 Downloaded and Installed Firmware](#).

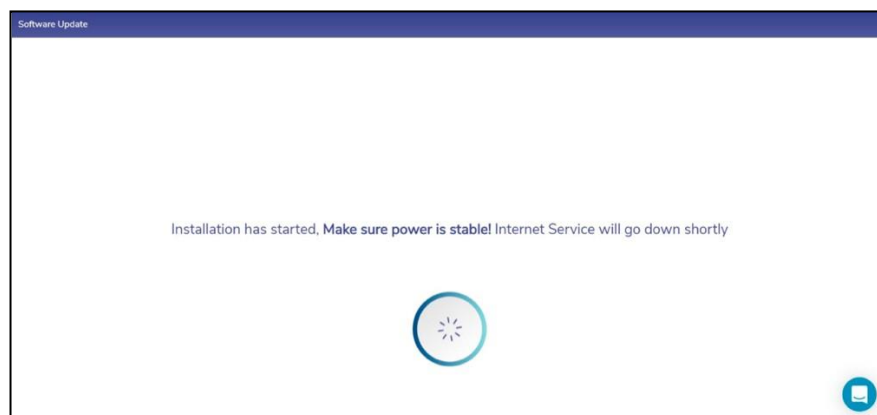


Figure 4.13 Installation Initiation

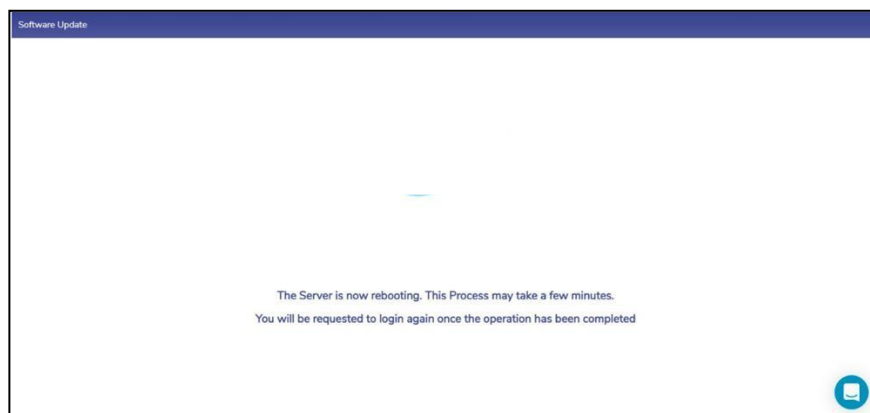


Figure 4.14 Rebooting Server

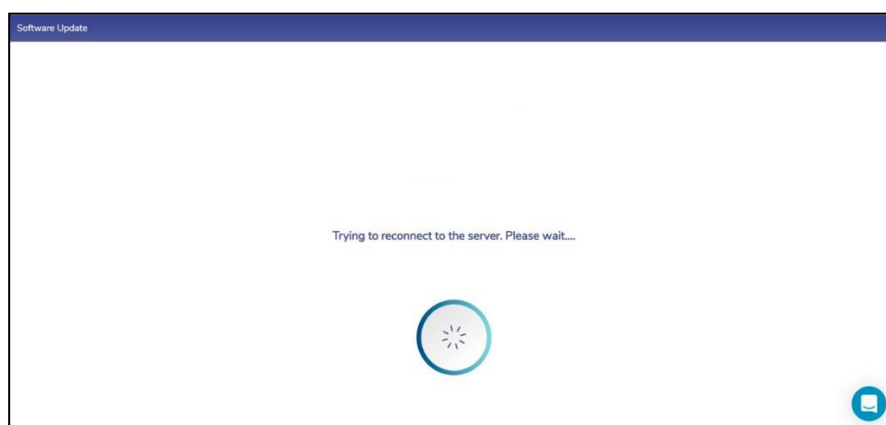


Figure 4.15 Reconnecting Server


System Information	
Site Name	MY-DEMO Site
Device Name	StarLink Setup
Device Make	K4 Edge Server
Device Model	700-00040-000
Device S/N	ES1K27AAAAA000999
Firmware Version	6.5.0.120_67
System Up Since	2023-01-25 20:29:44

Figure 4.16 Downloaded and Installed Firmware

4.2.3 Viewing System Uptime

To view the System Uptime, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click the System Info. The System Info Pop-up appears.
- The System Up Since field gives details of the System Uptime, see [Figure 4.17 System Information](#).
- To reboot the system, click on the icon. A confirmation popup appears, see [Figure 4.18 System Reboot](#).
- Click Confirm to proceed. The system will go for a reboot.

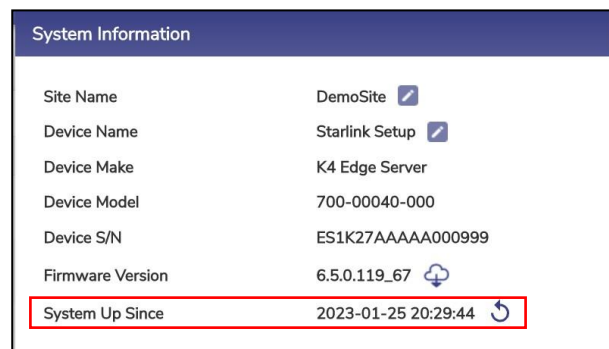


Figure 4.17 System Information



Figure 4.18 System Reboot

4.3 Manage Accounts

The user can create a user account and assign specific roles to access the EdgeOS applications. Additionally, they can also disable the user account, and change the login password with administrative rights. Other accounts will see Change Password option only in the menu.


Note: This menu item is visible to users with administrative rights.

4.3.1 Adding a User Account

The **Add Account** operation is available only for an administrator.

To add a user account, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Manage Accounts**, see figure below.

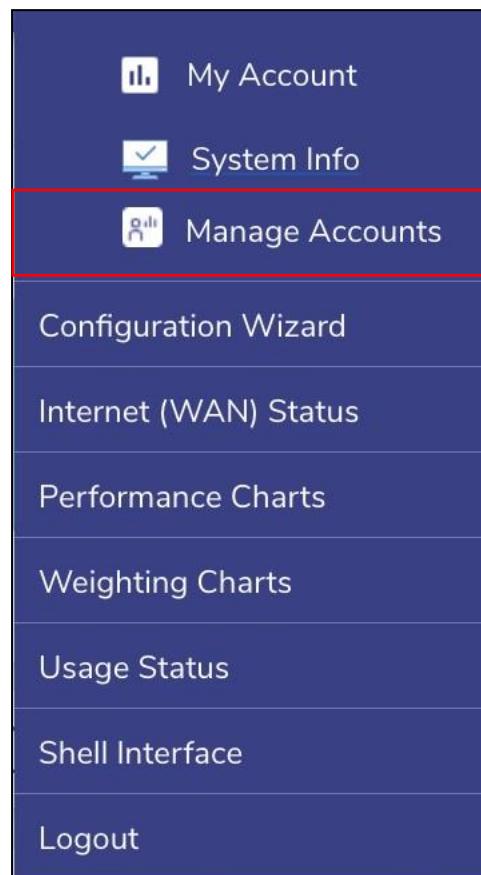


Figure 4.19 Manage Account

- The **User Account Management** pop-up window appears, see figure below.

User Account Management

Select Operation

☒ Add Account ☐ Disable Account ☐ Delete Account ☐ Change Password

Add User Account(s) to access K4 Applications

Select Organization Name

Enter Email

Demo@example.com

Access Privileges Expiry Date (optional)

Full Access

Resource

MY DEMO Site Add More Resources

Send Invitation Link

Figure 4.20 User Account Management

- To enter data in the respective fields, see table below.

Fields	Description
Operation	Click Add Account . By default, the Add Account is selected.
Organizational Unit	In the Organizational Unit list, click the name of the organization for which the user account is to be managed.
Email	This is the unique and operative email address of the user whose account is to be created. The email address is the username or login ID of the user.
Access Privileges	This identifies the access type the user wants to give to the account. It can be one of the following:


	<p>Full Access – This account has access to the entire EdgeOS Portal (read and edit)except Weighting Charts and Web Shell.</p> <p>Limited Access – This account has read only access to entire EdgeOS Portal andvery limited editing capabilities.</p> <p>Read Only Access – This account has access to Internet Status and Usage Status screens only.</p>
Expiry Date	This identifies the date of expiry of the account.
Resource	<p>This identifies the Sites to which this account has access to. By default, the current site is pre-filled in the resource field.</p> <p>To add more resources, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  . A new input field Select Resources appears, see Figure 4.21 Add Resources. Select the resources for which the user wants all access for the new account by clicking on the Select Resources drop down, see Figure 4.22 Select Organization.

Table 4-2 Add Account

User Account Management

Select Operation

☒ Add Account
☐ Disable Account
☐ Delete Account
☐ Change Password

Add User Account(s) to access K4 Applications

Select Organization Name

Enter Email

Demo@example.com

Access Privileges

Full Access

Expiry Date (optional)

Resource

MY DEMO Site

Add More Resources

Select Resources

Send Invitation Link

Figure 4.21 Add Resources

User Account Management

Select Operation

☒ Add Account
☐ Disable Account
☐ Delete Account
☐ Change Password

Add User Account(s) to access K4 Applications

Select Organization

MY-DEMO Site 1
MY-DEMO Site 2
MY-DEMO Site 3

Enter Email

Demo@example.com

Access Privileges

Full Access

Expiry Date (optional)

Resource

MY DEMO Site

Add More Resources

Select Resources

Send Invitation Link

Figure 4.22 Select Organization

- Click Send Invitation Link.

The invitation is sent to the email address specified in the Email field, see figure below.

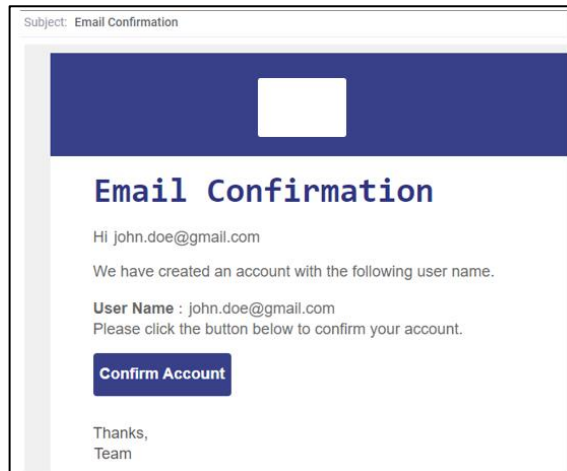


Figure 4.23 Email Confirmation

- Open the email and then click **Confirm Account**.
- The registration page appears, **Figure 4.24 Registration Page**.

Figure 4.24 Registration Page

- To enter data in the respective fields, **Table 4-3 Add Account Registration Details**.





Fields	Description
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Contact Number	In the Contact Number list, click the country and then enter the valid contact number.
Password	Enter the password of the user account.  To view the password, click the  icon.
Confirm Password	Re-enter the password for confirmation.  To view the password, click the  icon. The Register button becomes available.

Table 4-3 Add Account Registration Details

- Click **Register**. The user is registered, and a successful message is displayed, see figure below.

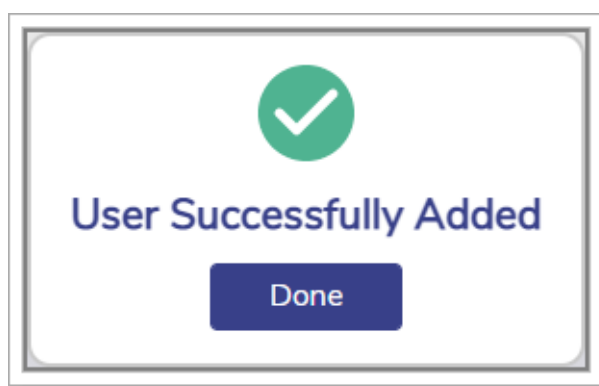


Figure 4.25 User Added Successfully

- Click **Done**.


Using the login credentials, the user can access the EdgeOS applications based on the role assigned to the user account.

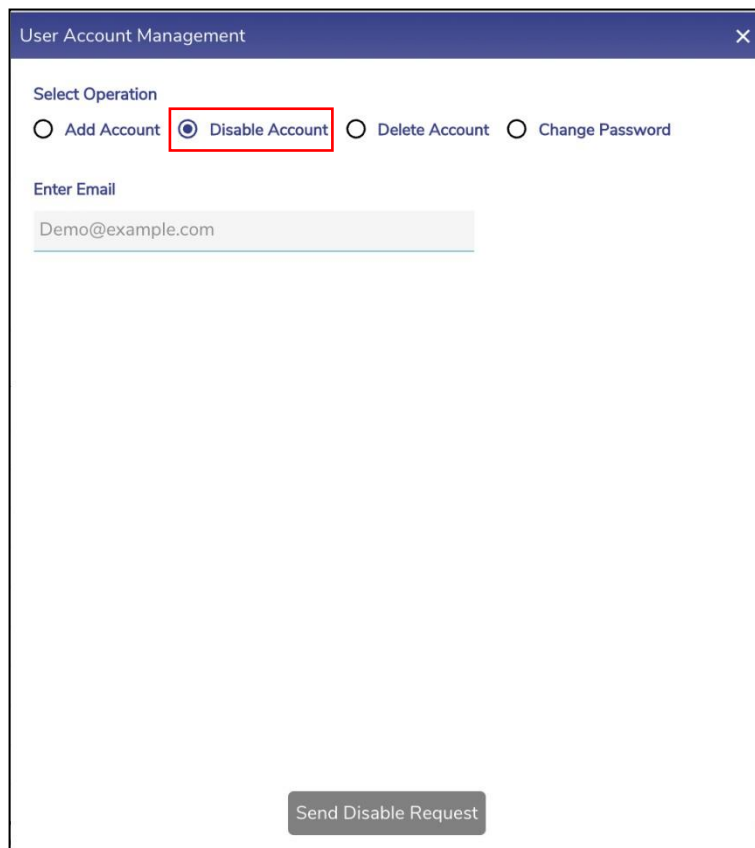
4.3.2 Disabling a User Account

The **Disable Account** operation is available for an administrator.

To disable the user account, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click Manage Accounts.
- The **User Account Management** pop-up window appears. See figure below.



The image shows a 'User Account Management' pop-up window. It has a dark blue header with the title 'User Account Management' and a close button (X). Below the header, there is a section titled 'Select Operation' with four radio button options: 'Add Account', 'Disable Account' (which is selected and highlighted with a red rectangle), 'Delete Account', and 'Change Password'. Below this, there is a section titled 'Enter Email' with a text input field containing 'Demo@example.com'. At the bottom right of the window, there is a button labeled 'Send Disable Request'.

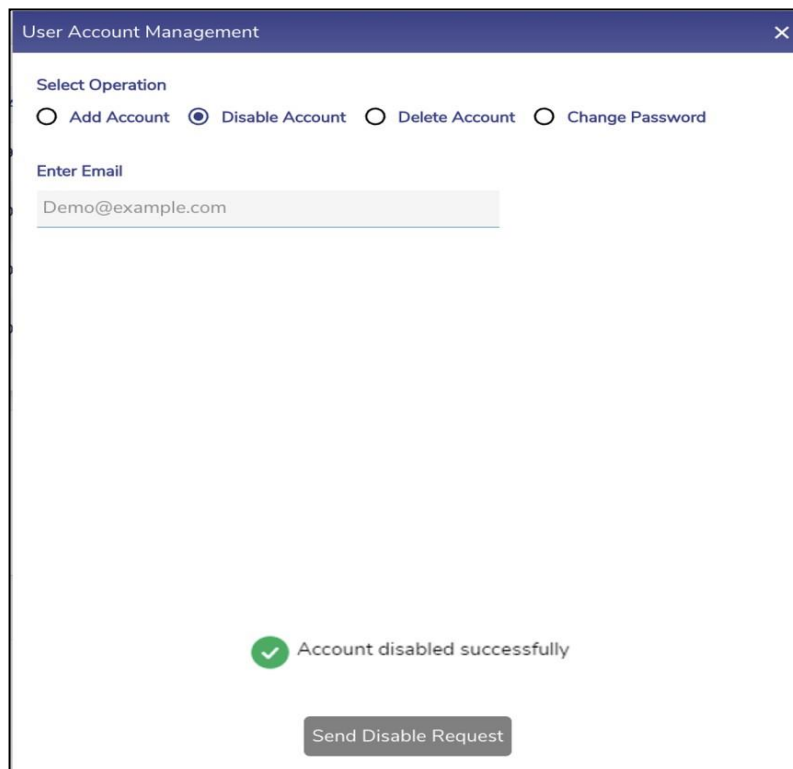
Figure 4.26 Disable Account

- To enter data in the respective fields, see table below.

Fields	Description
Operation	Click Disable Account . The User Account Management pop-up window appears, see figure below. By default, the Add Account is selected.
Email	Enter the email address to be disabled. The Send Disable Request button becomes available.

Table 4-4 Disable Account

- Click **Send Disable Request**. The user account is disabled, and a successful message is displayed, see figure below.



The screenshot shows a 'User Account Management' window with a dark blue header. Inside, there's a 'Select Operation' section with four radio buttons: 'Add Account', 'Disable Account' (which is selected), 'Delete Account', and 'Change Password'. Below this is an 'Enter Email' section with a text input field containing 'Demo@example.com'. At the bottom, there's a green checkmark icon followed by the text 'Account disabled successfully', and a grey button labeled 'Send Disable Request'.

Figure 4.27 Account Disabled Successfully


Therefore, using the login credentials, the user cannot log in to the portal or applications.

4.3.3 Deleting a User Account

The **Delete Account** operation is available for an administrator.

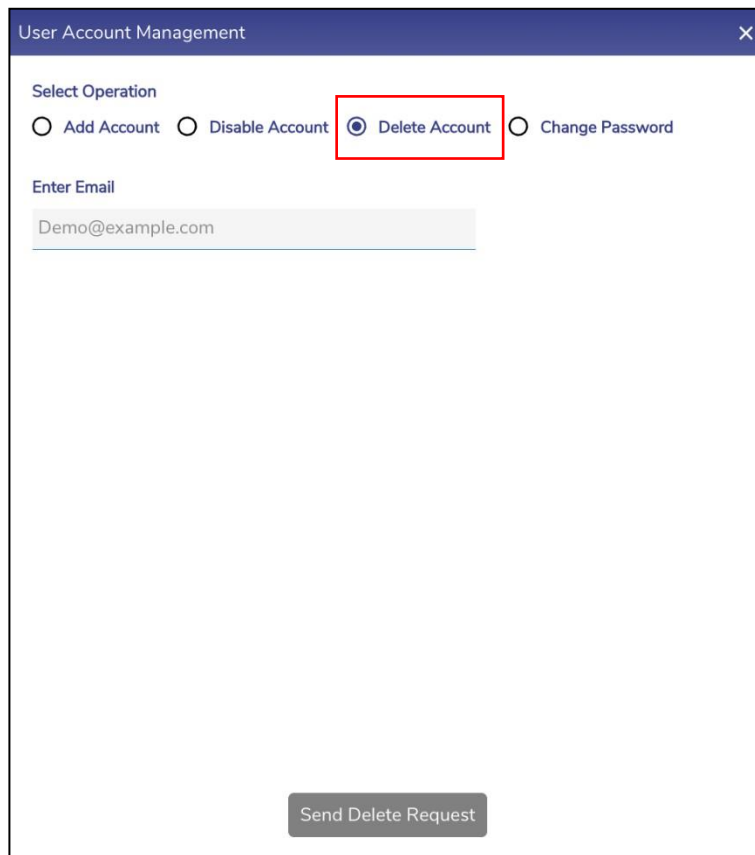
To delete the user account, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click Manage Accounts.
- The User Account Management pop-up window appears. see **Figure 4.28 Delete Account.**
- Select Delete Account.
- To enter data in the respective fields, see table below.

Fields	Description
Enter Email	Enter the email address to be disabled. The Send Delete Request button becomes available.

Table 4-5 Delete Account Fields



The image shows a 'User Account Management' dialog box with a dark blue header and a close button (X) in the top right corner. Below the header, there is a section titled 'Select Operation' containing four radio button options: 'Add Account', 'Disable Account', 'Delete Account', and 'Change Password'. The 'Delete Account' option is selected, indicated by a filled radio button and a red rectangular box around it. Below this section is a text input field labeled 'Enter Email' containing the text 'Demo@example.com'. At the bottom center of the dialog is a grey button labeled 'Send Delete Request'.

Figure 4.28 Delete Account

- Click **Send Delete Request**. The user account will be deleted.


Therefore, using the login credentials, the user cannot log in to the portal or applications.

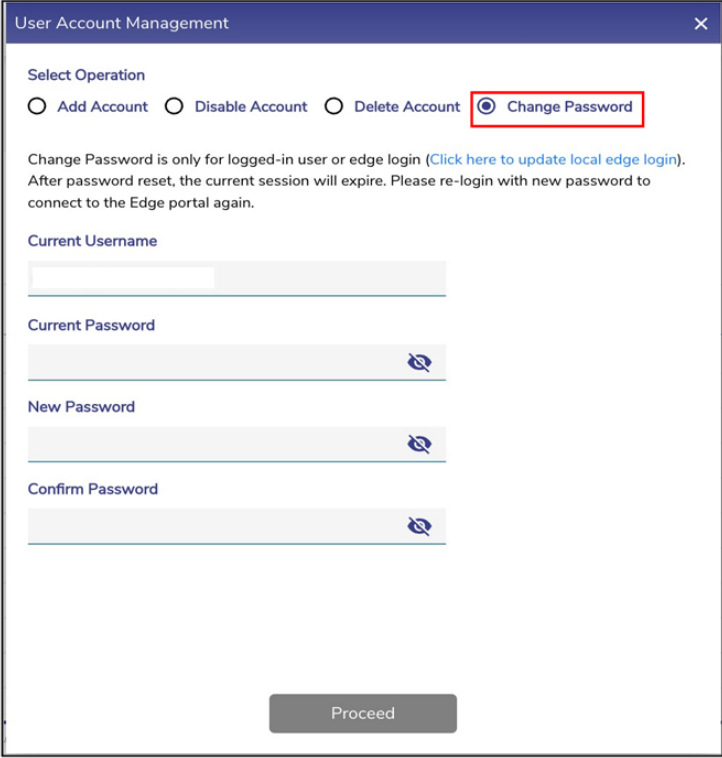
4.3.4 Changing the Login Password

The **Change Password** operation is available for all the users.

To change the login password, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click Manage Accounts.
- The **User Account Management** pop-up window appears.
- Click **Change Password**. The change password section appears, see figure below.



The image shows a 'User Account Management' pop-up window. At the top, there's a title bar with the text 'User Account Management' and a close button. Below the title bar, there's a section titled 'Select Operation' with four radio buttons: 'Add Account', 'Disable Account', 'Delete Account', and 'Change Password'. The 'Change Password' option is selected and highlighted with a red rectangle. Below this, there's a paragraph of text: 'Change Password is only for logged-in user or edge login ([Click here to update local edge login](#)). After password reset, the current session will expire. Please re-login with new password to connect to the Edge portal again.' Below the text, there are four input fields: 'Current Username', 'Current Password', 'New Password', and 'Confirm Password'. Each password field has a toggle icon to the right. At the bottom of the window, there is a 'Proceed' button.

Figure 4.29 Change Password

- To enter data in the respective fields, see table below.

Fields	Description
Current Username	Displays the current username
Current Password	Enter the current login password.
New Password	Enter the new login password.
Confirm Password	Re-enter the new login password for confirmation. The Proceed button becomes available.

Table 4-6 Change Password Fields

- Click **Proceed**.

The login password is changed, and a successful message is displayed. The current session ends. Therefore, the user must again log in to the EdgeOS portal using the new login password.

4.3.5 Changing EdgeOS Login Password

The EdgeOS **Change Password** operation is available for administrative users only.

To change the login password, perform the following steps.

Steps

- Click on Click here to update local EdgeOS login, see [Figure 4.29 Change Password](#). The EdgeOS Account Password Management Pop-up appears, see figure below.

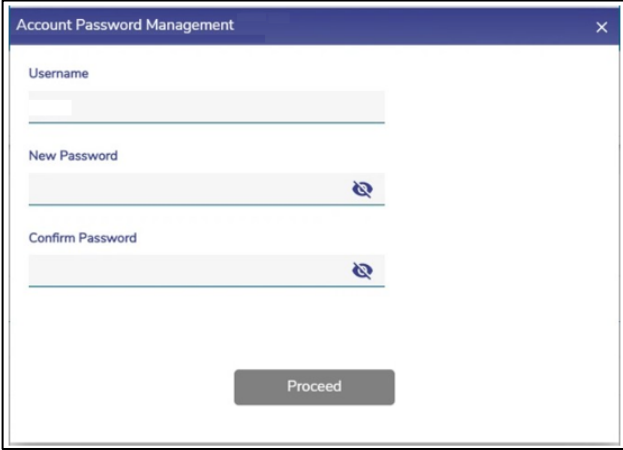
The image shows a web browser window titled "Account Password Management" with a close button (X) in the top right corner. Inside the window, there are three input fields: "Username" with a light blue border, "New Password" with a light blue border and a toggle icon (an eye with a slash) to its right, and "Confirm Password" with a light blue border and a toggle icon to its right. Below these fields is a grey button labeled "Proceed".

Figure 4.30 EdgeOS Account Password Management

- To enter data in the respective fields, see table below.

Fields	Description
Username	Displays EdgeOS Username.
New Password	Enter New Password.
Confirm Password	Confirm the New Password.

Table 4-7 Change Password Fields


- Click **Proceed**.

The EdgeOS Account password is changed. If the user has logged in with EdgeOS login, then the session is closed, and a re-login is required to access the EdgeOS Portal.

4.4 Configuration Wizard

To access the EdgeOS Configuration Wizard, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Configuration Wizard**, see figure below.

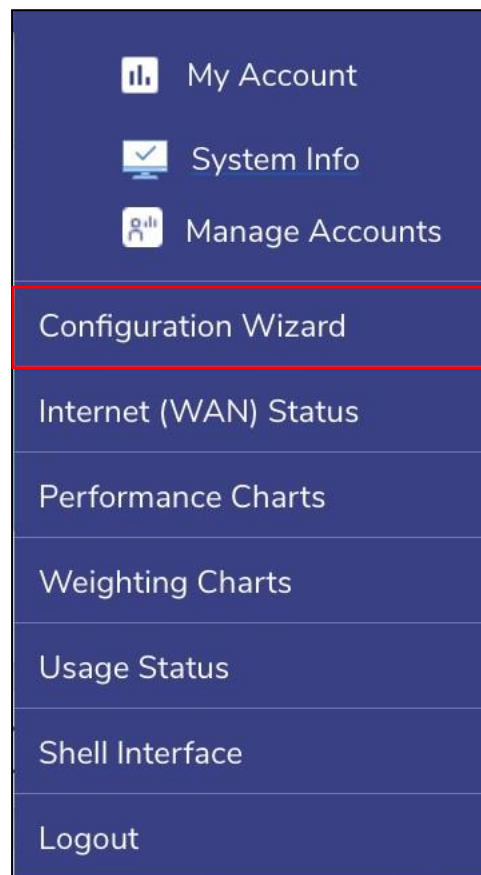


Figure 4.31 Configuration Wizard Option

For details, see [Commissioning EdgeOS System](#).

The steps specified to register the EdgeOS System are defined here and performed using the Edge Mobile App available on both App Store and Play Store with the title 'K4 Edge'.


4.5 Internet (WAN) Status

This is the landing page post Configuration completion. This screen provides a snapshot of the status of the Interfaces, Network Usage across Access Networks, Active Networks and Devices, Internet Profiles and Site Location.

4.5.1 Viewing Internet Status Page

To view Internet status, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Internet (WAN) Status**. The **Internet Status** page appears, see figure below.

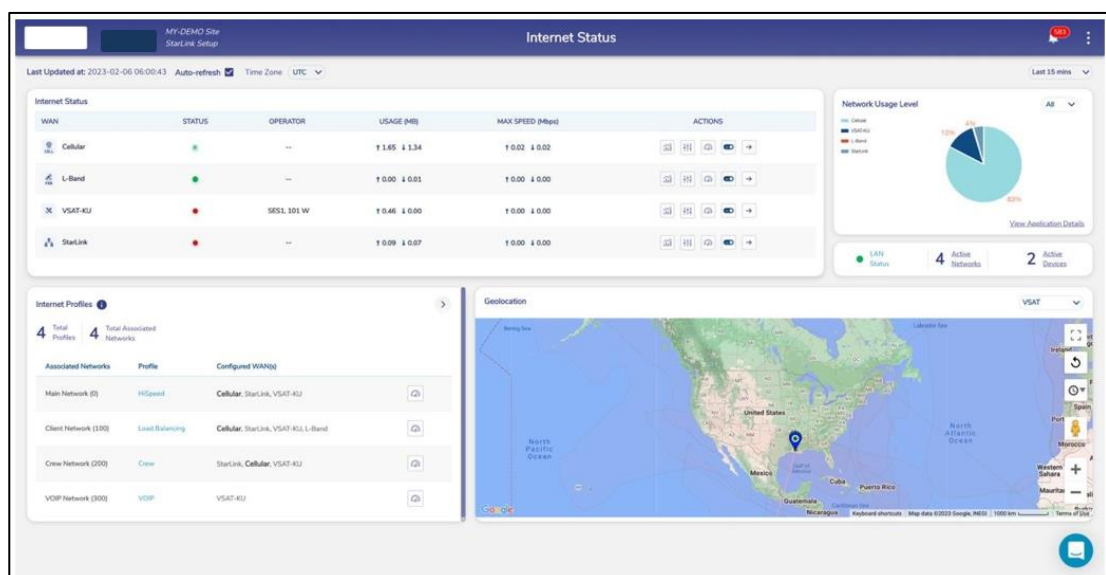
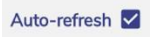


Figure 4.32 Internet Status Page

To view details of fields in the Internet Status screen, see table below.

Fields	Description	Configuration
Last Updated At	This shows the last timestamp at which this screen was updated.	N/A
Auto-refresh	<p>Allows data on this page is to be refreshed automatically.</p> <p>Data is updated at an interval of 30 seconds.</p>	<p>To automatically refresh the details of the WAN link, select the Auto-refresh  check box.</p>
Time Zone	Allows selection of time zone to access the details on this screen based in that time zone.	<p>By default, the UTC time zone is configured.</p> <p>In the Time Zone link, click a time zone, see Figure 4.64 Time Zone .</p> <p>Following options are available.</p> <ul style="list-style-type: none"> • UTC • EST • CST • PST • AST (Atlantic) • HST (Hawaii) • CET (Central Europe) • EET (Eastern Europe) • WET (Western Europe) • UAET • IST

Periodicity	<p>To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where</p> <ul style="list-style-type: none"> m is minutes h is hours d is days 	<p>By default, the periodicity of 15m is configured.</p> <p>Click the periodicity at the upper-right corner of the page to view the data on the screen at that periodicity, see Figure 4.34 Select Periodicity.</p>
--------------------	--	---

Table 4-8 Internet Status Fields

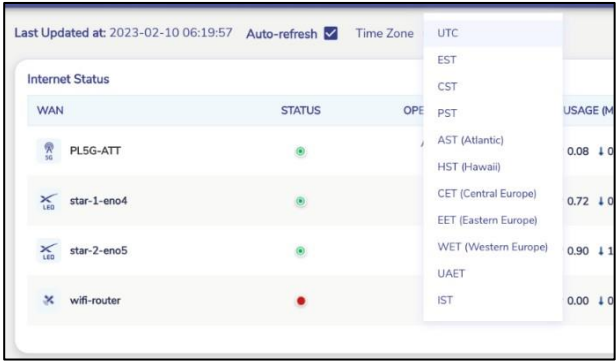


Figure 4.33 Select Time Zone

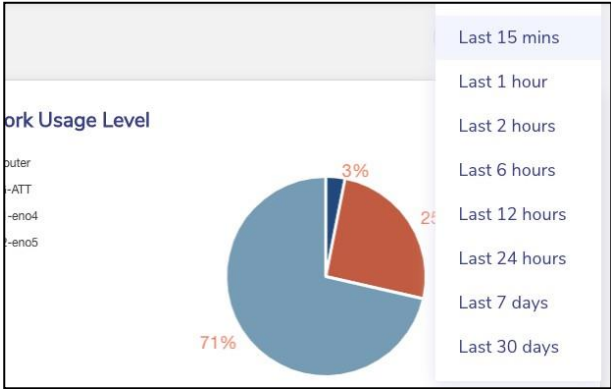


Figure 4.34 Select Periodicity

4.5.2 Viewing Interfaces Status



The user can view the Internet Status Section on Internet status page see figure below.

WAN	STATUS	OPERATOR	USAGE (MB)	MAX SPEED (Mbps)	ACTIONS
Cell 1		AT&T (5G)	1 0.09 1 0.08	1 0.00 1 0.00	
VSAT 1		---	1 13.10 1 37.80	1 3.43 1 10.36	
Starlink		---	1 43.38 1 68.05	1 4.83 1 11.19	
Ethernet		---	1 0.00 1 0.00	1 0.00 1 0.00	

Figure 4.35 Internet Status WAN Profiles

For details on Internet Status, see table below.


Fields	Description	Configuration
WAN	Displays the name of the Interface.	To view details of the Interface, Click on the Interface. The user will be routed to the respective Controller page or the modem.
Status	<p>Displays the status of the Interface. Following options are possible.</p> <ul style="list-style-type: none"> . Active. This indicates that the corresponding WAN link or interface 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 interface is working 	N/A

	<p>but not being used by the users on the vessel and the internet traffic is not moving through that WAN link or internet.</p> <ul style="list-style-type: none"> •  . Down. This indicates that the WAN link or interface is not working. •  . Disabled. This indicates that the corresponding WAN link or interface is disabled. Therefore, the internet will not work, and the internet traffic will not move through that link or internet. 	
Operator	Displays the Name of the Operator, for interface which is Active or Standby.	N/A
Usage (MB)	Displays the upload and download Usage on the interface.	N/A
Max Speed (Mbps)	Displays the Max upload and download speed of interface.	N/A
Actions	<p>There are five action buttons available per interface for the following actions.</p> <ul style="list-style-type: none"> • Realtime Charts • Controller or Interfaces 	<p>For details, see following sections.</p> <p>Viewing Realtime Chart.</p> <p>Viewing Controllers.</p> <p>Performing Speed Test on an Interface.</p>

	<ul style="list-style-type: none"> • Speed Test • Enable/Disable • Performance Chart 	<p><i>Disabling an enabled Interface.</i></p> <p><i>Enabling a disabled Interface.</i></p> <p><i>Viewing Performance Chart for an Interface.</i></p>
--	---	--

4.5.2.1 Viewing Realtime Chart

Steps

- Click  under the Action corresponding to the interface to view the real-time data usage on the interface. The Realtime Chart page appears, see [Figure 4.36 Realtime Chart](#).
- The chart plots last 5 minutes of data in the given window. The fields available on the chart are peak and average upload and download data rates.

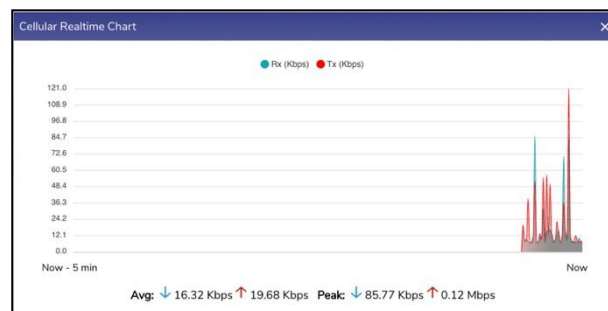



Figure 4.36 Realtime Chart

4.5.2.2 Viewing Controllers

To view the Controller for the Interface, perform the following steps.

Steps


- Click  under the Action corresponding to the WAN source. The Controller page appears, e.g., see [Figure 4.89 Starlink Information](#).

If there is no Controller for the interface, this button directs to the Interfaces Screen on the Configuration Wizard.

4.5.2.3 Performing Speed Test on an Interface

To run Speed Test on an Interface, perform the following steps.

Steps

- Click  under the Action column corresponding to the interface. The Speed Test Pop-up appears, see [Figure 4.37 Speed Test Pop-up](#).
- Select Internet Source from the drop-down list for which Speed Test is to be performed, see [Figure 4.38 Select Internet](#) . By default, the interface for which the Speed Test button has been clicked is selected. Before performing the speed test, user must ensure that the internet is up on this Interface.
- Click **GO**. The Speed Test result becomes available, see [Figure 4.39 Speed Test Result](#). The output consists of Server IP, Service Provider, Ping time, Upload and Download Speed.

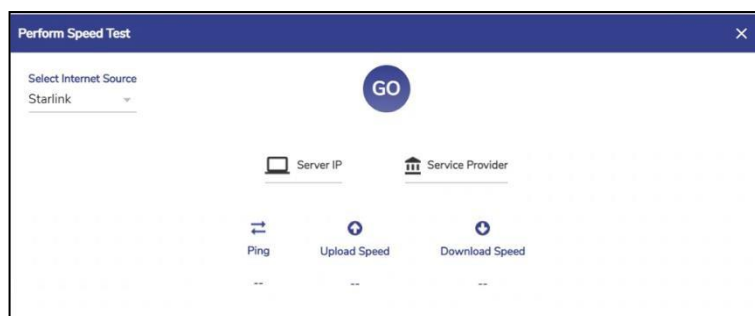


Figure 4.37 Speed Test Pop-up

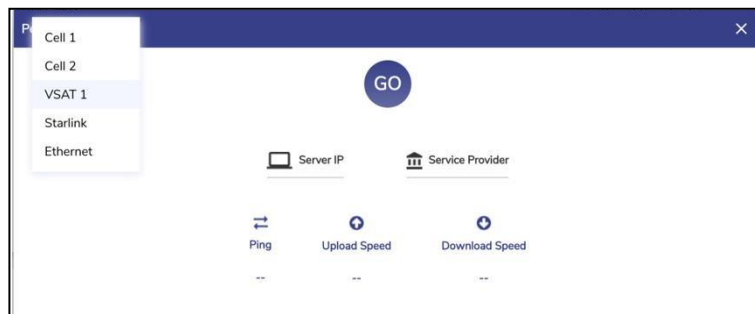


Figure 4.38 Select Internet Source

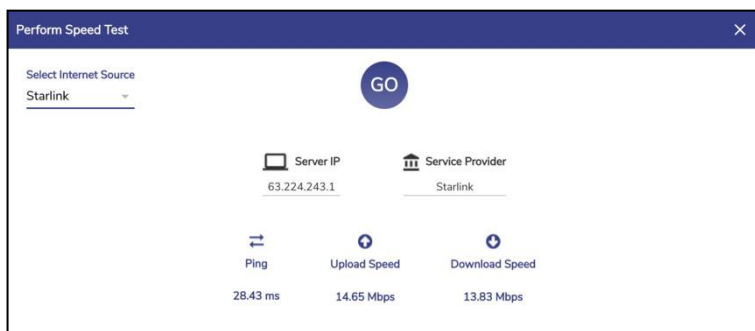



Figure 4.39 Speed Test Result

4.5.2.4 Disabling an enabled Interface

To Disable an Interface, perform the following steps.

Steps

- Click  Action corresponding to the interface that is enabled. The Disable Interface pop-up window appears, see [Figure 4.40 Disable](#) Pop-up.
- Click **Confirm**.
- The WAN source/Interface is switched off.

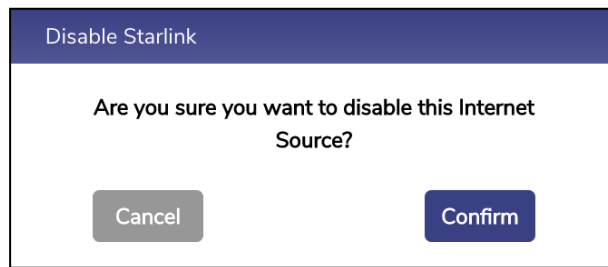



Figure 4.40 Disable Pop-up

4.5.2.5 Enabling a disabled Interface

To enable an Interface, perform the following steps.

Steps

- Click  Action corresponding to the Interface. The Enable Interface pop-up window appears, see [Figure 4.41 Enable](#) Pop-up.
- Click Confirm.
- The **Interface** is switched on.

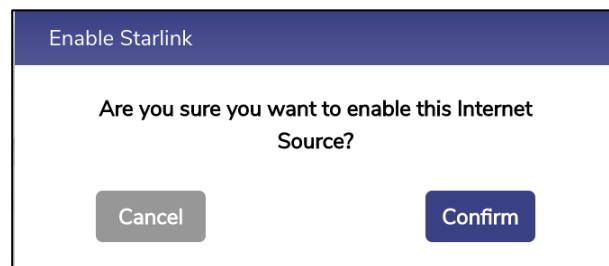


Figure 4.41 Enable Pop-up

4.5.2.6 Viewing Performance Chart for an Interface

To go to the Performance Chart for an Interface, perform the following steps.

Steps


- Click  Action corresponding to the Interface. The user will be directed to the corresponding interfaces' Performance Chart Screen, see figure below.



Figure 4.42 Performance Chart Starlink

4.5.3 Network Usage Level

- This section depicts the percentage of usage per Interface for a given period, see figure below. By default, the period selected is 15 minutes.

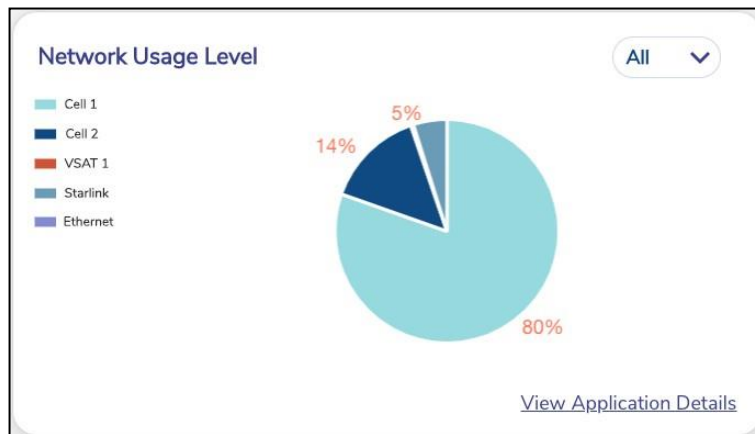


Figure 4.43 Network Usage Level Pie-Chart

4.5.3.1 Viewing Usage for an Interface

To see the % usage for an Interface across different Access Networks, perform the following steps.

Steps

- Click the drop down on the top right of this section and select the Interface, [Figure 4.44 Network Usage Drop-Down Selection](#).
- The pie chart updates with the details, see [Figure 4.45 Starlink Network Usage](#).

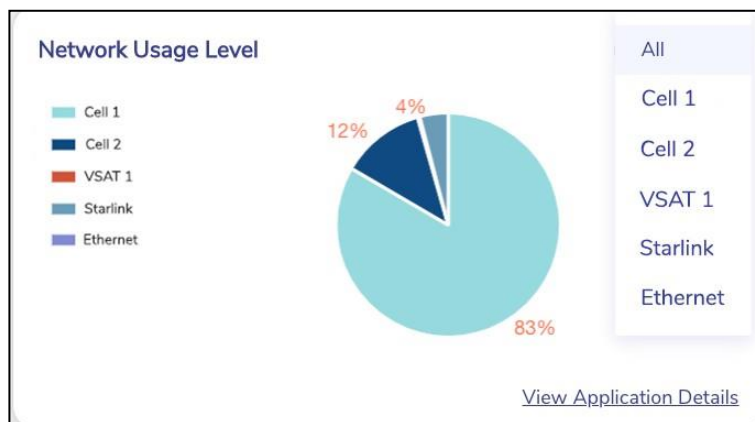


Figure 4.44 Network Usage Drop-Down Selection

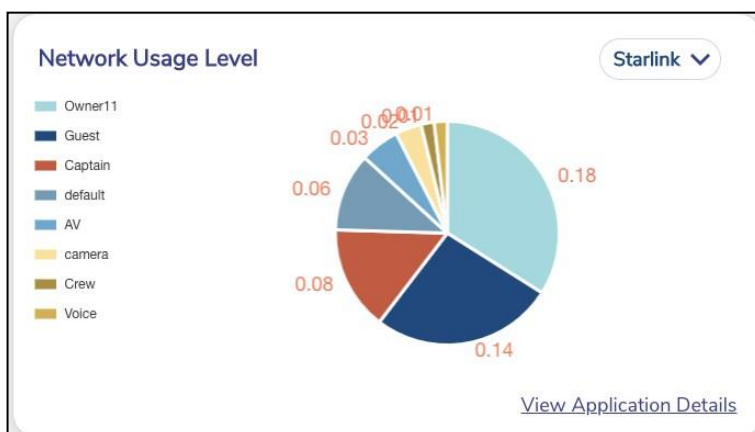


Figure 4.45 Starlink Network Usage

4.5.3.2 Viewing Top Applications

To see the Top Applications accessed for a period, perform the following steps.

Steps

- Click the at the bottom right of this section and select the Interface, see figure below.

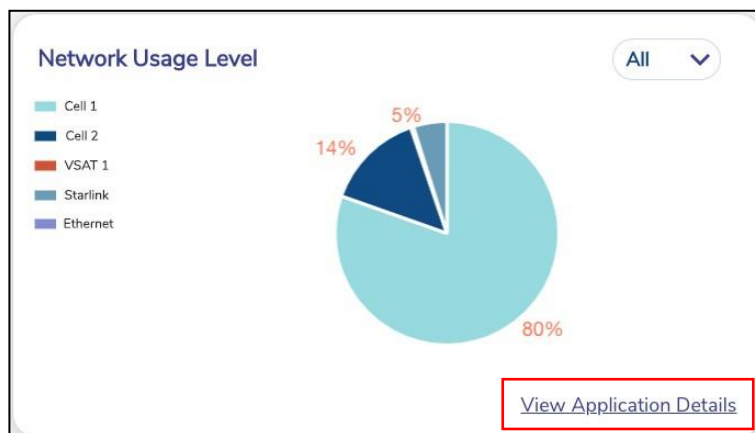


Figure 4.46 View Top Applications

A Pop-up with the details appears, see [Figure 4.47 Top Applications](#) By default, the periodicity set is same as that on the Internet Status screen, and can be changed through the drop down available, see [Figure 4.48 Change Periodicity - Top Applications](#).



Figure 4.47 Top Applications



Figure 4.48 Change Periodicity - Top Applications

4.5.4 LAN Status

- This section provides the status of the LAN, Active Networks and Active Devices in the system.

For details of the fields, see table below.



Fields	Description	Configuration
LAN Status	Displays LAN Status on the server. <ul style="list-style-type: none">• The icon  means that the LAN status is Active.• The icon  means that the LAN status is Inactive.	Click on LAN Status to go to Access Networks Screen .
Active Networks	Displays the total active networks in the system.	Click on Active Networks to go to Top Networks section of the Usage Screen .
Active Devices	Displays the total active devices.	Click on Active Devices to go to Top Devices section of the Usage Screen .

Table 4-9 LAN Status Fields

4.5.5 Konnect VPN

This is an optional section and displays the Konnect VPN Server and Client details and status, see figure below.

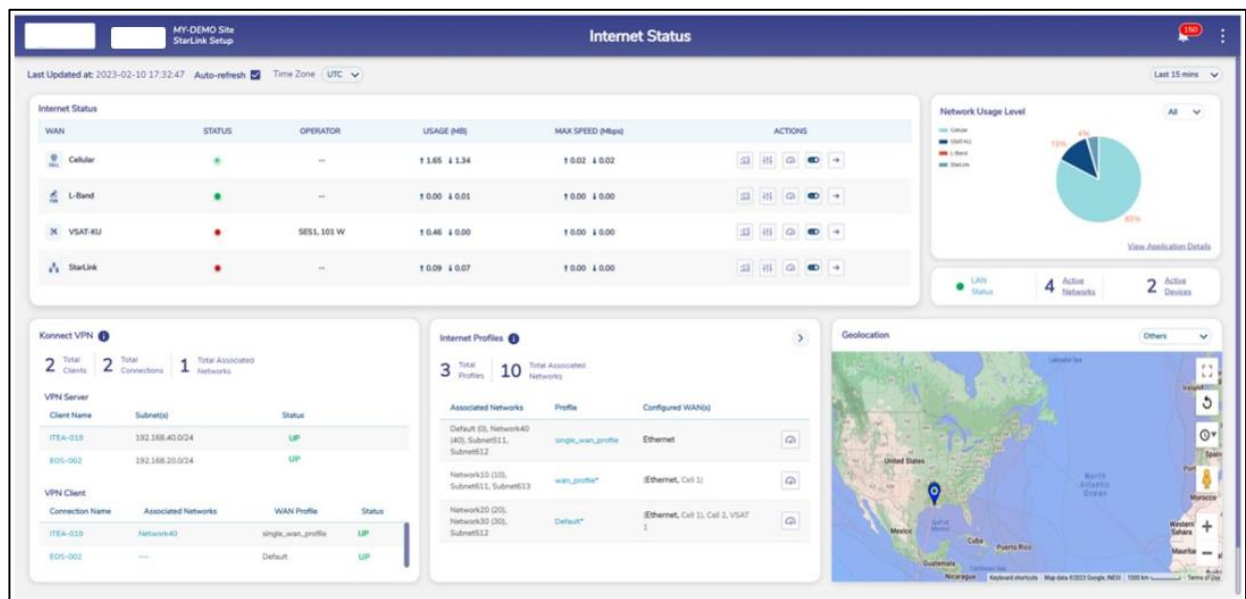


Figure 4.49 Internet Status with Konnect VPN

Note: If there is no Konnect VPN configuration present on the server, this section will not appear on the Internet Status Screen.

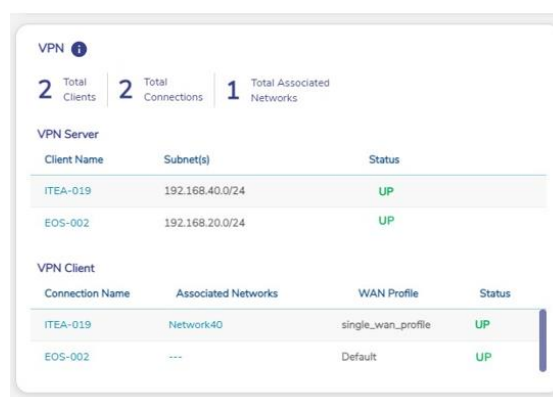


Figure 4.50 Konnect VPN Dashboard

For details of the top fields in this section, see tables below.

Fields	Description	Configuration
Total Clients	This is the number of configured clients. If there are no clients configured, then this field will not be present.	N/A
Total Connections	This is the number of configured connections. If there are no clients configured, then this field will not be present.	N/A
Total Associated Networks	This is the number of Access Networks configured for Konnect VPN.	N/A

Table 4-10 Konnect VPN Details

For details of the Konnect VPN Server section, see tables below.

Fields	Description	Configuration
Client Name	This is the name of the Client.	Click the Client Name to go the Konnect VPN -> Konnect VPN Client section .
Subnet(s)	This is the list of subnet(s).	N/A
Status	This is the status of the Client connection. It can have one of the following values.	N/A



	<ul style="list-style-type: none">  Indicates connection is up.  Indicates connection is down. 	
--	--	--

Table 4-11 VPN Server

For details of the Konnect VPN Client section, see tables below.




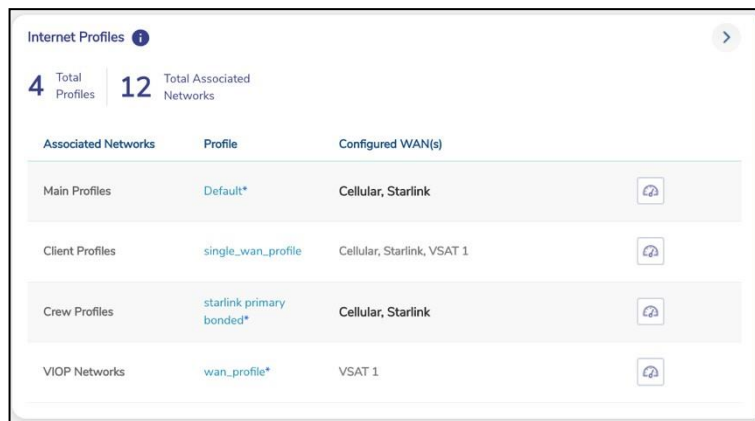
Fields	Description	Configuration
Connection Name	This is the name of the connection.	Click the Connection Name to go the Konnect VPN -> Konnect VPN Client section .
Associated Networks	This is the list of Associated Networks for this connection.	N/A
WAN Profile	This is the WAN Profile associated with the connection.	N/A
Status	<p>This is the status of the connection. It can have one of the following values.</p> <ul style="list-style-type: none">  Indicates connection is up.  Indicates connection is down. 	N/A

Table 4-12 VPN Client

4.5.6 Internet Profile

This Section displays the Internet profiles that are associated with at least one Access Network, see [Figure 4.51 Internet Profiles](#).

For information on this section, hover over to the  icon, see [Figure 4.52 Internet Profiles Hover Action](#).







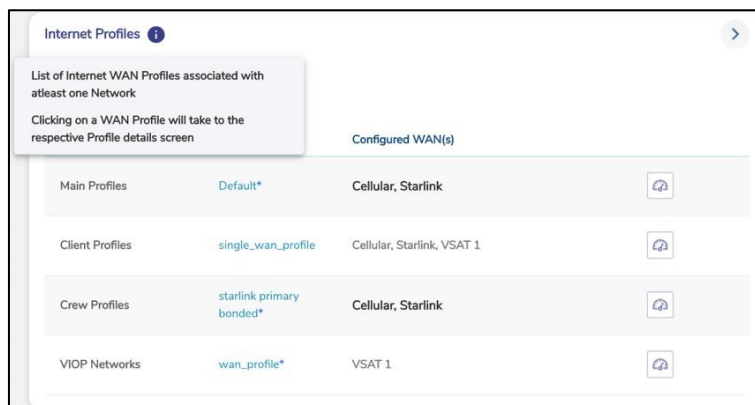





Associated Networks	Profile	Configured WAN(s)	
Main Profiles	Default*	Cellular, Starlink	
Client Profiles	single_wan_profile	Cellular, Starlink, VSAT 1	
Crew Profiles	starlink_primary_bonded*	Cellular, Starlink	
VIOP Networks	wan_profile*	VSAT 1	

Figure 4.51 Internet Profiles



		Configured WAN(s)	
Main Profiles	Default*	Cellular, Starlink	
Client Profiles	single_wan_profile	Cellular, Starlink, VSAT 1	
Crew Profiles	starlink_primary_bonded*	Cellular, Starlink	
VIOP Networks	wan_profile*	VSAT 1	

Internet Profiles 

List of Internet WAN Profiles associated with atleast one Network

Clicking on a WAN Profile will take to the respective Profile details screen

Figure 4.52 Internet Profiles Hover Action.

For details of fields in this section, see table below.

Fields	Description	Configuration
Total Profiles/ Total Associated Network	Displays total WAN Profiles and total Associated Networks in the system.	N/A
Associated Networks	Displays the list of Associated Networks to which a WAN Profile is assigned.	N/A
Profile	Displays the WAN profile used by these Associated Networks.	Click on the WAN Profile to go to the WAN Profile screen on the Configuration Wizard. The WAN Profile appears on this screen.
Configured WANs	Displays the list of WANs configured in the WAN Profile in priority order, with the active WAN highlighted in bold. Bonded WANs in a profile are shown in brackets.	N/A
Speed Test	This allows to run Speed test over 'bonded' links, or any WAN links based on the WAN profile configured for the Access Network.	To perform Speed Test over bonded links, see section <i>Performing Speed Test on a Bonded</i> .


Table 4-13 Internet Profile Fields

4.5.6.1 Performing Speed Test on a Bonded Link

Note: The Speed Test traffic follows the Traffic policies assigned for that Access network. If there are multiple Access Networks using the same WAN profile and the user wants to run the Speed Test over the specific Access Network, the same can be selected from the drop down.

To perform Speed Test on a Bonded Link, perform the following steps.

Steps

- Click  corresponding to the WAN Profile. The Speed Test Pop-up appears, see [Figure 4.53 Bonded Link Speed Test](#).
- Click the drop down to select the Access Network on which the user wants to run the Speed Test on, see [Figure 4.54 Bonded Link Speed Test Drop Down](#).
- Click **GO**.

The Speed Test results appear on the Pop-up after completion of Speed Test run.

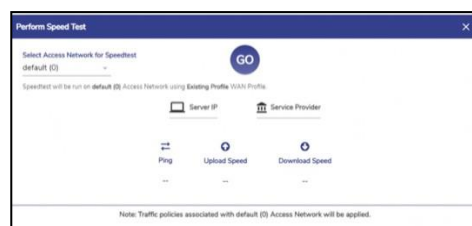


Figure 4.53 Bonded Link Speed Test

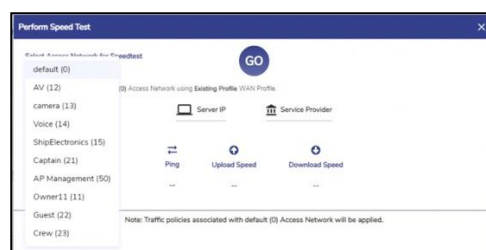



Figure 4.54 Bonded Link Speed Test Drop Down

4.5.6.2 Viewing detailed status of WAN Profiles

To see detailed view of WAN Profiles, perform the following steps.

Steps

- Click  on the top right of the Internet Profiles section. The Internet Profile Status Pop-up appears, see figure below.

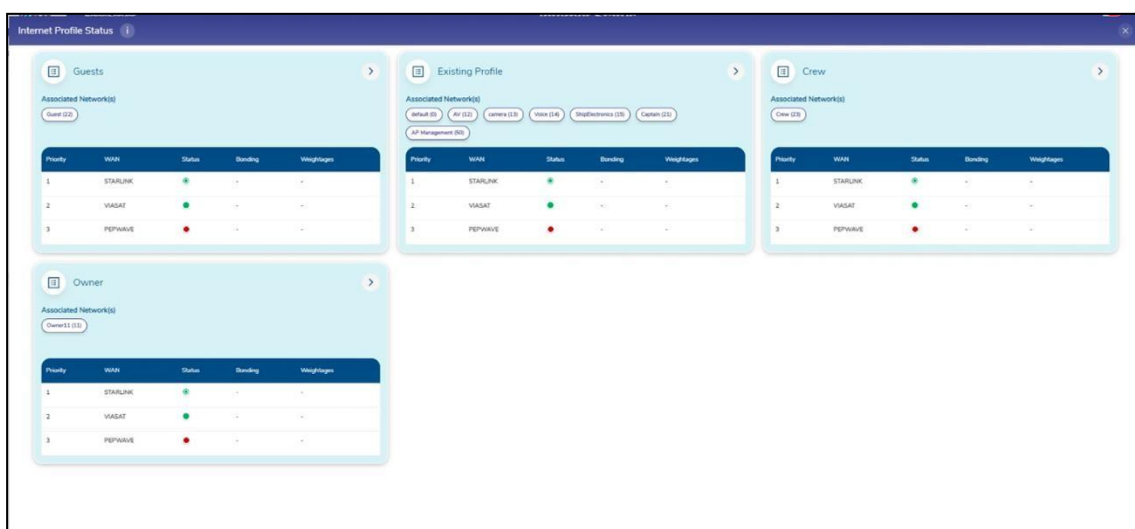


Figure 4.55 Internet Profile Status Pop-up

- The user can see the WAN Profiles in the system along with the status of the WANs, Bonding and Weighting details.
- User can change the WAN Profile associated with an Access Network by dragging the Access Network from the current WAN Profile card to the new WAN Profile card.

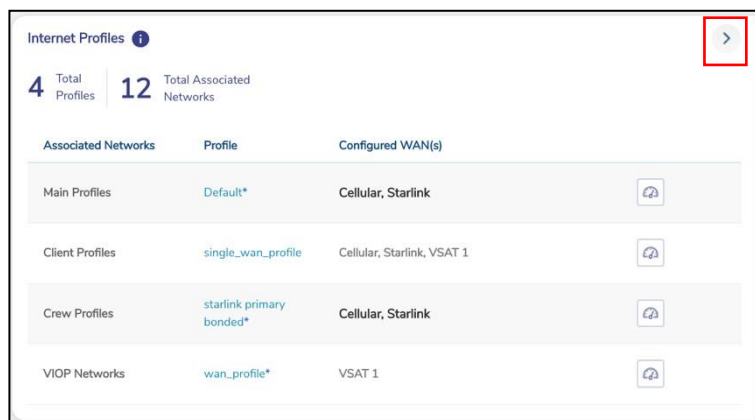


Figure 4.56 Arrow Button Internet Profiles

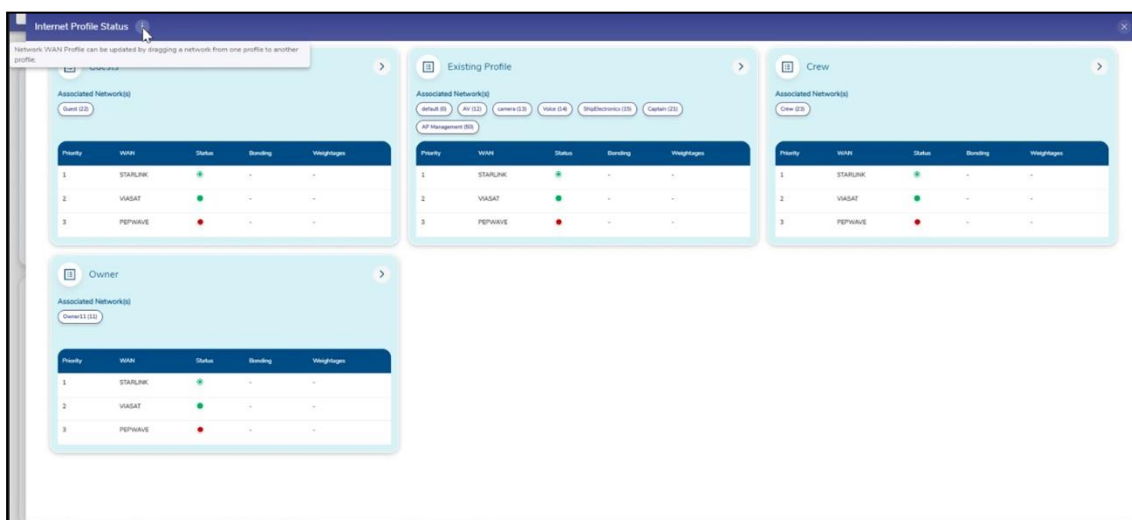


Figure 4.57 Internet Profile Status Info Icon

4.5.7 Geolocation

The Site Location and Voyage Path can be viewed on the Geolocation section, see figure below.

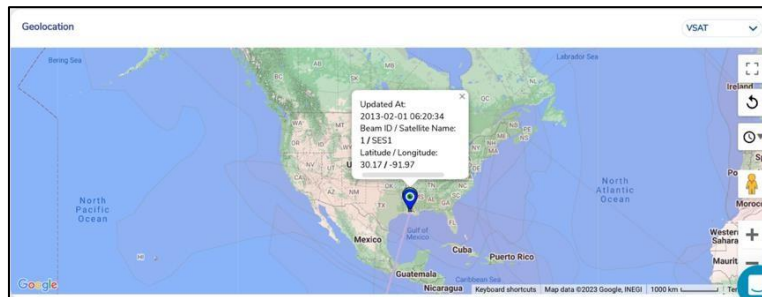


Figure 4.58 Geolocation - VSAT

By default, the VSAT geolocation map is plotted, however if this is not available, then Cellular map is plotted, and if this is also not available, then it is updated from other source. It is possible that in the absence of any source having this data, this section will be blank. The user can select the desired source from the Source drop down on the top right of this section to view the respective map, see [Figure 4.59 Geolocation - Others](#).

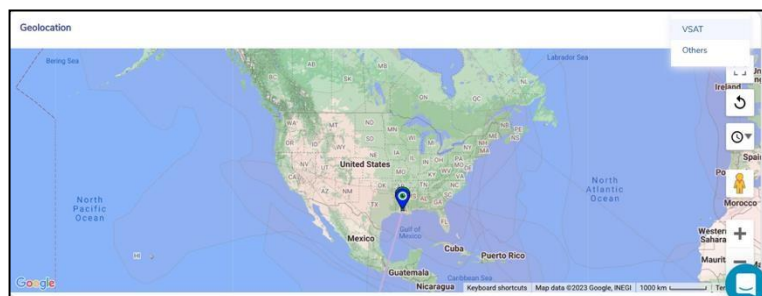


Figure 4.59 Geolocation - Others

4.6 Performance Charts

Once the EdgeOS System is configured, user can monitor the performance of the interface or WAN links.

4.6.1 Viewing Performance Charts

To view the performance charts, perform the following steps.

Steps



- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Performance Charts**. The **Performance Charts** page appears. See figure below.



Figure 4.60 Performance Chart

For description of the information displayed on the Performance Charts, see Table below.

Fields	Description	Configuration
Data Rates	DL/UL rates chart of the internet source for a specific network is generated.	<p>To view the DL/UL rate chart for a network, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> In the Internet Source list, click a WAN link or an internet source. In the Network list, click single or multiple networks. Click Apply. <p>The performance chart is generated.</p> <p>To view the network level usages for VSAT and Cell, user must click either VSAT or Cell.</p> <p>If the network selected in the Network list does not apply to the internet source selected in the Internet Source list, then the alert is displayed.</p>
Link Status	The status chart of the probe and link is available.	<p>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.</p> <p>Or,</p> <p>To view the link status chart for a network based on day and time, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Switch on the Custom Search  . The Start Time, End Time, and Interval (sec) fields become

		<p>available, see Figure 4.61 Custom search.</p> <ul style="list-style-type: none"> Click Start Time. The calendar becomes available. Select the start day and time. The start day and time become available in the time zone selected on the portal. Click End Time. The calendar becomes available. Select the end day and time. The start day and time become available in the time zone selected on the portal. In the Interval (sec) field, click the minimum interval specified. Click Apply. <p>The chart is generated.</p> <p>Additionally, Probe Success % and Link Down Time % is also available.</p>
Latency & Jitter	Latency & Jitter chart is available.	N/A
Speed Test Results	Periodic speed test results for an interface are available. The periodicity is as per the configuration set for that interface.	<p>To view the Speed Test Results chart, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> In the Internet Source list, click a WAN link or an internet source. Click the calendar in the Date field and select the date of when the speed test result chart is to be generated.

		<p>The chart is generated.</p> <p>To view Peak Rate estimate results for the interface, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none">• Check the ^{Peak Rate Estimate} <input checked="" type="checkbox"/> box on the top right of the Speed Test chart, see Figure 4.62 Peak Rate Estimate.• The Peak Rate estimates plots are available in the Speed Test chart.
--	--	---

Table 4-14 Performance Chart Information

Start Time	End Time	Interval (sec)	APPLY
02/07/2023 07:41	02/07/2023 07:56	60 Min value is 60 sec	

Figure 4.61 Custom search

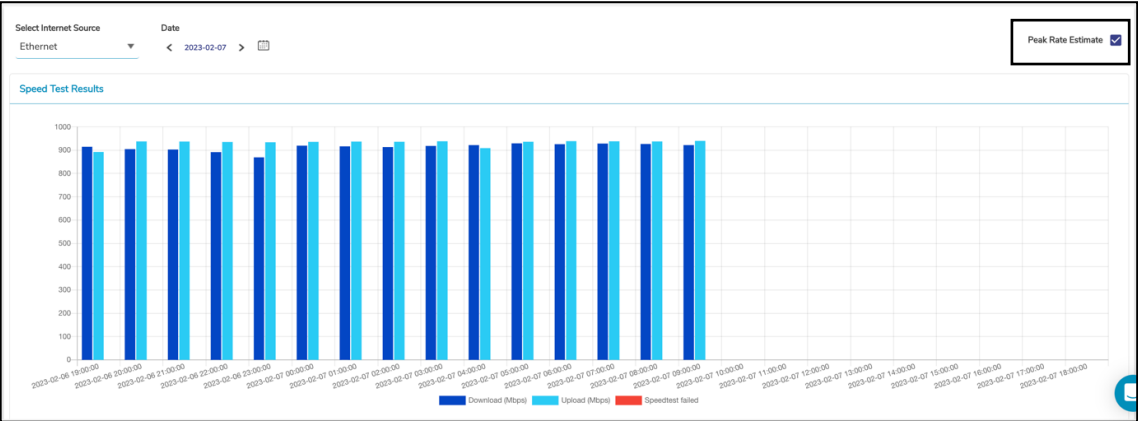


Figure 4.62 Peak Rate Estimate

4.7 Weighting Charts


Once the EdgeOS System is audited and possibly reconfigured, user can view the weighting % of the bonded interfaces at the periodicity of 10 seconds. If the US internet is down, then only the Native - Peak Rate Estimate chart becomes available, and the weighting of the bonded interfaces is performed based on the Native - Peak Rate Estimate. If the US internet is up, then the PEP - Peak Rate Estimate chart also becomes available, and the weighting of these bonded interface is done based on the PEP - Peak Rate Estimate.

Note: This menu item is available for administrative users only.

4.7.1 Viewing Weighting Charts

To view the weighting %, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Weighting Charts**. The **Weighting Charts** page appears, see figure below.

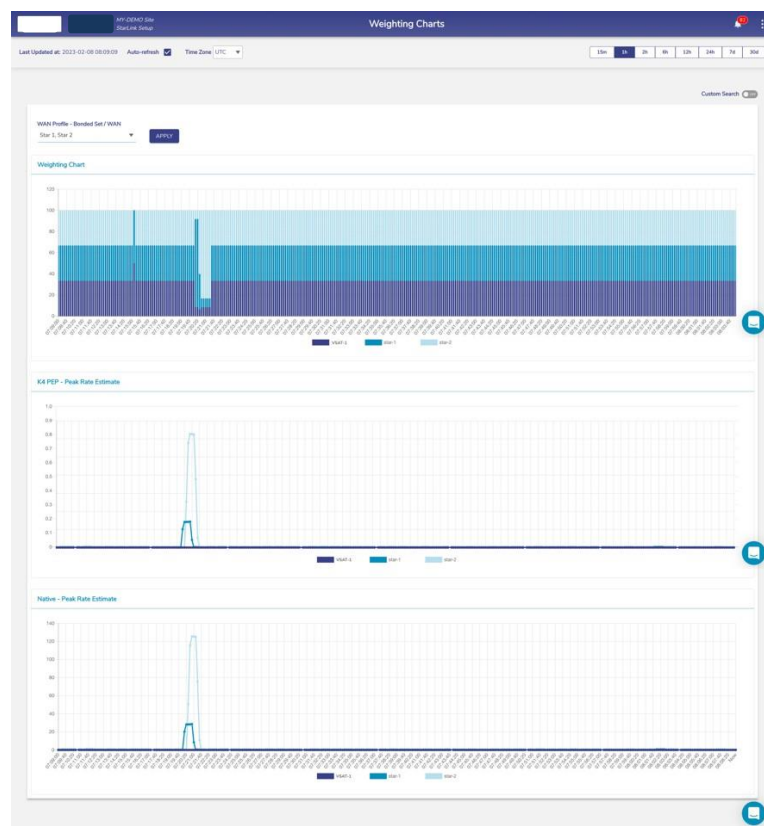


Figure 4.63 Weighting Charts

For description of the fields in Weighting Charts, see Table below.

Fields	Description	Configuration
Auto-refresh	<p>Whether the data on the page is to be refreshed automatically.</p> <p>Data is updated at an interval of 30 seconds.</p>	To automatically refresh the details of the WAN link, select the Auto-refresh check box.
Time Zone	<p>To access the details of the WAN link based on the time zone.</p> <p>By default, the UTC is configured.</p> <p>To view data at a period of 15m, 1h, 2h, 6h, 12h, 24h, 7d, and 30d, where,</p> <ul style="list-style-type: none"> m is minutes h is hours d is days <p>By default, the periodicity of 15m is configured.</p>	In the Time Zone link, click a time zone, see Figure 4.64 Time Zone
		Click the periodicity at the upper-right corner of the page.
Custom Search		<p>To create and view the chart based on a day and time, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Switch on the Custom Search. The custom search section appears, see Figure 4.65 Custom Search. Click Start Time. The calendar becomes available.

		<ul style="list-style-type: none"> • Select the start day and time. The start day and time become available in the time zone selected on the portal. • Click End Time. The calendar becomes available. • Select the end day and time. The start day and time become available in the time zone selected on the portal. • In the Interval (sec) field, click the minimum interval specified. • Click Apply. <p>The chart is created.</p>
WAN Profile - Bonded Set / WAN	Bonded set for which Weighting Charts need to be viewed.	<p>To view the weighting chart, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • In the WAN Profile - Bonded Set / WAN list, select the WAN check box, see Figure 4.66 WAN Profile - Bonded Set/WAN. • Click Apply. <p>The weighting chart becomes available.</p> <hr/> <p>Neither bonded set can be selected with the single WAN(s), nor a single WAN can be selected with the bonded set.</p>

Table 4-15 Weighting Charts Fields

Time Zone

UTC

UTC

EST

CST

PST

AST (Atlantic)

HST (Hawaii)

CET (Central Europe)

EET (Eastern Europe)

WET (Western Europe)

UAET

IST

Figure 4.64 Time Zone

Start Time

End Time

Interval (min)

APPLY

02/07/2023 09:50

02/07/2023 10:06

10

Min value is 10 sec

Figure 4.65 Custom Search

WAN Profile - Bonded Set / WAN

STAR - Star 1, Star 2

APPLY

☒ STAR - Star 1, Star 2
 ☐ VSAT 1
 ☐ VSAT 2
 ☐ Ethernet

Weighting Chart

120

100

80


Figure 4.66 WAN Profile - Bonded Set/WAN

4.8 Usage Status

Once the EdgeOS System is configured, user can monitor the usage of the networks and devices connected to the networks.

To view the Network usage details, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click Usage Status. The Usage Status page appears, see figure below.

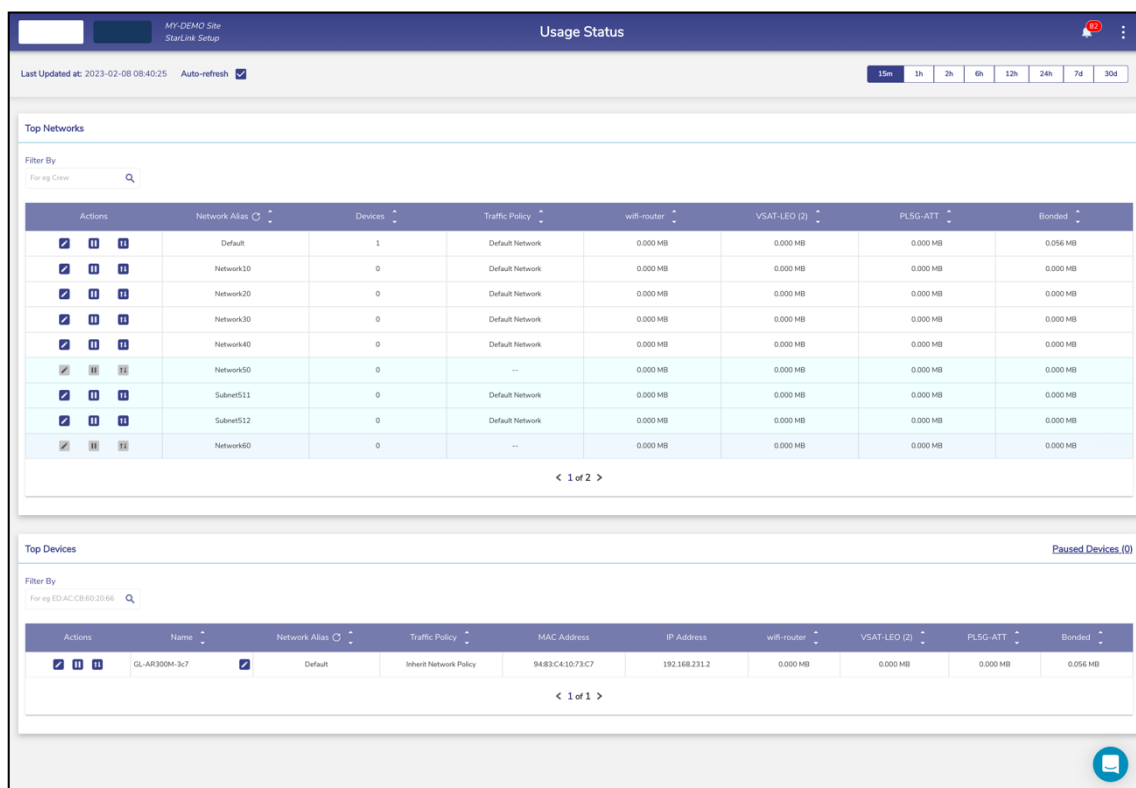


Figure 4.67 Usage Status

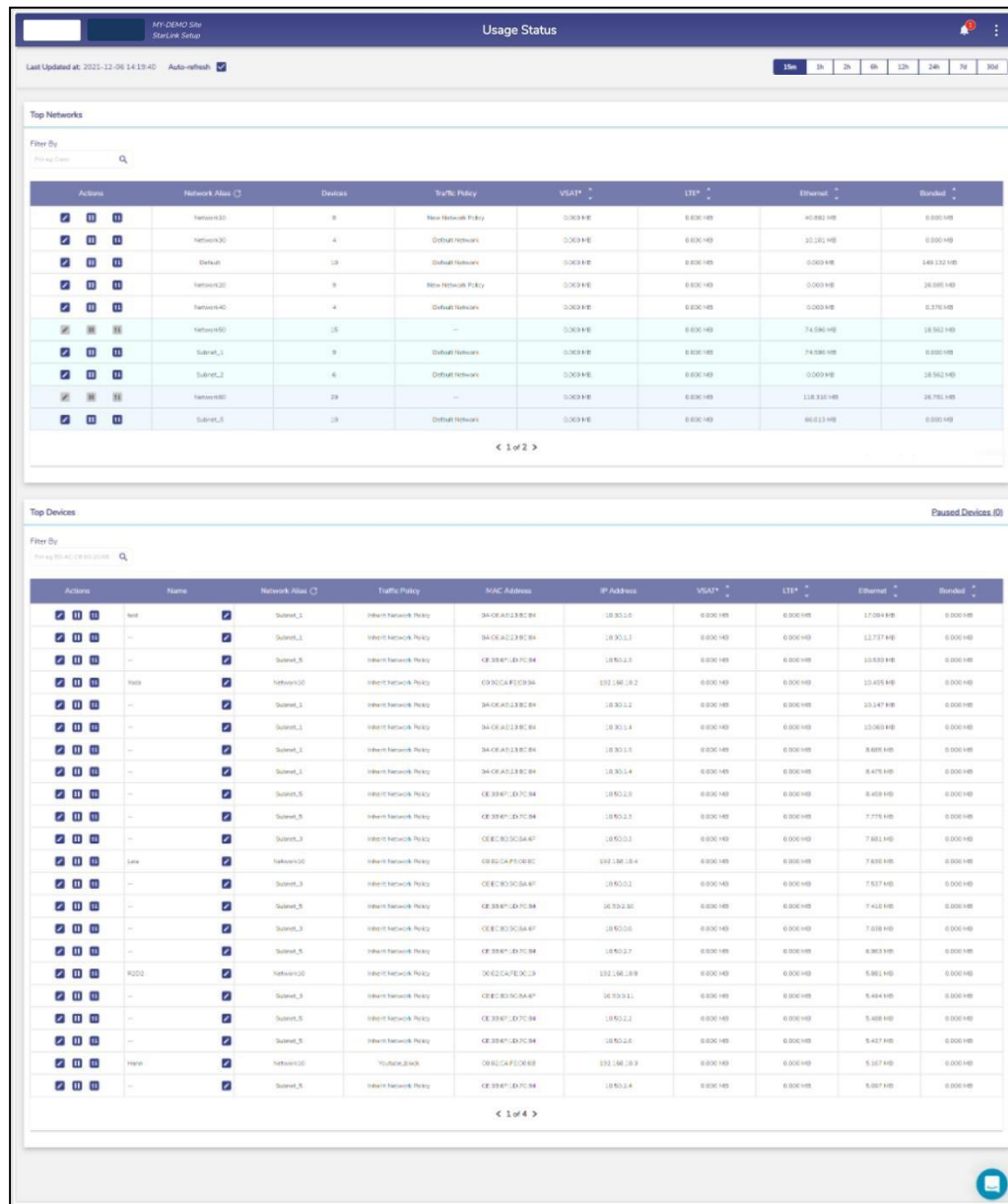


Figure 4.68 Configured Usage Status

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

4.8.1 Top Networks

- This table lists the networks in descending order of the usage. The following details are available under the **Top Networks** section.
- Traffic policy assigned to the network.
- Data usage on each Interface by the network.
- Count of the devices connected to the network.
- The routed access network and corresponding grouping.
- View details of the specific network, user can search for 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 usage of the network based on periodicity, click the duration in the upper right of the page.

4.8.1.1 Modifying Traffic Policy of a Network

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

Steps

- Click  corresponding to the Network in the Action field under the **Top Networks** section. The **Edit Traffic Policy profile** page appears, see figure below.

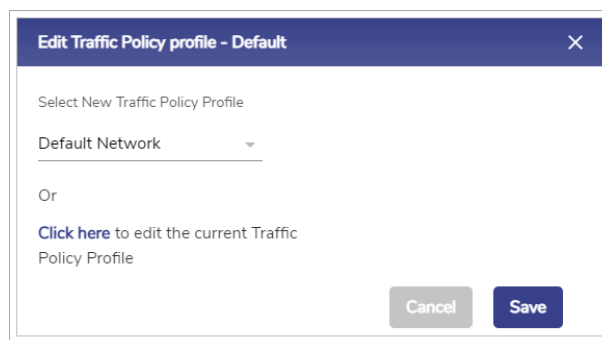


Figure 4.69 Edit Traffic Policy Profile

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

Or,


To modify the current traffic policy, select **Click here**. The **Traffic Policies** page appears. For details, see **3.4 Traffic Policies**.

- Click **Save**.

4.8.1.2 Pausing Traffic on a Network

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

Steps

- Click  corresponding to the routed network in the Action field under the **Top Networks** section. The **Pause Internet** page appears, see figure below.

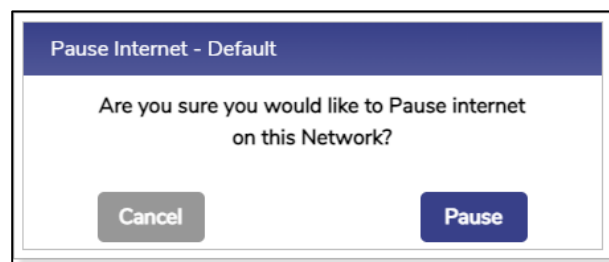



Figure 4.70 Pause Internet

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

Additionally, the pause icon  becomes available corresponding to the network, see figure below.

A screenshot of the "Top Networks" interface. It shows a table with columns: Actions, Network Name, Devices, Traffic Policy, VLAN, VST, Features, and Bandwidth. The first row, "Default", has a red pause icon in the Actions column. The other rows are "Operation", "VST", "Management", and "Core", all with blue play icons in the Actions column.

Actions	Network Name	Devices	Traffic Policy	VLAN	VST	Features	Bandwidth
	Default	0	Default Network	0.000.000	0.000.000	0.000.000	0.000.000
	Operation	0	OPERATION-BLOCK-DEFAULT	0.000.000	0.000.000	0.000.000	0.000.000
	VST	0	SERVICE-NETWORK-BLOCK-DEFAULT	0.000.000	0.000.000	0.000.000	0.000.000
	Management	0	Default Network	0.000.000	0.000.000	0.000.000	0.000.000
	Core	0	CORE-Traffic-POLICY	0.000.000	0.000.000	0.000.000	0.000.000

Figure 4.71 Paused Network

The internet is paused. However, this does not impact the other networks.

4.8.1.3 Resuming Traffic on a Network

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

Steps

- Click  corresponding to the network in the Action field under the **Top Networks** section. The **Resume Internet** page appears, see figure below.



Figure 4.72 Resume Network

- Click **Resume**.

The Internet on the network is resumed.

4.8.1.4 Viewing Top Applications for a Network

To view top application details on a network, perform the following steps.

Steps

- Click  corresponding to the network in the Action field under the **Top Networks** section. The **Traffic Details** page appears, see figure below.

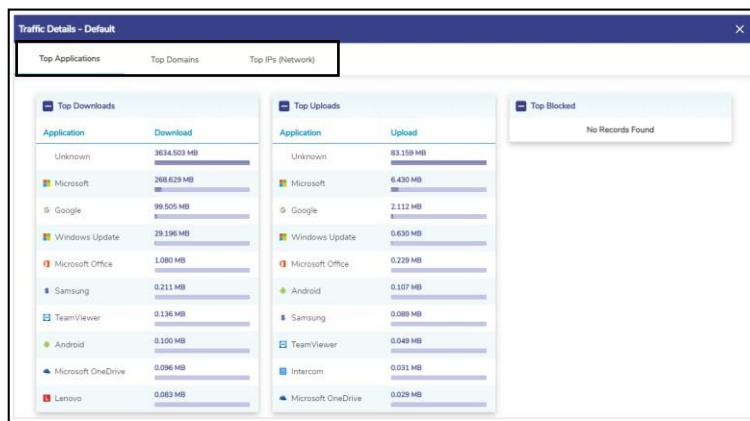


Figure 4.73 Traffic Details

- To view details of the top applications, click **Top Applications**. By default, details of the top applications are available. This shows the **Top Downloads, Uploads and Blocked applications**.
- To view details of the top domains, click **Top Domains**.
- To view details of the top IPs, click **Top IPs (Network)**.

4.8.2 Top Devices

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

- 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 of all the 20 devices become available.
- MAC address of the device.
- IP Address of the device.
- Data consumed by device on interfaces in the network.


To search the device, enter the name of the network in the Filter By field. Details of the network become available.

On the top right of the table, there is Paused Devices hyperlink along with number of paused devices in the system mentioned in brackets.

4.8.2.1 Viewing list of Paused Devices

To view list of Paused Devices, perform the following steps.

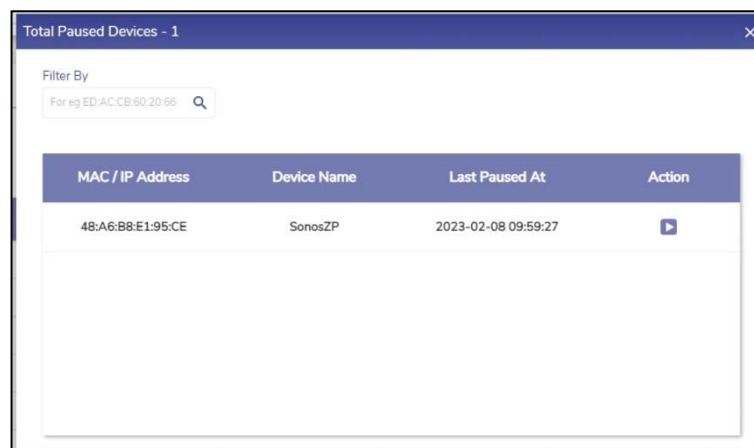
Steps

- Click Paused Devices on the top right of the Top Devices table, see [Figure 4.74 Paused Devices Link](#). The Paused Devices Pop-up appears, see [Figure 4.76 Resume Internet](#). This shows the list of paused devices in the system.
- Click the resume button  next to the paused device to resume internet on that device.



Top Devices									
Paused Devices (1)									
Filter By For eg ED:AC:CB:60:20:66									
Actions	Name	Network Alias	Traffic Policy	MAC Address	IP Address	CELL (2)	ATT Fiber	Bonded	
  	sonytv	 default	none	04:5D:4B:BF:86:B0	192.168.231.100	0.000 MB	14.923 MB	0.000 MB	
  	LAPTOP-61R50M9	 default	none	94:E6:F7:D4:94:D7	192.168.231.17	0.000 MB	2.888 MB	0.000 MB	

Figure 4.74 Paused Devices Link




Total Paused Devices - 1			
Filter By For eg ED:AC:CB:60:20:66			
MAC / IP Address	Device Name	Last Paused At	Action
48:A6:B8:E1:95:CE	SonosZP	2023-02-08 09:59:27	

Figure 4.75 Paused Devices




Figure 4.76 Resume Internet

4.8.2.2 Editing Traffic Policy of a device

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

Steps

- Click  corresponding to the Device in the Action field under the **Top Devices** section. The **Edit Traffic Policy profile** page appears, see figure below.

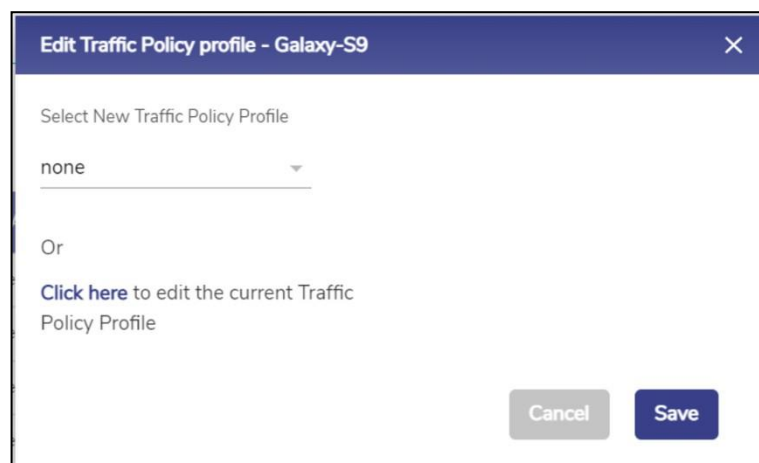


Figure 4.77 Edit Traffic Policy Profile

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

Or,


To modify the current traffic policy, [Click here](#). The **Traffic Policies** page appears. For details, see [3.4 Traffic Policies](#).

- Click **Save**.

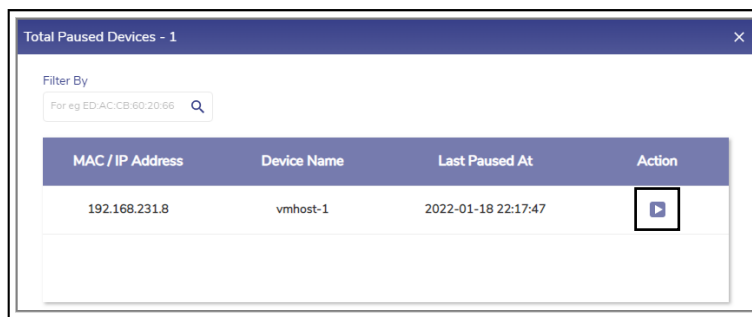
4.8.2.3 Pausing internet on a device

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

Steps

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

The internet is paused. However, this does not impact the other devices in the network.



The screenshot shows a window titled "Total Paused Devices - 1". It contains a search bar labeled "Filter By" with the placeholder text "For eg ED:AC:CB:60:20:66". Below the search bar is a table with the following data:



MAC / IP Address	Device Name	Last Paused At	Action
192.168.231.8	vmhost-1	2022-01-18 22:17:47	

Figure 4.78 Total Paused Devices

4.8.2.4 Resuming internet on a Device

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

Steps

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

The internet is resumed on the device.

4.8.2.5 Viewing Top Applications for a Device

To view top application details for a device, perform the following steps.

Steps

- Click  corresponding to the device in the Action field under the **Top Devices** section. The **Traffic Details** page appears, see figure below.

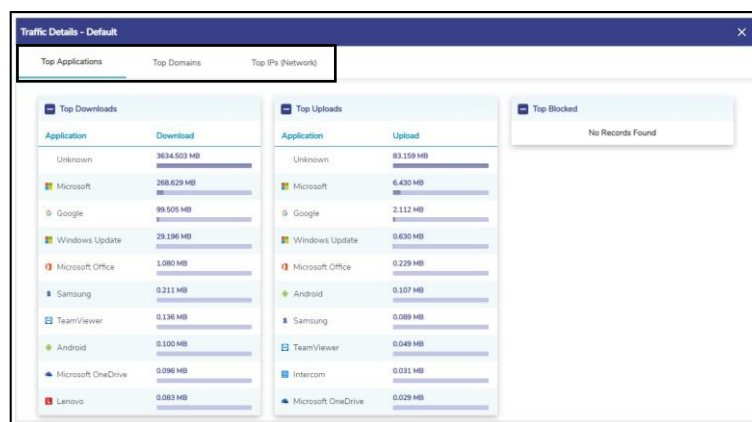


Figure 4.79 Traffic Details

- To view details of the top applications, click **Top Applications**. By default, details of the top applications are available. This shows the **Top Downloads, Uploads and Blocked applications**.
- To view details of the top domains, click **Top Domains**.
- To view details of the top IPs, click **Top IPs (Network)**.


4.9 VSAT Controller

Once the EdgeOS System is configured, user can view analytics from the VSAT modem connected to the EdgeOS System. If VSAT-LEO (Starlink) is available on the system, then analytics from Starlink modem can also be viewed. There are different sub screens for each of the VSATs on the VSAT Controller.

4.9.1 Viewing VSAT Analytics

To view the VSAT controller, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **VSAT Controller**. The **VSAT Controller** page appears, see figure below.

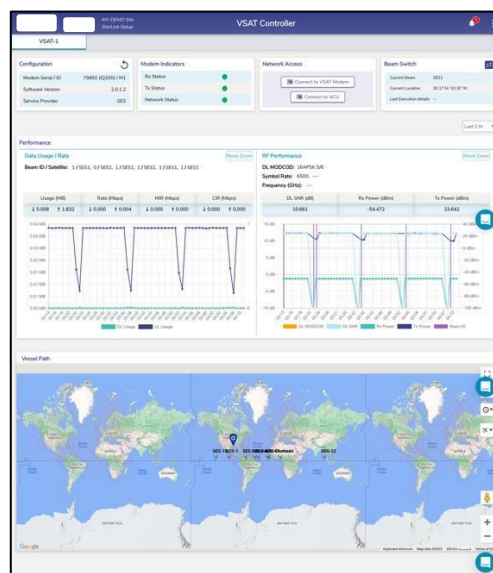






Figure 4.80 VSAT Controller Page

To view the details of VSAT, click the **VSAT-1** tab. For details of the VSAT controller, see Table below.

Fields	Description	Configuration
Configuration	Following details of the VSAT Controller becomes available. <ul style="list-style-type: none"> VSAT modem serial number VSAT modem software version Date and time when the details were uploaded 	To upload the new configuration file of the VSAT modem, click  and then upload the configuration file.
		To reboot the VSAT modem, perform the following steps. <ul style="list-style-type: none"> VSAT modem, click . see Figure 4.81 Reboot Modem. The confirmation message is displayed, see Figure 4.82 Reboot VSAT Modem Confirmation Message. Click Confirm. The VSAT modem takes a few minutes to come up.
Modem Indicators	Following details of the VSAT modem becomes available. <ul style="list-style-type: none"> Receive (Rx) status. Transmit (Tx) status. Network status 	N/A
Network Access	To access the VSAT modem and ACU.	To connect to the VSAT modem, click Connect to VSAT Modem.

		To connect the ACU, click Connect to ACU .
Beam Switch	The details of the beam currently used by the VSAT are displayed.	<p>To switch to a distinct beam, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click , see Figure 4.83 Beam Switch. The VSAT Beam Switch pop-up window appears, see Figure 4.84 VSAT Beam Switch Pop-up. In the Beam to switch to list, click the beam to be switched. <hr/> <p>In the list, highlighted beams are available based on priority.</p> <p>The non-highlighted beams may not provide coverage at the vessel's location.</p> <ul style="list-style-type: none"> Click Proceed. <p>The Beam switch is successfully performed.</p> <hr/> <p>Before switching to the distinct Beam, user must ensure that the VSAT network is in the network.</p>
Vessel Path	This shows the site location and its voyage path on map interface.	<p>To view the Beam and Satellite details, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click , see Figure 4.85 Site.



		<ul style="list-style-type: none"> The connected beam and satellite details along with latitude and longitude appear. <p>To view the voyage path for a time duration, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  icon on the top right of the map, see Figure 4.86 Voyage . Select start and end date of the duration for which user wants to see the path. The voyage path appears on the map, see Figure 4.87 . <p>To view satellites for a particular service provider, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  icon on the top right of the map, see Figure 4.83 Beam Switch Figure 4.85 Site . Select the satellites of the service provider that user wants to see on the map. The map will show these satellites only and hide the satellites of the unchecked service provider, Figure 4.88 Satellite Selection Pop-up.
--	--	---

Table 4-16 VSAT Controller Information

Configuration

Modem Serial / ID

79492 (iQ200) / M1

Software Version

2.0.1.2

Service Provider

SES

Figure 4.81 Reboot Modem

×

Please confirm to reboot the VSAT modem.

Note that the modem will take a few minutes to come back up.

Cancel

Confirm

Figure 4.82 Reboot VSAT Modem Confirmation Message

Beam Switch

Current Beam

SES1

Current Location

30.17 N / 91.97 W

Last Execution details

--

Figure 4.83 Beam Switch

VSAT Beam Switch

The VSAT Terminal is currently connected to: SES1

Select Beam to switch to

Note:

- Highlighted Beams are priority-ordered. Non-highlighted Beams likely do not provide coverage at the vessel's location.
- The Beam Switch requires the VSAT remote to be "in network".
- The Beam Switch can take up to 5-10 minutes to perform.

Proceed

Figure 4.84 VSAT Beam Switch Pop-up



Figure 4.85 Site Location

A pop-up form for selecting voyage duration. It features a background map of Asia. The form contains the following fields and controls:

- Start Date:** 02/01/2023 (with a calendar icon)
- End Date:** 02/07/2023 (with a calendar icon)
- Apply:** A blue button to confirm the selection.

Figure 4.86 Voyage Duration Pop-up

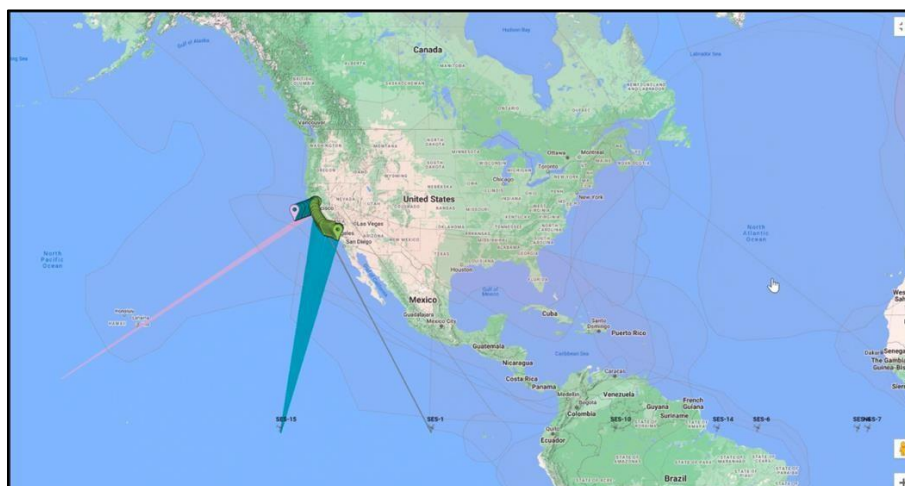


Figure 4.87 Site Voyage Path

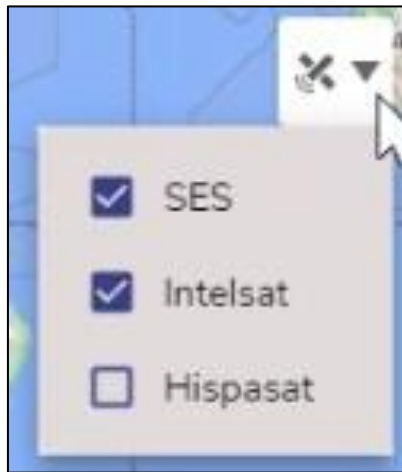


Figure 4.88 Satellite Selection Pop-up

To view the performance chart based for a particular periodicity, in the periodicity list click the periodicity. The following details become available under the **Performance** section.

- Data Usage / Rate
- Beam ID / Satellite
- Usage (MB)
- Rate (Mbps)
- MIR (Mbps)
- CIR (Mbps)
- RF (VSAT Modem) Performance
- Modulation constellation (MODCOD). This indicates the constellation and FEC code rate.
- DL SNR (dB)
- Receive (Rx) power (dBm). ≥ -60 dBm is a good Rx power.
- Transit (Tx) power (dBm). ≥ 30 is a good Tx power.

4.9.2 Viewing Starlink Analytics

To view details of Starlink, click on STAR 1 tab, following sub screen appears, see figure below. If there are two Starlink interfaces in the systems, then two such tabs will be present on the Controller page.

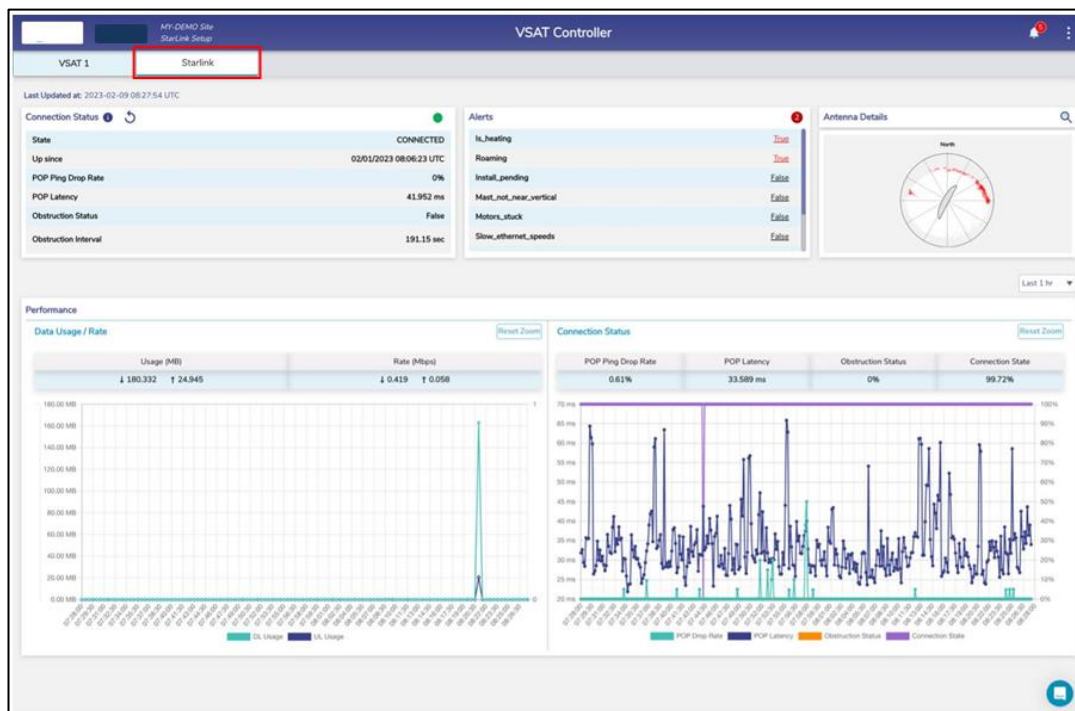


Figure 4.89 Starlink Information

For details of the Starlink controller, see Table below.

Fields	Description	Configuration
Connection Status	<p>Details of connection status become available.</p> <ul style="list-style-type: none"> State (● stands for Up and ● stand for Down). 	<p>To view modem software and hardware information, click i and the overlay for configuration details appears, see Figure 4.90 Connection Status.</p>



	<ul style="list-style-type: none"> • Up since • POP Ping Drop Rate • POP Latency • Obstruction Status • Obstruction Interval 	<p>To reboot the VSAT modem, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Connection status, click . see • The confirmation message is displayed, see Figure 4.91 VSAT Starlink Reboot. • Click Confirm. <p>The VSAT Starlink modem will take a few minutes to come up.</p>
Alerts	Any active alerts are shown at the top of the list and the counter shows number of active alerts. On clicking the individual alerts, the historical details of when that specific alert was raised is available.	<p>To view alert details, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click an alert. <p>Alert details Pop-up appears, see Figure 4.92 Alert Details.</p>
Antenna Details	This provides the current obstruction view for the antenna and the current antenna azimuth.	<p>To view enlarged image of the current obstruction, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click  on the top right of this image. <p>Enlarged view of the obstruction is available, see Figure 4.93 Enlarged view of Antenna Details.</p>

Table 4-17 Starlink Controller Information

Connection Status ? ↺	
Configuration	CONNECTED
Id : ut01000000-00000000-001ab1de	02/01/2023 08:06:23 UTC
Software Version : 191e4dfa-d63a-46b1-a73b-9fa907733864.uterm.release	0%
Hardware Version : hp1_proto0	
POP Latency	37.714 ms
Obstruction Status	False
Obstruction Interval	227.368 sec

Figure 4.90 Connection Status

Alert

Please confirm to reboot the modem.

Note that the modem will take a few minutes to come back up.

Cancel

Confirm

Figure 4.91 VSAT Starlink Reboot

Alert Details

Alert - Is_heating

Current Status - True

Last Raised At - 2023-02-09 08:11:00 UTC

Total raised since 7 days - 3

Raised at (Duration) -

2023-02-09 08:11:00 UTC (41 min)

2023-02-09 05:59:00 UTC (1 hr 51 min)

2023-02-09 04:57:00 UTC (1 hr 2 min)

View More

Figure 4.92 Alert Details

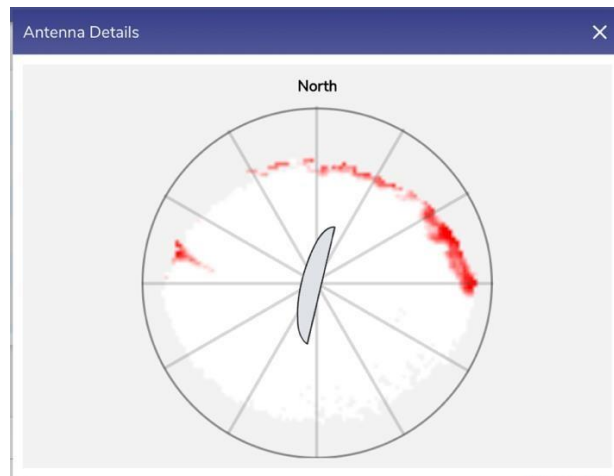


Figure 4.93 Enlarged view of Antenna Details

To view the charts based on the periodicity, in the periodicity list click the periodicity, see [Figure 4.94 Periodicity Selection](#).

The following details become available under the **Performance** section.

- Data Usage / Rate
- Usage (MB)
- Rate (Mbps)

The following details become available under the **Connection Status** section.

- POP Ping Drop Rate
- POP Latency
- Obstruction Status
- Connection State

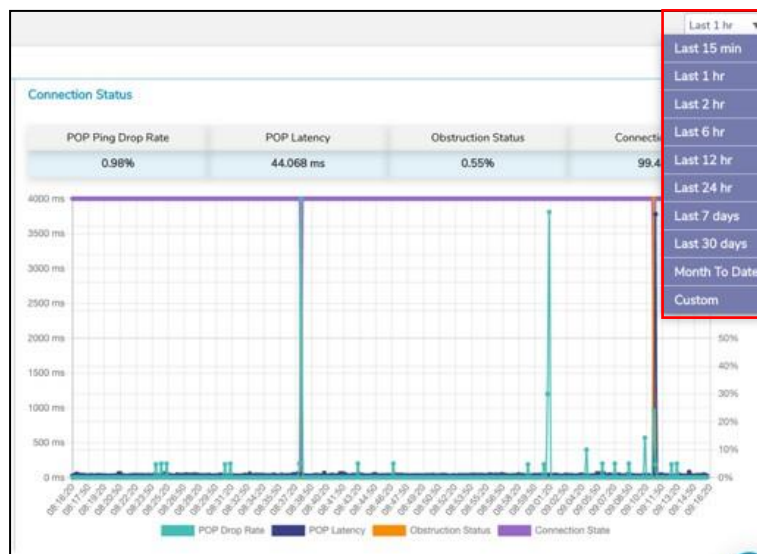


Figure 4.94 Periodicity Selection


4.10 Cellular Controller

Once the EdgeOS System is configured, user can view analytics from the Cellular modem(s) connected to the EdgeOS System provided the access details (login/password) are available and updated as part of server configuration. If Ext5G interface is configured on the system, then analytics from this modem are also available on the Cellular Controller on a separate tab.

4.10.1 Viewing Cellular Analytics

To view the Cellular controller, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Cellular Controller**. The **Cellular Controller** page appears, see figure below.

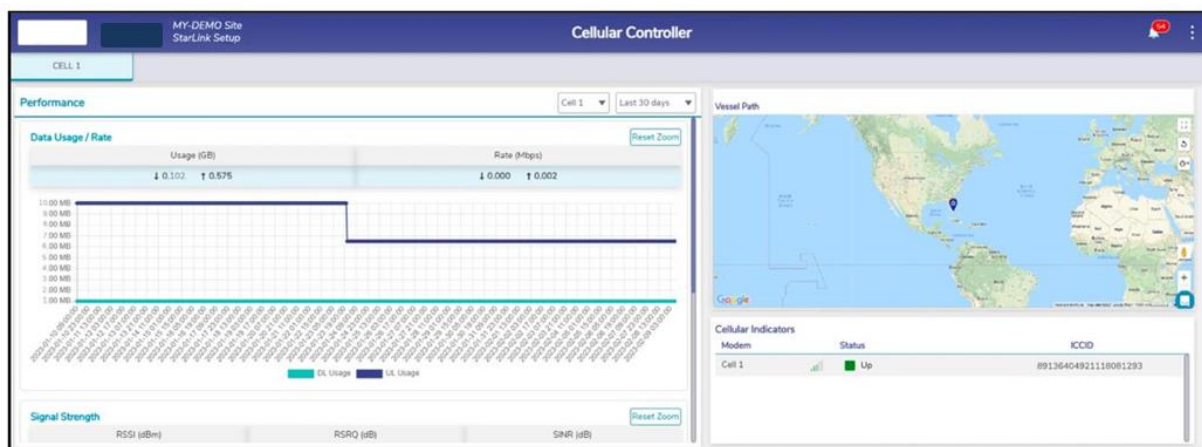


Figure 4.95 Cellular Controller

To view the performance chart based for a particular cellular interface, click on the Cellular dropdown. If there is only one modem, the interface alias name corresponding to the cellular interface is available in the Cellular field.

To view the performance chart based for a particular periodicity, in the periodicity list click the periodicity.





The following details become available under the **Performance** section.

- Data Usage / Rate
- Usage (MB)
- Rate (Mbps)
- Signal Strength
- RSSI (dBm)
- RSRQ (dB)
- SINR (dB)

For details of the signal strength, see [Table 4-19 Signal Strength](#).

Details of the information on the Cellular Indicator is listed in the below table.

Fields	Description	Configuration
Modem	Displays the cells and the respective signal strength.	To view the details of a cell, click the cell. The cell details pop-up window appears, see Figure 4.96 Cellular Indicator .
		To view the signal strength of the cell, point the mouse to the signal corresponding to the cell. For details of the signal strength, see Table 4-19 Signal Strength .

Status	<p>Displays one of the following statuses of the modem of the respective cell.</p> <ul style="list-style-type: none"> . This indicates that the modem is active and in use. . This indicates that the modem is inactive and not in use. Displays the name of the network operator. 	N/A
ICCID	Displays the unique ICCID number of the SIM that is in use.	N/A
Vessel Path	This shows the site location on map interface.	<p>To view the Vessel/Site Location details, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click , see Figure 4.95 Cellular Controller. The latitude and longitude details appear. <p>To view the voyage path for a time duration, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  icon on the top right of the map, Figure 4.98 Vessel Path Pop-up.

		<ul style="list-style-type: none"> Select start and end date of the duration for which user wants to see the path. <p>The voyage path appears on the map.</p>
--	--	--

Table 4-18 Cellular Indicator Details

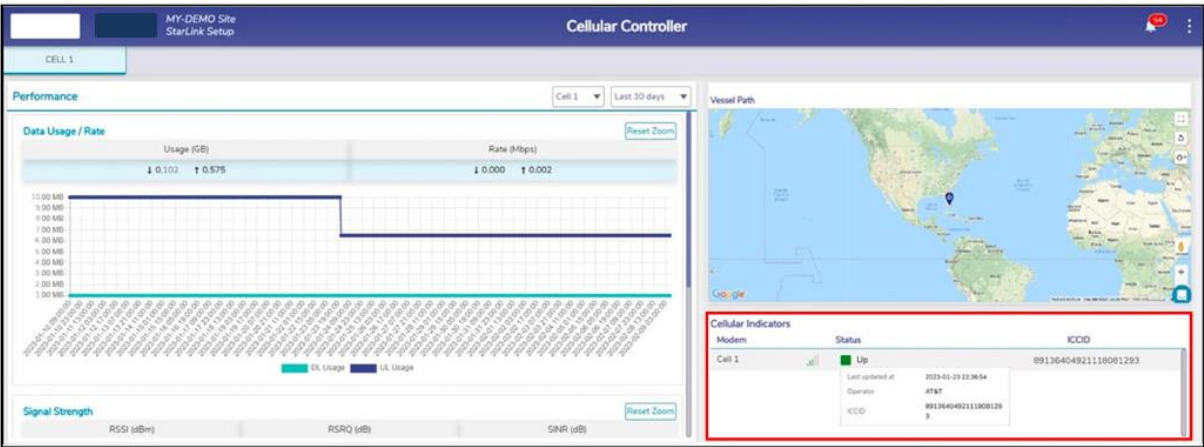


Figure 4.96 Cellular Indicator

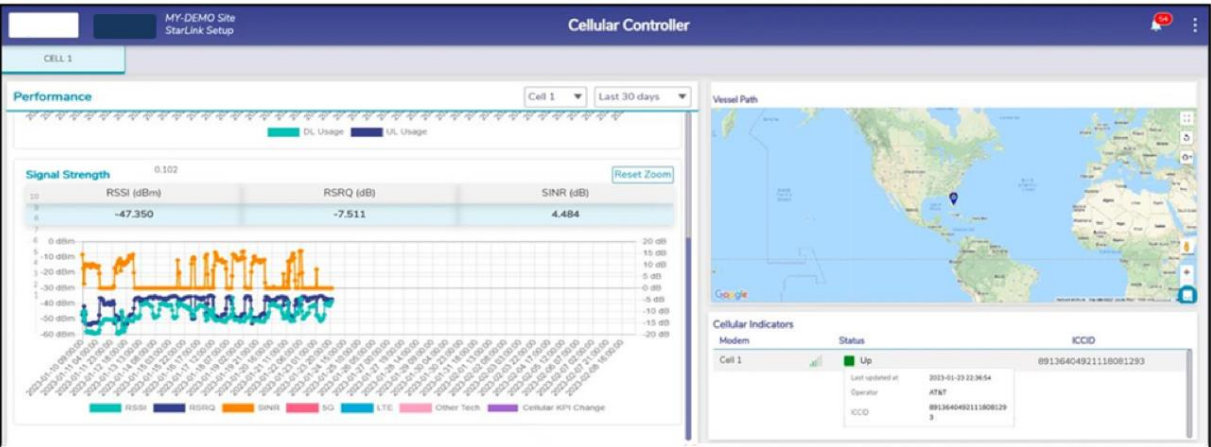


Figure 4.97 Signal Strength

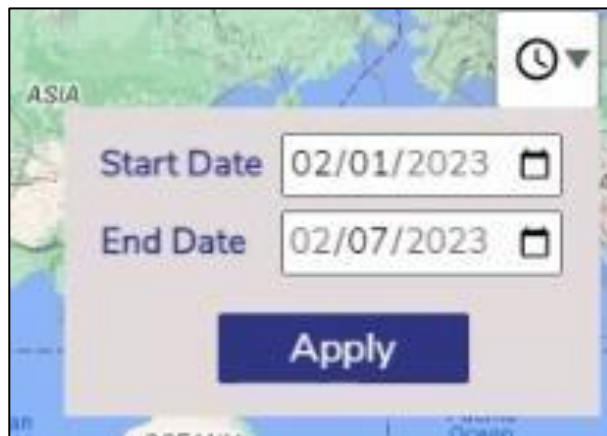


Figure 4.98 Vessel Path Pop-up

Signal Strength Range	Status
Received Signal Strength Indicator (RSRI) dBm	
-65 or near to zero (0)	Excellent
-65 to -75	Good
-75 to -85	Mid Cell
-85 or -95	Poor
-95 or less	No signal
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

Table 4-19 Signal Strength

4.10.2 Viewing Ext5G Analytics

Once the Ext5G is configured on the EdgeOS System, user can view analytics from the modem.

To view the Ext5G controller, perform the following steps.

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Cellular Controller**. The **Cellular Controller** page appears, see figure below. There are two tabs, first for CELL 1 as in the above section and second for Ext5G.

Note: It is possible that there is no Cellular interface on the system other than Ext5G, in which case there will be only one tab on the Cellular Interface. Click on Ext5G tab to view the analytics of Ext5G.

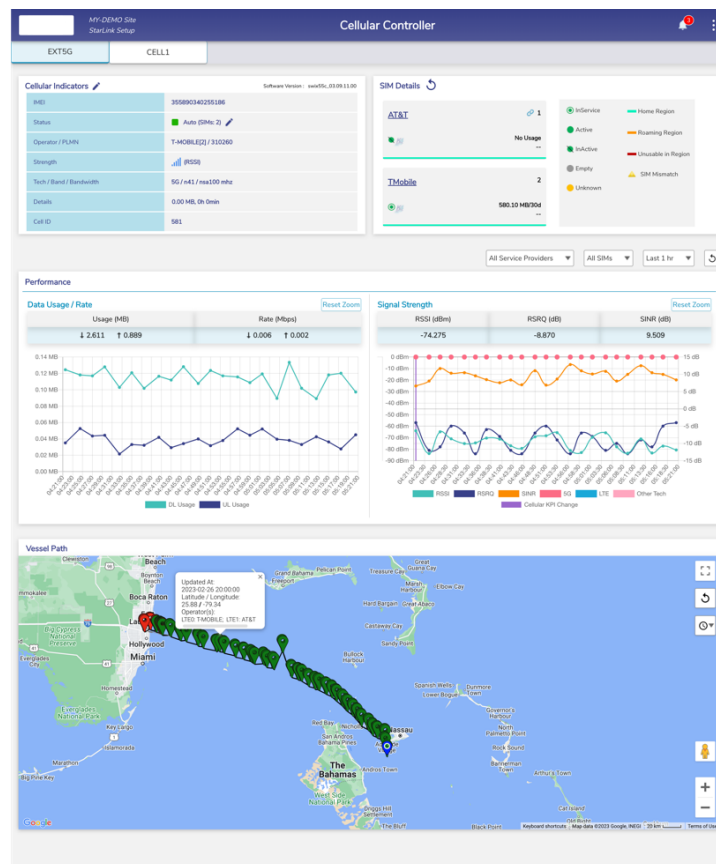








Figure 4.99 Cellular Controller

- For details about the Ext5G Controller, see table below.

Fields	Description	Configuration
Software Version	The version of the Ext5G Modem Firmware.	N/A
IMEI	IMEI of the modem.	N/A
Status	Displays the status of the modem. Additionally, specifies the SIM Priority Configuration (Auto or Manual) and the number of SIMs.	<p>SIM Priority Configuration is set to 'Auto' by default.</p> <p>To update SIM Priority Configuration, perform the following steps.</p> <p>Steps</p>

	<ul style="list-style-type: none"> • . This indicates that the modem is active and in use. • . This indicates that the modem is inactive and not in use. 	<ul style="list-style-type: none"> • Click  next to status field. The SIM Priority Configuration popup appears, see Figure 4.100 SIM Priority Settings. • Click radio button next to Manual. The SIM Slot Priority field becomes enabled. • Enter the SIM Slots in priority order of the preference, see Figure 4.101 SIM Priority Settings - Manual. • Click Save. • User can click Advanced Settings to update the remaining fields such as SIM Connection Retry Count and Network Performance Thresholds, see Figure 4.102 SIM Priority Advanced Settings.
Operator/PLMN	<p>The name of the service provider and slot number of the SIM in which the SIM of that service provider is inserted is displayed in the following format.</p> <p>The name of the service provider [Number of the SIM slot in which the SIM is inserted]</p> <p>This is an example.</p> <p>T-Mobile[2]</p>	N/A

	Additionally, PLMN is specified.	
Strength	The strength of the signal (RSSI, RSRP, RSRQ) is displayed on hover.	To view the signal strength of the cell, point the mouse to the signal corresponding to the Strength field.
		<p>To lock the modem, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click  corresponding to the Cellular Indicators. The Cellular Actions page, appears, see Figure 4.103 Cellular Actions. Click Cell Lock/Unlock/Reset. The cell lock/unlock becomes available, see Figure 4.104 Cellular Actions Options. In the Select Cell list, click a cell whose modem is to be locked. In the Select Operation list, click Lock Modem. The Proceed button becomes available. Click Proceed. Click OK <p>The cell locking process starts, see Figure 4.106 Cell Lock in Progress. Once the modem is locked, a successful message is displayed, see Figure 4.107 Cell Lock Successful.</p>

	User can unlock the Modem.	<p>To unlock the modem, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click  corresponding to the Cellular Indicators. The Cellular Actions page, appears, see Figure 4.103 Cellular Actions. • Click Cell Lock/Unlock/Reset. The cell lock/unlock becomes available, see Figure 4.104 Cellular Actions Options. • In the Select Cell list, click a cell whose modem is to be unlocked. • In the Select Operation list, click Unlock Modem. The Proceed button becomes available. • Click Proceed. • Click OK. <p>The cell unlocking process starts, see Figure 4.108 Cell Unlock in Progress.</p> <p>Once the cell is unlocked, a successful message is displayed, see Figure 4.109 Cell Unlock Successful.</p>
	User can reset the Modem.	<p>To reset the modem, perform the following steps.</p> <ul style="list-style-type: none"> • Click  corresponding to the Cellular Indicators. The Cellular Actions page, appears, see Figure 4.103 Cellular Actions.

		<ul style="list-style-type: none"> Click Cell Lock/Unlock/Reset. The cell lock/unlock becomes available, see Figure 4.103 Cellular Actions. In the Select Cell list, click a cell whose modem is to be reset. In the Select Operation list, click Reset Modem. The Proceed button becomes available. Click Proceed. The Alert pop-up window appears, see Figure 4.105 Ext5G Connectivity Alert. Click OK. <p>Modem reset starts, see Figure 4.110 Cell Reset In Progress The modem will be down, and the status of the cell is reflected by the red square. Therefore, the Cellular connectivity will be down.</p> <p>Once the modem resets a successful message is displayed, see Figure 4.111 Cell Reset Successful.</p> <p>In addition to this, the Cellular controller will again scan and select the operator to connect for the Cellular connectivity.</p>
Tech/ Band/ Bandwidth	The technology, band and bandwidth of the signal is displayed.	N/A
Details	If the modem is active, then the data consumed with duration is displayed. Else	N/A

	the status of the operator is displayed.	
Cell ID	The ID of the Ext5G Modem is displayed.	N/A

Table 4-20 Cellular Indicators

SIM Priority Settings

SIM Priority Configuration ☒ Auto ☐ Manual

SIM Slot Priority ? 2

Priority	SIM Slot	Service Provider	ICCID
Prio 1	2	T-Mobile	8901260882259423157

[Advanced Settings >](#)

Figure 4.100 SIM Priority Settings

SIM Priority Settings

SIM Priority Configuration

☐ Auto
☒ Manual

SIM Slot Priority

2

Priority	SIM Slot	Service Provider	ICCID
Prio 1	2	T-Mobile	8901260882259423157

Advanced Settings >

Cancel

Save

Figure 4.101 SIM Priority Settings - Manual

SIM Priority Settings

SIM Priority Configuration

☐ Auto
☒ Manual

SIM Slot Priority

2

Priority	SIM Slot	Service Provider	ICCID
Prio 1	2	T-Mobile	8901260882259423157

Advanced Settings ▾

SIM Connection Retry Count (Range 3-25)

5

Retry Higher Priority SIM Frequency (Range 1-24 hrs)

☐ 1

Network Performance Thresholds

Minimum SNR (Range -10 to 20 dB)

☐ -3

Minimum RSSI (Range -105 to -60 dBm)

☐ -90

Minimum Speed (Range 0.1 to 50 Mbps)

☐ 0.1

Threshold Interval (Range 1 to 180 min)

☐ 1

Cancel

Save

Figure 4.102 SIM Priority Advanced Settings

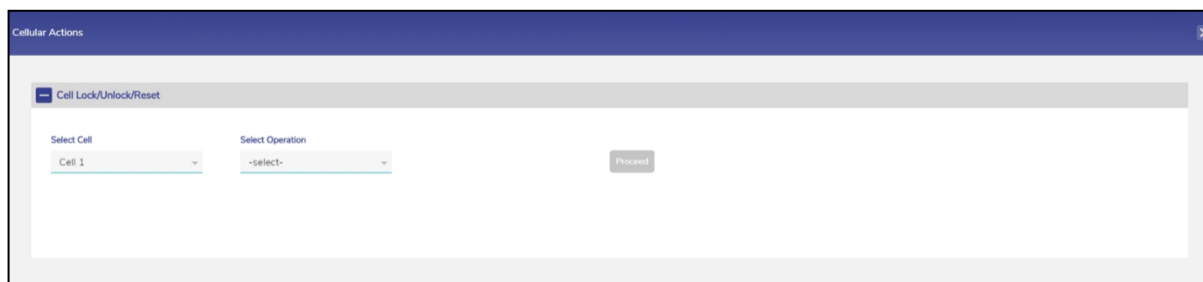


Figure 4.103 Cellular Actions



Figure 4.104 Cellular Actions Options

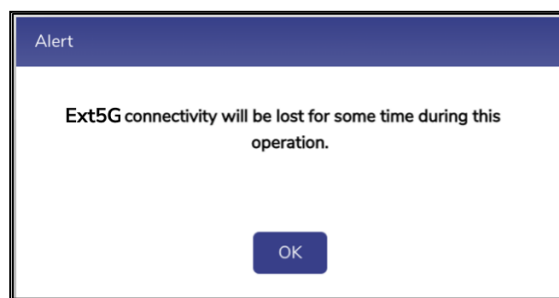


Figure 4.105 Ext5G Connectivity Alert

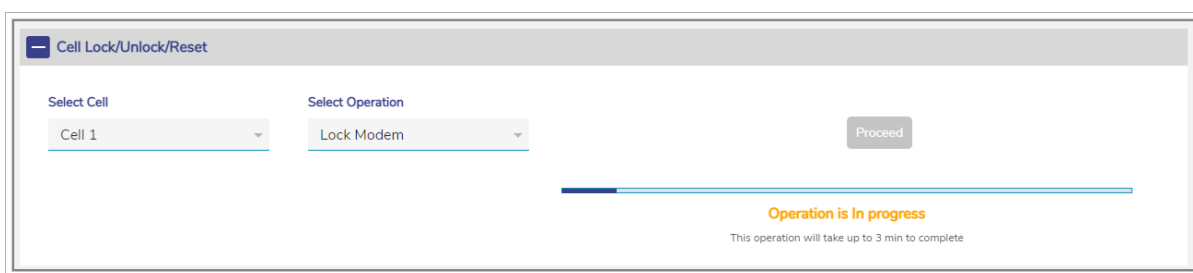


Figure 4.106 Cell Lock in Progress

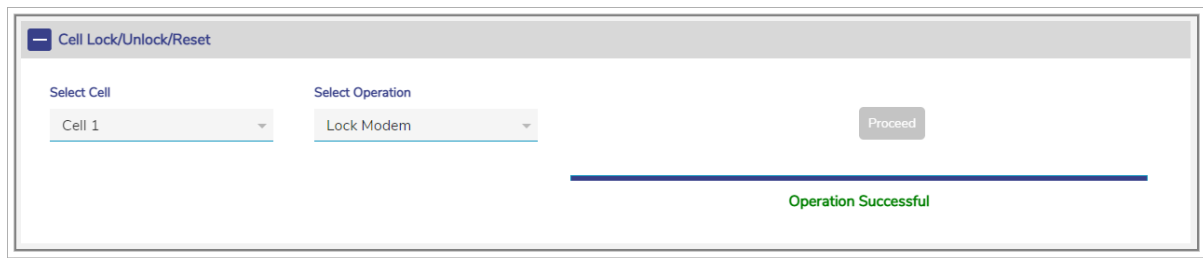


Figure 4.107 Cell Lock Successful

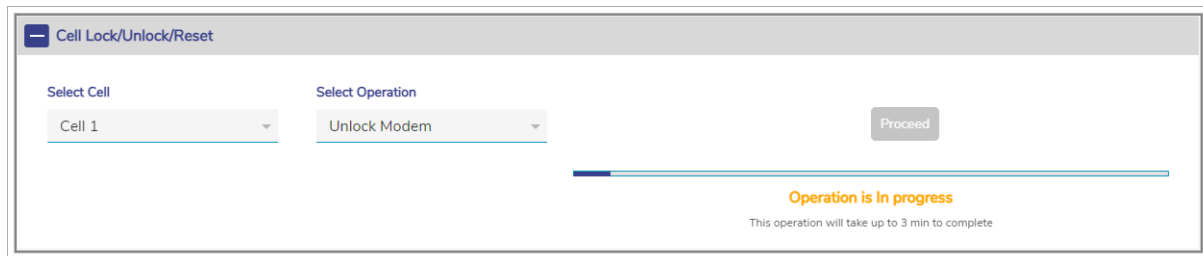


Figure 4.108 Cell Unlock in Progress

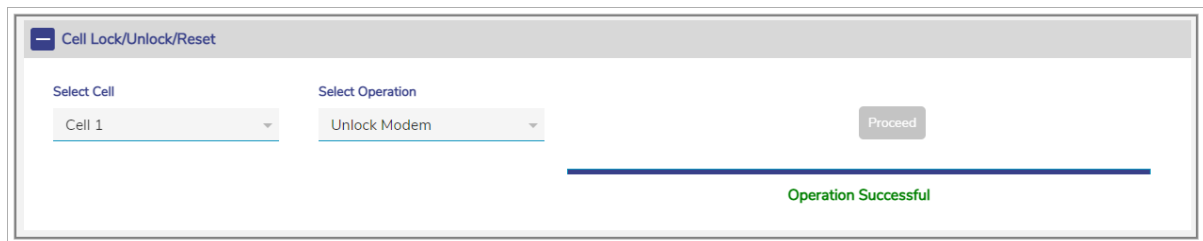


Figure 4.109 Cell Unlock Successful

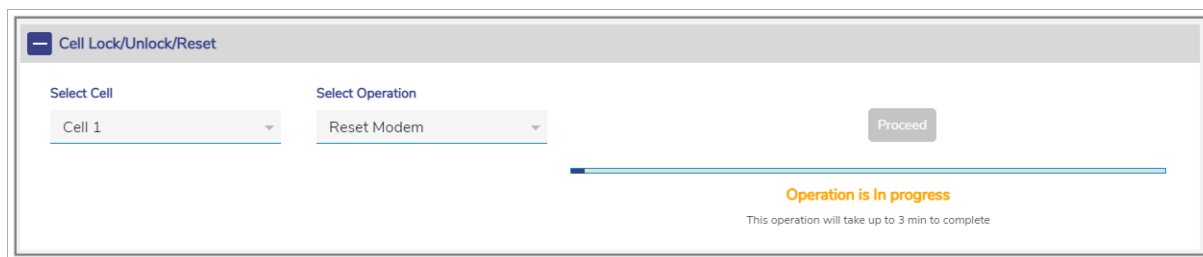


Figure 4.110 Cell Reset In Progress

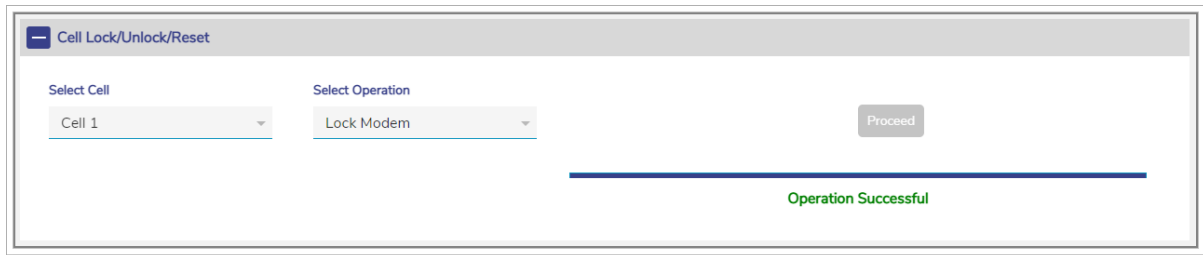













Figure 4.111 Cell Reset Successful

Fields	Description	Configuration
SIM Details	<p>The Ext5G modem supports 2 SIMs.</p> <p>The following details are displayed per SIM.</p> <ul style="list-style-type: none"> Name of the service provider. Physical slot number. Duration since the SIM is in use or service. Data usage. Registration details. <p>One of the following states of the SIM.</p> <ul style="list-style-type: none">  InService. This indicates that the SIM is in use.  Active. This indicates that the SIM is available, but it is not in use. 	<p>To create the performance chart based on the data usage and signal strength, click  under the service provider. The chart becomes available, see Figure 4.112 Performance Charts.</p>
		<p>To view details about a SIM, click the service provider. The Slot SIM Details pop-up window appears, see Figure 4.113 Details of Active or Inactive SIMs.</p>
		<p>If the SIM registration is denied, then  is displayed next to the name of the service provider.</p> <p>Point the mouse to , the registration denied message is displayed. In addition to this, MCC and MNC are displayed.</p>

	<ul style="list-style-type: none"> •  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. 	
	<p>User can lock or disable the SIM whose current state is defined as Active or InActive.</p> <p>Once the SIM is locked, user cannot perform the intended tasks from that SIM.</p> <p>User cannot lock the SIM whose status is defined as Unknown.</p>	<p>To lock the SIM whose status is defined as Active or InActive, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see Figure 4.113 Details of Active or Inactive SIMs. • Click Disable in the Disable/Enable SIM field. • Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. • Click OK. <p>The SIM is locked and  is displayed next to the name of the service provider to reflect that the SIM is locked. Once the SIM is</p>





		locked, user cannot perform the intended tasks from that SIM.
	The user can lock or disable the SIM that is in use or whose current state is defined as InService.	<p>To lock the SIM whose status is defined as InService, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see Figure 4.115 Details of Inservice SIM. • Click Disconnect. The call is disconnected, and the state is defined as Active in the State field., see Figure 4.116 State of InService SIM after the Call is Disconnected. • Click Disable in the Disable/Enable SIM field. • Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. • Click OK. <p>The SIM is locked and  is displayed next to the name of the service provider to reflect that the SIM is locked. Once the SIM is locked, user cannot perform the intended tasks from that SIM.</p>
	The user can unlock or enable the SIM.	<p>To unlock the SIM, perform the following steps.</p> <p>Steps</p>


		<ul style="list-style-type: none"> Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see Figure 4.117 Details of Locked SIM for Manual Settings. Click Enable in the Disable/Enable SIM field. Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. Click OK. <p>The SIM is unlocked and  is removed. Now user can perform the intended tasks.</p> <p>The SIM which was in use previously or in the previous state was InService, will automatically connect to the network, and the state is again defined as InService.</p>
	<p>By default, the APN is configured for every SIM to connect to the specific service provider. However, user can manually configure the APN.</p>	<p>To manually modify the APN settings, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see Figure 4.118 Details of Locked SIM for Auto Settings. Click Manual in the Auto/Manual SIM field. The APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection sections become available, see Figure 4.119 APN Settings, Data Roaming,

		<p><i>LTE/3G Selection, and Carrier Selection Sections.</i></p> <ul style="list-style-type: none"> • Enter the APN in the APN field. • Enter the username in the Username field. • Enter the password in the Password field. • Click Save. The Alert pop-up window appears, see <i>Figure 4.114 SIM Configuration Alert.</i> • Click OK. <p>The APN is configured.</p>
	<p>By default, the data roaming is turned off for every SIM. Therefore, the data will not be available in the visitor network. However, user can turn on the data roaming.</p> <p>The user can block and allow the MCC of a country.</p>	<p>To turn on the data roaming, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see <i>Figure 4.118 Details of Locked SIM for Auto Settings.</i> • Click Manual in the Auto/Manual SIM field. The APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection sections become available, see <i>Figure 4.119 APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection Sections.</i> • Click Enable in the Data Roaming section.

		<p>The blocked MCCs' are displayed in the Block List under the Data Roaming section.</p> <p>And,</p> <p>The allowed MCCs' are displayed in the Allow List under the Data Roaming section.</p> <ul style="list-style-type: none"> • Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. • Click OK. <p>The data will be available on roaming.</p>
	<p>By default, the LTE/3G/5G (Auto) is selected.</p> <p>However, user can configure the SIM to connect only to the 5G of the service provider (carrier).</p>	<p>To configure the SIM to connect only to the 5G network, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears see Figure 4.118 Details of Locked SIM for Auto Settings. • Click Manual in the Auto/Manual SIM field. The APN Settings, Data Roaming, LTE/3G/5G Selection, and Carrier Selection sections become available, see Figure 4.119 APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection Sections.

		<ul style="list-style-type: none"> Click 5G Only in the LTE/3G/5G Selection field. Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. Click OK. <p>By default, Auto is selected in the LTE/3G Selection field.</p> <hr/> <p>The user must select the 5G Only while configuring the PLMN.</p> <p>If the SIM is in use with a current Cellular radio, then the call will drop using that SIM.</p>
	<p>The user can configure the cellular parameters, PLMN MCC & MNC settings of the service provider (carrier) for every SIM to connect only to the specific service provider (carrier).</p> <p>By default, the carrier selection for every SIM is configured to Auto.</p>	<p>To configure the network selection, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> Click the service provider in the SIM Details section. The Slot SIM Details pop-up window appears, see Figure 4.118 Details of Locked SIM for Auto Settings.
	<p>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</p>	<ul style="list-style-type: none"> Click Manual in the Auto/Manual SIM field. The APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection sections become available, see Figure 4.119 APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection Sections. Click Manual in the Carrier Selection section. The Select Carrier section

	<p>the current geographical location but may not function in a distinct geographical location.</p> <p>This is an example.</p> <p>If the vessel is in geographical location A, then based on the PLMN settings, the SIM continues to work in that geographical location.</p> <p>If the vessel sails to geographical location B, then based on the PLMN settings, the SIM may not work in that geographical location.</p> <p>To simplify the MCC/MNC configuration for the SIM, based on the current geographical location, the EdgeOS system provides Cellular Scan Output and updates for that SIM.</p>	<p>becomes available, see Figure 4.120 Carrier Selection Configuration.</p> <hr/> <p>To view the MCC/MNC reference, click  next to the Carrier Selection section. The MCC/MNC reference pop-up window appears, see Figure 4.121 MCC/MNC Reference Link.</p> <ul style="list-style-type: none"> • The carrier Name/Alias and MCC/MNC are displayed under the Scan Output section. • The saved profiles are displayed under the Saved Profiles section. • To delete the entire saved profiles, click  next to the Saved Profiles section. • Enter the name of the carrier or alias in the Set Carrier Name/Alias field. <p>Or,</p> <p>Select the name of the carrier or alias and MCC/MNC from the scan output displayed under the Scan Output section.</p> <ul style="list-style-type: none"> • Click Save. The Alert pop-up window appears, see Figure 4.114 SIM Configuration Alert. • Click OK. <p>The PLMN is configured. The icon  is displayed next to the name of the service provider to reflect that the custom PLMN settings are implemented for that service provider. Point the mouse to the icon .</p>
--	---	---

		<p>The following details of the SIM are displayed.</p> <ul style="list-style-type: none"> • Custom PLMN. • MCC/MNC. • Name of the service provider.
	<p>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 perform the SIM Reload procedure. LTE service must be restarted. Therefore, the SIM bank will restart.</p>	<p>To perform the SIM Reload procedure, perform the following steps.</p> <p>Steps</p> <ul style="list-style-type: none"> • Click  next to the SIM Details. The SIM Reload pop-up window appears, see Figure 4.122 SIM Reload. • Click Reload. <p>The LTE service restarts. Therefore, the SIM banks are reset. Details of the SIMs become available.</p>
	<p>The EdgeOS System supports third party SIMs. The SIM that is provided by K4 is deemed to be the K4 SIM.</p> <p>The SIM that is not provided by K4 is deemed to be the third-party SIM.</p>	N/A




	 is displayed next to the SIM whose details are not available in the database.	N/A
	<p>Provides information about the SIMs that are not available in the slot.</p> <p>However, details about the SIMs are available in the database.</p>	<p>To view details about the missing SIMs, point the mouse to . A list of the missing SIMs is displayed.</p>

Table 4-21 SIM Details



Figure 4.112 Performance Charts

Slot 2 SIM Details

SIM Details

State	Active
Service Provider	AT&T
IMSI	310030003124796
ICCID (8)	89010303300031247969

Disable/Enable SIM
☒ Disable ☐ Enable

Auto/Manual SIM
☐ Auto ☒ Manual

APN Settings

APN	broadband	
Username		
Password		

Data Roaming
☐ Disable ☒ Enable

Block List
 368, 746, 702, 734, 400, 415, 417, 418, 421, 432, 438, 472, 514, 528, 540, 544

Allow List
 -

LTE/3G Selection
☒ Auto ☐ LTE Only

Carrier Selection ⓘ
☒ Auto ☐ Manual

Save

Figure 4.113 Details of Active or Inactive SIMs

Alert

Configuration of SIM in Slot 2 will take approximately 1-3 minutes to be processed.

Ok

Figure 4.114 SIM Configuration Alert

Slot 1 SIM Details

SIM Details

State	InActive
Service Provider	T-Mobile
IMSI	310260885942316
ICCID (2)	8901260882259423165

Connect Now ⓘ
☒ No ☐ Yes

Disable/Enable SIM
☐ Disable ☒ Enable

APN Settings

APN	iot.tmowholesale	
Username		
Password		

Data Roaming - Disabled

Block List
 -

Allow List
 -

LTE/3G/5G Selection
☒ Auto ☐ 5G Only

Carrier Selection ⓘ
☒ Auto ☐ Manual

Save

Figure 4.115 Details of Inservice SIM

Slot 1 SIM Details

SIM Details	
State	Active
Service Provider	T-Mobile
IMSI	310030003124796
ICCID (1)	89010303300031247969

Figure 4.116 State of InService SIM after the Call is Disconnected

Slot 2 SIM Details

SIM Details	
State	Active
Service Provider	T-Mobile
IMSI	310260244891866
ICCID (3)	8901260245748918668

Disable/Enable SIM
☒ Disable ☐ Enable

Auto/Manual SIM
☐ Auto ☒ Manual

APN Settings

APN	fast.t-mobile.com
Username	
Password	

Data Roaming
☒ Disable ☐ Enable

Block List

Allow List

LTE/3G/5G Selection
☒ Auto ☐ 5G Only

Carrier Selection ⓘ
☒ Auto ☐ Manual

Save

Figure 4.117 Details of Locked SIM for Manual Settings

Slot 2 SIM Details

SIM Details	
State	Active
Service Provider	T-Mobile
IMSI	310260244891866
ICCID (3)	8901260245748918668

Disable/Enable SIM
☒ Disable ☐ Enable

Auto/Manual SIM
☒ Auto ☐ Manual

Save

Figure 4.118 Details of Locked SIM for Auto Settings

Slot 1 SIM Details

Save

SIM Details

State	InActive
Service Provider	TMobile
IMSI	310260885942316
ICCID (2)	8901260882259423165

Connect Now ⓘ

☒ No ☐ Yes

Disable/Enable SIM

☐ Disable ☒ Enable

APN Settings

APN	iot.tmowholesale
Username	
Password	

Data Roaming - Disabled

Block List

Allow List

LTE/3G/5G Selection

☒ Auto ☐ 5G Only

Carrier Selection ⓘ

☒ Auto ☐ Manual

Save

Figure 4.119 APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection Sections

Carrier Selection ⓘ

☐ Auto ☒ Manual

Select Carrier

Scan Output

Carrier Name/Alias	MCC/MNC
t-mobile	310/260
verizon	311/480
311 490	311/490
313 100	313/100
at&t	310/410

Saved Profiles

No Saved Profiles

Select from the above tables or enter below

Set Carrier Name/Alias	
Set MCC/MNC	

Save

Figure 4.120 Carrier Selection Configuration

To restrict network on particular carrier select Custom PLMN option. For MCC/MNC reference please click [here](#).

Carrier Selection ?
☐ Auto ☒ Manu

Select Carrier

Scan Output

Carrier Name/Alias	MCC/MNC
t-mobile	310/260
verizon	311/480
311 490	311/490
313 100	313/100
at&t	310/410

Saved Profiles

No Saved Profiles

Select from the above tables or enter below

Set Carrier Name/Alias

Set MCC/MNC

Save

Figure 4.121 MCC/MNC Reference Link

SIM Reload ×

Note:

- LTE Service will be restarted upon SIM Reload.
- Current LTE Call would be disconnected.
- Please wait for this screen to refresh in few minutes.

Reload

Figure 4.122 SIM Reload

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 based on the periodicity, in the **Last 1 hour** list, click the periodicity.

The following details become available under the **Performance** section.

- Data Usage / Rate
- Usage (MB)
- Rate (Mbps)

- Signal Strength (see figure below)
- RSSI (dBm)
- RSRQ (dB)
- SINR (dB)
- Technology (5G/LTE/Other)
- Change in Cellular KPI (indicated by vertical line)

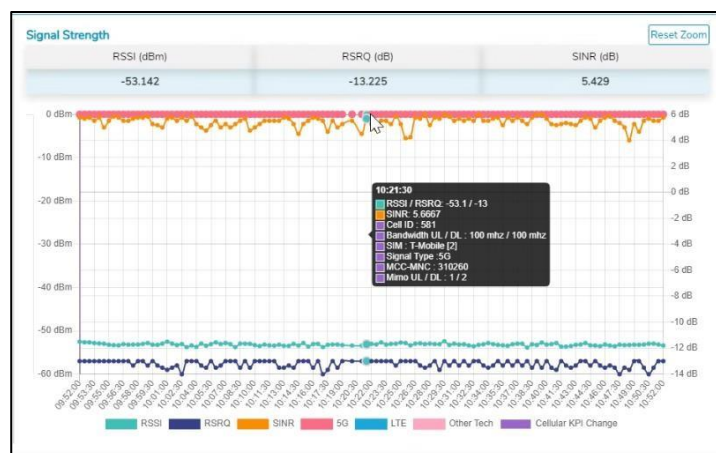


Figure 4.123 Signal Strength Hover Action

The **Vessel Path** displays the path traveled by the Site.

4.11 Shell Interface


This section provides a limited command line access to the system, with a restricted command set that is available through a web shell.

Note: This interface is available to users with administrative access only.

4.11.1 Accessing the Shell Interface

To access the Shell Interface, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click **Shell Interface**. The **Shell Interface** page appears, see figure below.

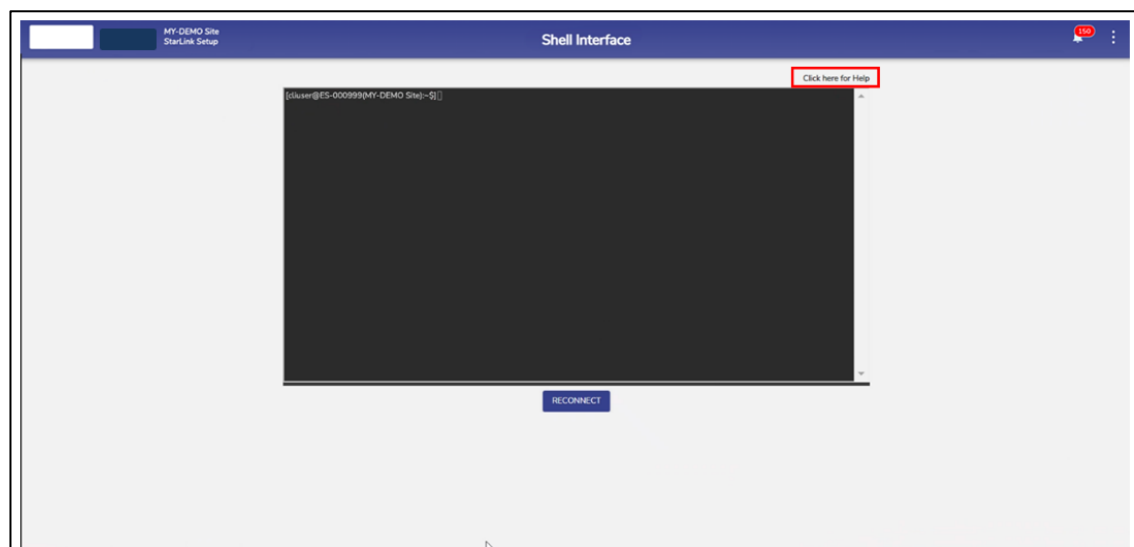


Figure 4.124 Shell Interface

- Click '**Click here for Help**' on top right of the screen to view the Help Page for the commands available on this interface, see **Figure 4.125 Commands –**

Shell Interface.

```
k4.debug.tunmgr help
k4.debug.tunmgr dump
k4.debug.tunmgr <parameter> <value>
This command can be used to tune the FVE parameters.
'parameters' = rtt_timeout, rtt_window, rate_window, rate_threshold, sample_interval,
               average_time, min_bonded_links or min_bonded_rtt_vfp
Run the 'help' sub-command to see details of the parameters
The 'dump' sub-command will show the current values of these parameters

k4.monitor.iftop [-i interface] [-t target] [-- iftop-options]
This command can be used to run the linux 'iftop' command.
'iftop' listens to network traffic on a named interface, or on the first interface it
can find which looks like an external interface if none is specified, and displays a
table of current bandwidth usage by pairs of hosts.
When used with the '-i' option, it will show the named native WAN interface.
When used with the '-t' option, it will show traffic for the named native target host.
The 'iftop-options' are the same as in the usual linux 'iftop' command.
Run 'man iftop' for details of the linux 'iftop' command

k4.monitor.ping [-i interface] [-- ping-options] target
k4.monitor.ping [-v interface] [-- ping-options] target
k4.monitor.ping [-i viaid] [-- ping-options] target
k4.monitor.ping [-- ping-options] target
This command can be used to 'ping' a target IP or FQDN.
'ping' uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP
ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams ('pings') have an
IP and ICMP header, followed by a struct timeval and then an arbitrary number of
'pad' bytes used to fill out the packet.
When used with the '-i' option, it will ping through the named native WAN interface.
When used with the '-v' option, it will ping through the VFP tunnel over the named WAN interface.
When used with the '-t' option, the ping will be as if coming from the named VLAN.
The 'ping-options' are the same as in the usual linux 'ping' command.
Run 'man ping' for details of the linux 'ping' command

k4.monitor.speedtest [-s server] [-i interface] [-- speedtest-options]
k4.monitor.speedtest [-s server] [-v interface] [-- speedtest-options]
k4.monitor.speedtest [-s server] [-i viaid] [-- speedtest-options]
This command will run a speed test using the linux 'speedtest' utility.
'speedtest' is an application that measures the latency, jitter, packet loss, download bandwidth,
and upload bandwidth of the network connection between the client and a nearby Speedtest Server.
When used with the '-i' option, the speed test will be run through the named native WAN interface.
When used with the '-v' option, the speed test will be run through the VFP tunnel over the named WAN interface.
When used with the '-t' option, the speed test will be as if coming from the named VLAN.
The '-s' option selects a specific server.
The 'speedtest-options' are the same as in the usual linux 'speedtest' command.
Run 'man speedtest' for details of the linux 'speedtest' command

k4.monitor.traceroute parameters
This command will run the linux 'traceroute' utility.
```

Figure 4.125 Commands – Shell Interface

5 Debugging


The user 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.

Steps


- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click on Configuration Wizard, see [Figure 4.31 Configuration Wizard Option](#).
- The Configuration Wizard appears.
- Click Access Networks. The Access Networks page appears, see [Figure 3.40 Access Networks](#).
- Perform steps to view network usage. For details, see [Viewing Network Usage Data](#).

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

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

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

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click on Usage Status. The Usage Status appears, see [Figure 4.67 Usage Status](#).
- Perform steps to view details of the network and device. For details, see [Top Networks](#) and [Top Devices](#).


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 view the historical details of the network, perform the following steps.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click on Usage Status. The Usage Status appears, see [Figure 4.67 Usage Status](#).
- 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](#).

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](#).

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.

Steps

- Log on to the EdgeOS System. The home page appears.
- Click the menu  icon. The menu appears.
- Click on Configuration Wizard, see [Figure 4.31 Configuration Wizard Option](#).
- The Configuration Wizard appears.
- Click General Settings. The General Settings page appears, see [Figure 3.99 General Settings Configuration Wizard](#).
- Access the **Device Traffic Policies** section.
- Verify the device traffic policy.
- Click Traffic Policies. The Traffic Profiles page appears, see [Figure 3.84 Traffic Policies](#).
- Click **Device**.
- Click  corresponding to the traffic policy.
- Access the Application Policy Profile section.

Verify the rules configured and allow the application.

6 Appendix

6.1 Viewing EdgeOS System through Konnect VPN

Post successful registration, the EdgeOS System becomes accessible via the Konnect VPN.

To view the EdgeOS System on Konnect VPN, perform the following steps.

Steps

- Login to the Konnect VPN with valid account.
- Enter the Site Name of the System in the Search By Location input field, see [Figure 6.2 Konnect VPN Landing Page](#). The Site Name becomes available in the drop down, see [Figure 6.3 Konnect VPN - Select a Site](#).
- Click Add next to the Site Name. The Site becomes available in the main table.
- Click on the expand arrow icon to expand the site. The systems available in this Site are listed. The user can access the System shell and portal, see [Figure 6.4 Konnect VPN - View System Details](#).
- Click on corresponding Start button. Stop and Open button appear, see [Figure 6.5 Konnect VPN - Open Connection](#).
- Click on Open button to access the Shell and the Portal of the EdgeOS System.
- Click on **Stop** to release the connection.

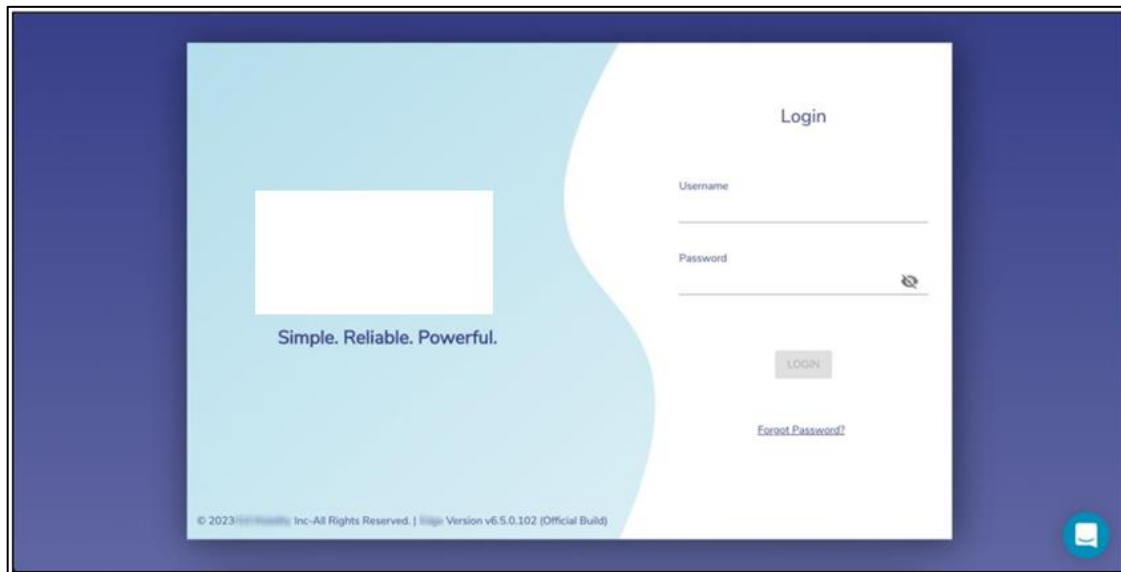


Figure 6.1 Konnect VPN Login Page

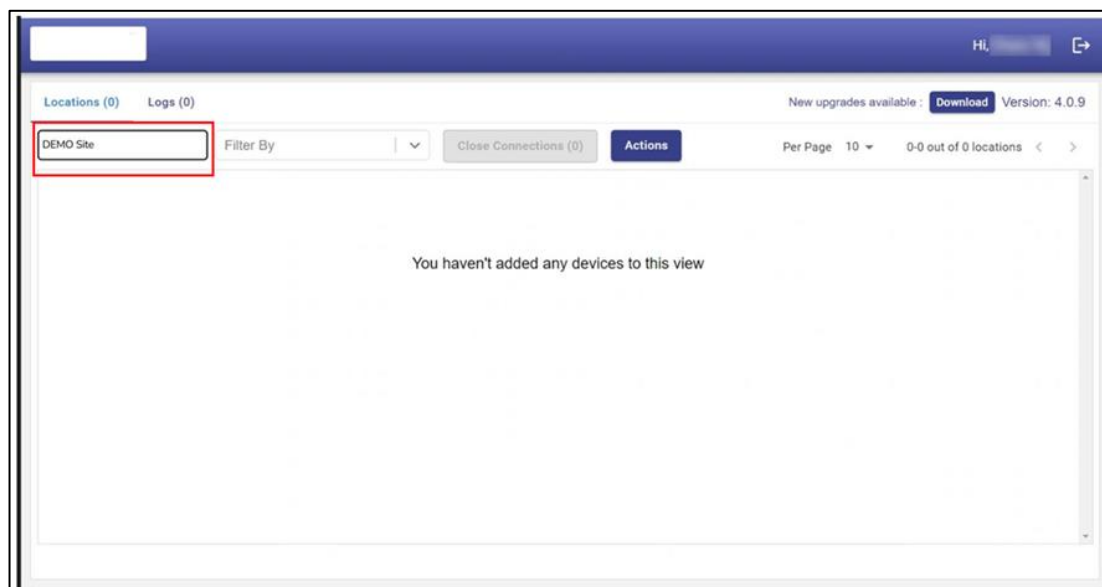


Figure 6.2 Konnect VPN Landing Page

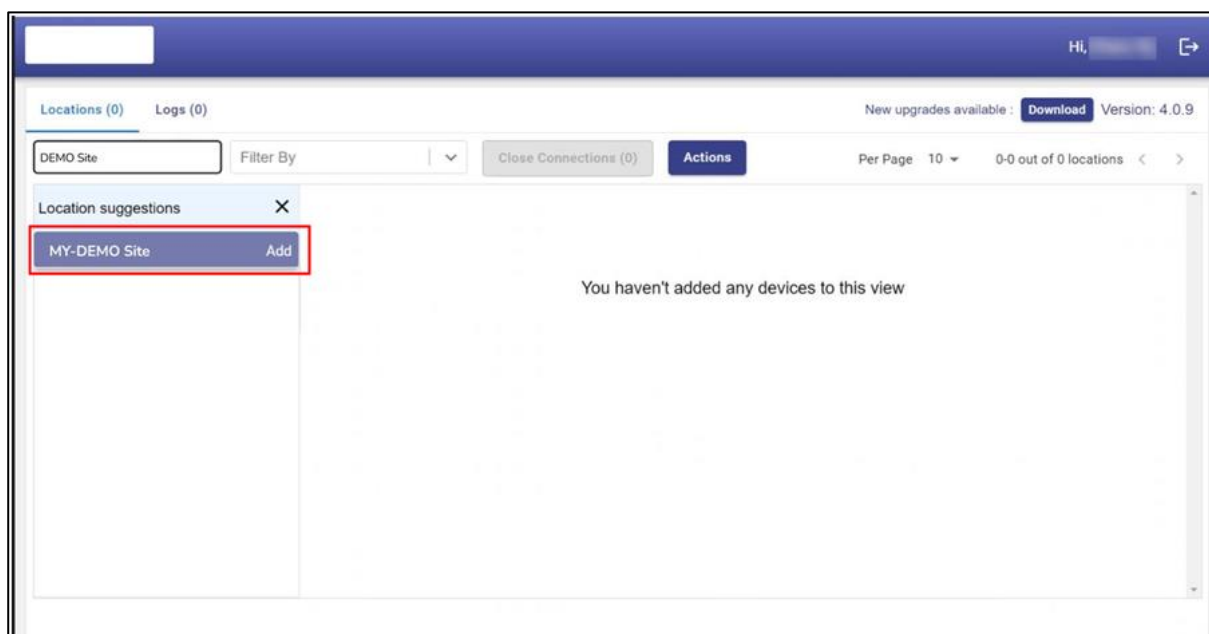


Figure 6.3 Konnect VPN - Select a Site

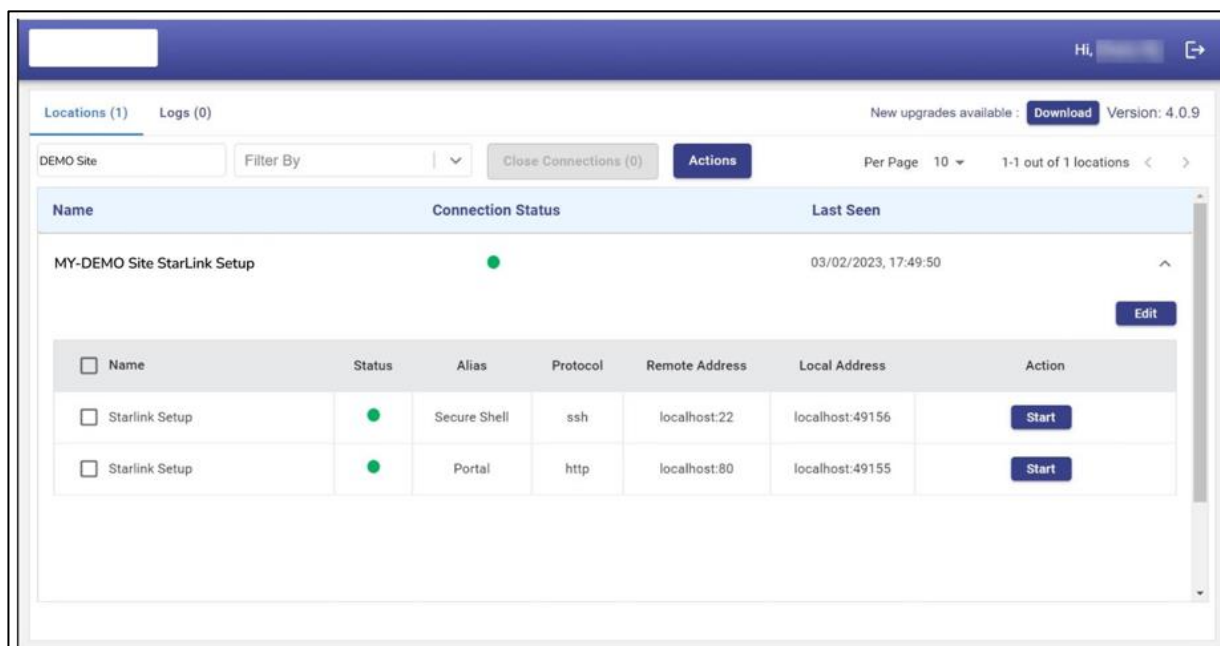


Figure 6.4 Konnect VPN - View System Details

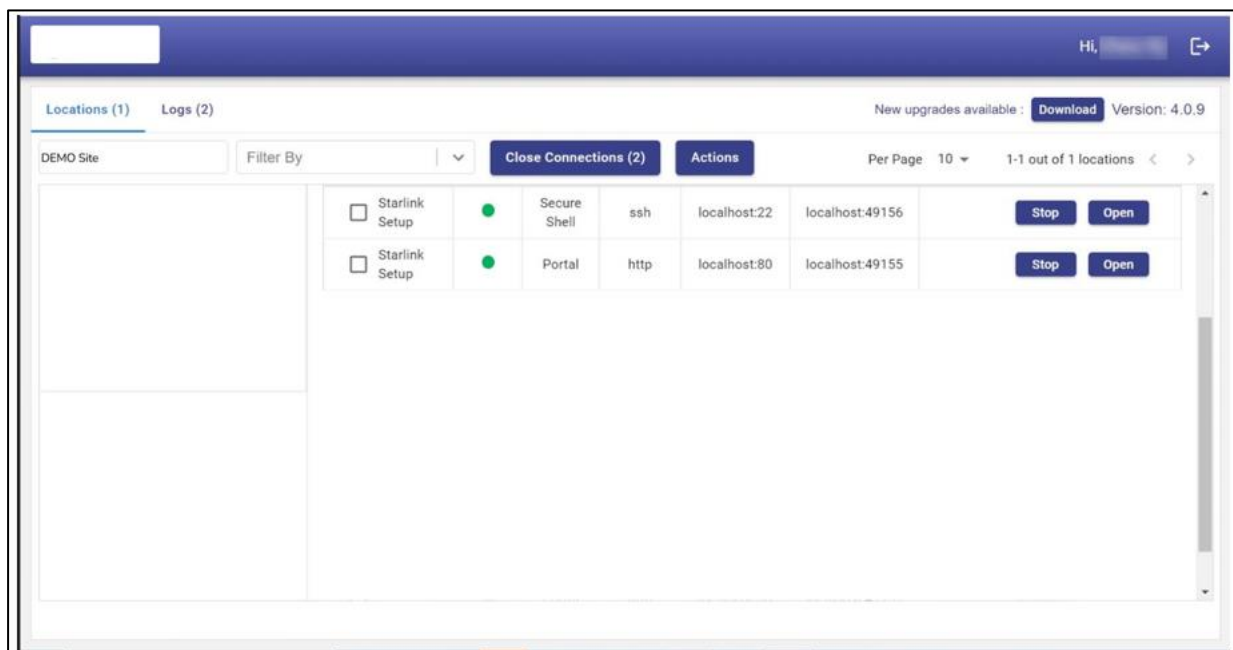


Figure 6.5 Konnect VPN - Open Connection

Table of Figures

Figure 1.1 Configuration of Equipment.....	8
Figure 1.2 Rear View of EdgeOS System.....	9
Figure 1.3 Front View of EdgeOS System.....	9
Figure 2.1 Invitation to Register Account.....	13
Figure 2.2 Registration Page.....	13
Figure 2.3 Application Login Page	14
Figure 2.4 Warehouse Tab	17
Figure 2.5 Assign Inventory Dialog Box	18
Figure 2.6 Deployed Tab	19
Figure 2.7 Registration Workflow.....	20
Figure 2.8 Registration Flow via Edge Mobile App	22
Figure 2.9 Login Page	23
Figure 2.10 Logout Menu Option.....	24
Figure 2.11 SPORT Login Page	25
Figure 2.12 SPORT Portal	26
Figure 3.1 Configuration Wizard.....	27
Figure 3.2 Classification of Home Page.....	27
Figure 3.3 Interface Screen	29
Figure 3.4 Interface Dialogue Box.....	33
Figure 3.5 WAN Configuration	33
Figure 3.6 LAN Type	33
Figure 3.7 LAN Type Sub I/F ID.....	34
Figure 3.8 VSAT Management	34
Figure 3.9 Update WAN Interface	35
Figure 3.10 Select WAN Type	36
Figure 3.11 WAN Interface VSAT-LEO	37
Figure 3.12 Interface VSAT-FBB.....	38
Figure 3.13 Interface Type Selection.....	38
Figure 3.14 WAN Type Selection	39

Figure 3.15 Interface EXT5G.....	39
Figure 3.16 LAN Type.....	40
Figure 3.17 LAN Type Sub I/F ID	41
Figure 3.18 Select VSAT Mgmt Interface	42
Figure 3.19 Add New Interface	43
Figure 3.20 Interface Name	43
Figure 3.21 Interface Type	44
Figure 3.22 Type Alias Name	44
Figure 3.23 Select WAN Type	44
Figure 3.24 Sub Interface ID	45
Figure 3.25 Configuration Wizard – Sub Interface Created.....	45
Figure 3.26 Configuration Wizard – View Enabled Interfaces	46
Figure 3.27 Ethernet/ Hardline.....	46
Figure 3.28 CELL Configuration	47
Figure 3.29 VSAT Configuration	47
Figure 3.30 Eth State Hover.....	51
Figure 3.31 Peplink Access Details.....	55
Figure 3.32 VSAT Type default pop-up.....	55
Figure 3.33 VSAT Type Selection	56
Figure 3.34 VSAT-LEO.....	56
Figure 3.35 Add to Konnect	56
Figure 3.36 Probe Profiles Information	60
Figure 3.37 Configure Probe	60
Figure 3.38 Speed Test	62
Figure 3.39 Speed Test List	63
Figure 3.40 Access Networks.....	64
Figure 3.41 Expanded View	65
Figure 3.42 Add Connected Network.....	66
Figure 3.43 Add Managed Connected Network.....	66
Figure 3.44 Configure Managed Connected Network	73
Figure 3.45 Network Updated Successfully	73
Figure 3.46 Configure DNS Policy (Not in Use).....	74

Figure 3.47 Bulk Upload	74
Figure 3.48 IP Reservations Template in CSV Format	74
Figure 3.49 Example of IP Reservations Template in CSV Format.....	74
Figure 3.50 IP Reservations Details	75
Figure 3.51 Add Managed Routed Network.....	76
Figure 3.52 Grouped Networks	78
Figure 3.53 Update Connected Network	79
Figure 3.54 Device Profile.....	80
Figure 3.55 Network Usage	81
Figure 3.56 Quota Details.....	84
Figure 3.57 Pause Device Confirmation Message.....	84
Figure 3.58 Resume Device Confirmation Message.....	85
Figure 3.59 Captive Access Network Configuration	87
Figure 3.60 Aggregate Network Policy	87
Figure 3.61 Captive Access Network.....	87
Figure 3.62 Device Traffic Policy	88
Figure 3.63 Konnect VPN Configuration	89
Figure 3.64 LAN Monitoring	90
Figure 3.65 Network Design Scan Progress.....	90
Figure 3.66 LAN Monitoring	91
Figure 3.67 Monitored Devices.....	91
Figure 3.68 Periodicity of Monitoring	92
Figure 3.69 Add to Konnect	93
Figure 3.70 Port Added to the Konnect.....	93
Figure 3.71 Add/Remove from Konnect.....	94
Figure 3.72 Remove from Konnect Pop-up	94
Figure 3.73 Stop Monitoring	95
Figure 3.74 Pause Network Pop-up	96
Figure 3.75 Resume Traffic Pop-up	97
Figure 3.76 Delete Network Pop-up	98
Figure 3.77 Advance Bonding	101
Figure 3.78 WAN Profile	102

Figure 3.79 Bonding Mechanism	104
Figure 3.80 Static Bonding Mechanism	105
Figure 3.81 Error Message.....	105
Figure 3.82 WAN Profile Creation	106
Figure 3.83 Delete Profile	108
Figure 3.84 Traffic Policies.....	109
Figure 3.85 Category list	119
Figure 3.86 Applications List	119
Figure 3.87 Domain Rules	120
Figure 3.88 Application Allow or Deny	120
Figure 3.89 Domain Rule CSV Format	120
Figure 3.90 Example of Domain Rule.....	121
Figure 3.91 Domain Rule Section	121
Figure 3.92 IP & Port Section.....	122
Figure 3.93 IP & Port Rule.....	122
Figure 3.94 IP & Port Rule Example CSV Rule.....	122
Figure 3.95 Valid IP & Ports.....	123
Figure 3.96 Application Allow or Deny	123
Figure 3.97 Create Device Policy	124
Figure 3.98 Delete Network Policy	133
Figure 3.99 General Settings Configuration Wizard	134
Figure 3.100 Device Traffic Policies.....	135
Figure 3.101 Device Traffic Policy Creation	138
Figure 3.102 Static Route Configuration	139
Figure 3.103 Add Static Route	140
Figure 3.104 Firewall Settings.....	141
Figure 3.105 Add New Rule Firewall Settings	142
Figure 3.106 Add New Firewall Domain Rule.....	142
Figure 3.107 Firewall New Rules	144
Figure 3.108 Firewall Rules Info.....	145
Figure 3.109 Firewall Refresh	145
Figure 3.110 Firewall Upload Config from Backup	145

Figure 3.111 Firewall Rules List.....	146
Figure 3.112 Edit Firewall Rules	146
Figure 3.113 Enable/Disable Toggle Firewall Rules	147
Figure 3.114 Disable Firewall Rule Pop-up	147
Figure 3.115 Enable Firewall Pop-up	148
Figure 3.116 Delete Firewall Rule Icon	148
Figure 3.117 Delete Firewall Rule Pop-up	149
Figure 3.118 Defining New Priority of the Firewall Rules Icon	149
Figure 3.119 Resetting the Number of Packets Icon	150
Figure 3.120 Reset Counter Pop-up.....	150
Figure 3.121 DNS Proxy Settings.....	151
Figure 3.122 Network Updated Successfully.....	154
Figure 3.123 DNS Server In Use	154
Figure 3.124 DNS Server Not in Use.....	155
Figure 3.125 Multicast Settings	156
Figure 3.126 Select Access Network.....	157
Figure 3.127 Konnect VPN Settings.....	160
Figure 3.128 Konnect VPN Server Settings	161
Figure 3.129 Konnect VPN Server Settings Pop-up	161
Figure 3.130 Konnect VPN Server Section	162
Figure 3.131 Add New Client Pop-up	162
Figure 3.132 Configured Clients Table	163
Figure 3.133 Konnect VPN Client Section.....	164
Figure 3.134 Add New Connection	164
Figure 3.135 Configured Connections Table.....	164
Figure 3.136 Edit Client Connection.....	164
Figure 3.137 Quality of Service	165
Figure 3.138 Quality of Service Disable	166
Figure 3.139 Config Backup/ Config Upload	167
Figure 3.140 Initiate New Configuration Backup.....	168
Figure 3.141 Select Configuration Backup Type	168
Figure 3.142 Available Config Backups	169

Figure 3.143 Initiate New Configuration Upload	170
Figure 3.144 Upload Configuration	170
Figure 3.145 Apply Configuration	170
Figure 3.146 Apply Configuration Intermediate Step	171
Figure 3.147 Apply Configuration Reboot Server	171
Figure 3.148 Reboot Confirmation.....	171
Figure 4.1 Notification Pop-up.....	173
Figure 4.2 Notification Count	173
Figure 4.3 Filter by Category Drop-Down.....	173
Figure 4.4 Clear All Notifications	177
Figure 4.5 System Information.....	178
Figure 4.6 Update Site Name	181
Figure 4.7 Update Device Name.....	181
Figure 4.8 Updated Firmware Version	181
Figure 4.9 System Reboot	182
Figure 4.10 New Update Available.....	183
Figure 4.11 Downloading latest version	183
Figure 4.12 Download Successful.....	184
Figure 4.13 Installation Initiation	184
Figure 4.14 Rebooting Server	185
Figure 4.15 Reconnecting Server	185
Figure 4.16 Downloaded and Installed Firmware.....	185
Figure 4.17 System Information.....	186
Figure 4.18 System Reboot	186
Figure 4.19 Manage Account	188
Figure 4.20 User Account Management	189
Figure 4.21 Add Resources	191
Figure 4.22 Select Organization	191
Figure 4.23 Email Confirmation	192
Figure 4.24 Registration Page	192
Figure 4.25 User Added Successfully	193
Figure 4.26 Disable Account	194

Figure 4.27 Account Disabled Successfully.....	195
Figure 4.28 Delete Account.....	198
Figure 4.29 Change Password.....	200
Figure 4.30 EdgeOS Account Password Management	201
Figure 4.31 Configuration Wizard Option	203
Figure 4.32 Internet Status Page	205
Figure 4.33 Select Time Zone	207
Figure 4.34 Select Periodicity.....	207
Figure 4.35 Internet Status WAN Profiles	208
Figure 4.36 Realtime Chart.....	210
Figure 4.37 Speed Test Pop-up.....	211
Figure 4.38 Select Internet Source.....	212
Figure 4.39 Speed Test Result	212
Figure 4.40 Disable Pop-up.....	213
Figure 4.41 Enable Pop-up	214
Figure 4.42 Performance Chart Starlink	215
Figure 4.43 Network Usage Level Pie-Chart	216
Figure 4.44 Network Usage Drop-Down Selection	217
Figure 4.45 Starlink Network Usage	217
Figure 4.46 View Top Applications	218
Figure 4.47 Top Applications.....	218
Figure 4.48 Change Periodicity - Top Applications	219
Figure 4.49 Internet Status with Konnect VPN	221
Figure 4.50 Konnect VPN Dashboard.....	221
Figure 4.51 Internet Profiles	224
Figure 4.52 Internet Profiles Hover Action	224
Figure 4.53 Bonded Link Speed Test	226
Figure 4.54 Bonded Link Speed Test Drop Down	226
Figure 4.55 Internet Profile Status Pop-up.....	227
Figure 4.56 Arrow Button Internet Profiles.....	228
Figure 4.57 Internet Profile Status Info Icon.....	228
Figure 4.58 Geolocation - VSAT	229

Figure 4.59 Geolocation - Others	229
Figure 4.60 Performance Chart	230
Figure 4.61 Custom search	233
Figure 4.62 Peak Rate Estimate	233
Figure 4.63 Weighting Charts.....	235
Figure 4.64 Time Zone	238
Figure 4.65 Custom Search.....	238
Figure 4.66 WAN Profile - Bonded Set/WAN	238
Figure 4.67 Usage Status	239
Figure 4.68 Configured Usage Status	240
Figure 4.69 Edit Traffic Policy Profile	242
Figure 4.70 Pause Internet	243
Figure 4.71 Paused Network.....	243
Figure 4.72 Resume Network.....	244
Figure 4.73 Traffic Details	245
Figure 4.74 Paused Devices Link.....	247
Figure 4.75 Paused Devices.....	247
Figure 4.76 Resume Internet.....	248
Figure 4.77 Edit Traffic Policy Profile	248
Figure 4.78 Total Paused Devices	249
Figure 4.79 Traffic Details	250
Figure 4.80 VSAT Controller Page	252
Figure 4.81 Reboot Modem	256
Figure 4.82 Reboot VSAT Modem Confirmation Message	256
Figure 4.83 Beam Switch.....	256
Figure 4.84 VSAT Beam Switch Pop-up	256
Figure 4.85 Site Location	257
Figure 4.86 Voyage Duration Pop-up.....	257
Figure 4.87 Site Voyage Path.....	257
Figure 4.88 Satellite Selection Pop-up	258
Figure 4.89 Starlink Information	259
Figure 4.90 Connection Status	261

Figure 4.91 VSAT Starlink Reboot	261
Figure 4.92 Alert Details	261
Figure 4.93 Enlarged view of Antenna Details	262
Figure 4.94 Periodicity Selection	263
Figure 4.95 Cellular Controller	264
Figure 4.96 Cellular Indicator	267
Figure 4.97 Signal Strength	267
Figure 4.98 Vessel Path Pop-up.....	268
Figure 4.99 Cellular Controller.....	271
Figure 4.100 SIM Priority Settings	276
Figure 4.101 SIM Priority Settings - Manual	277
Figure 4.102 SIM Priority Advanced Settings	277
Figure 4.103 Cellular Actions.....	278
Figure 4.104 Cellular Actions Options	278
Figure 4.105 Ext5G Connectivity Alert.....	278
Figure 4.106 Cell Lock in Progress.....	278
Figure 4.107 Cell Lock Successful.....	279
Figure 4.108 Cell Unlock in Progress.....	279
Figure 4.109 Cell Unlock Successful.....	279
Figure 4.110 Cell Reset In Progress.....	279
Figure 4.111 Cell Reset Successful	280
Figure 4.112 Performance Charts	289
Figure 4.113 Details of Active or Inactive SIMs.....	288
Figure 4.114 SIM Configuration Alert.....	290
Figure 4.115 Details of Inservice SIM	290
Figure 4.116 State of InService SIM after the Call is Disconnected.....	291
Figure 4.117 Details of Locked SIM for Manual Settings.....	291
Figure 4.118 Details of Locked SIM for Auto Settings.....	291
Figure 4.119 APN Settings, Data Roaming, LTE/3G Selection, and Carrier Selection Sections	292
Figure 4.120 Carrier Selection Configuration	292
Figure 4.121 MCC/MNC Reference Link.....	293

Figure 4.122 SIM Reload	293
Figure 4.123 Signal Strength Hover Action	294
Figure 4.124 Shell Interface	295
Figure 4.125 Commands – Shell Interface	296

Table of Tables

Table 1-1 Technical Specifications.....	10
Table 3-1 Sections of Home Page.....	28
Table 3-2 Enable Interface	31
Table 3-3 Interface Name.....	33
Table 3-4 Interface Name Hyperlinks.....	47
Table 3-5 LAN/WAN Type.....	49
Table 3-6 Alias.....	50
Table 3-7 Internet State	50
Table 3-8 Eth State/Reset.....	51
Table 3-9 IP Address/ Subnet Mask.....	52
Table 3-10 Gateway Address.....	54
Table 3-11 Probe/Latency (msec).....	59
Table 3-12 DNS Server	60
Table 3-13 Public IP Address/Service Provider.....	61
Table 3-14 Speed Test	62
Table 3-15 US Internet.....	63
Table 3-16 Connected Network Information.....	73
Table 3-17 Managed Routed Network Information.....	77
Table 3-18 Network Usage.....	84
Table 3-19 WAN Profile	104
Table 3-20 Traffic Policy	119
Table 3-21 Device Traffic Policies	130
Table 3-22 Static Route	133
Table 3-23 Add New Rule	137
Table 3-24 DNS Proxy Settings	146
Table 4-1 System Information.....	174
Table 4-2 Add Account	183
Table 4-3 Add Account Registration Details.....	186
Table 4-4 Disable Account.....	188

Table 4-5 Delete Account Fields	190
Table 4-6 Change Password Fields	193
Table 4-7 Change Password Fields	194
Table 4-8 Internet Status Fields.....	200
Table 4-9 LAN Status Fields.....	213
Table 4-10 Konnect VPN Details.....	215
Table 4-11 VPN Server	216
Table 4-12 VPN Client	216
Table 4-13 Internet Profile Fields	218
Table 4-14 Performance Chart Information.....	226
Table 4-15 Weighting Charts Fields	230
Table 4-16 VSAT Controller Information	248
Table 4-17 Starlink Controller Information	253
Table 4-18 Cellular Indicator Details.....	260
Table 4-19 Signal Strength	262
Table 4-20 Cellular Indicators	269
Table 4-21 SIM Details	282

Revision History

Date	Version	Remark
Jan-15-2023	0.1	Draft User Guide for EdgeOS System
Feb-01-2023	0.2	Draft User Guide for EdgeOS System – Configuration Wizard
Feb-14-2023	0.3	First Draft User Guide for EdgeOS System
16-Jun-2023	1.0	Final User Guide post incorporating review comments

----- END OF DOCUMENT -----