

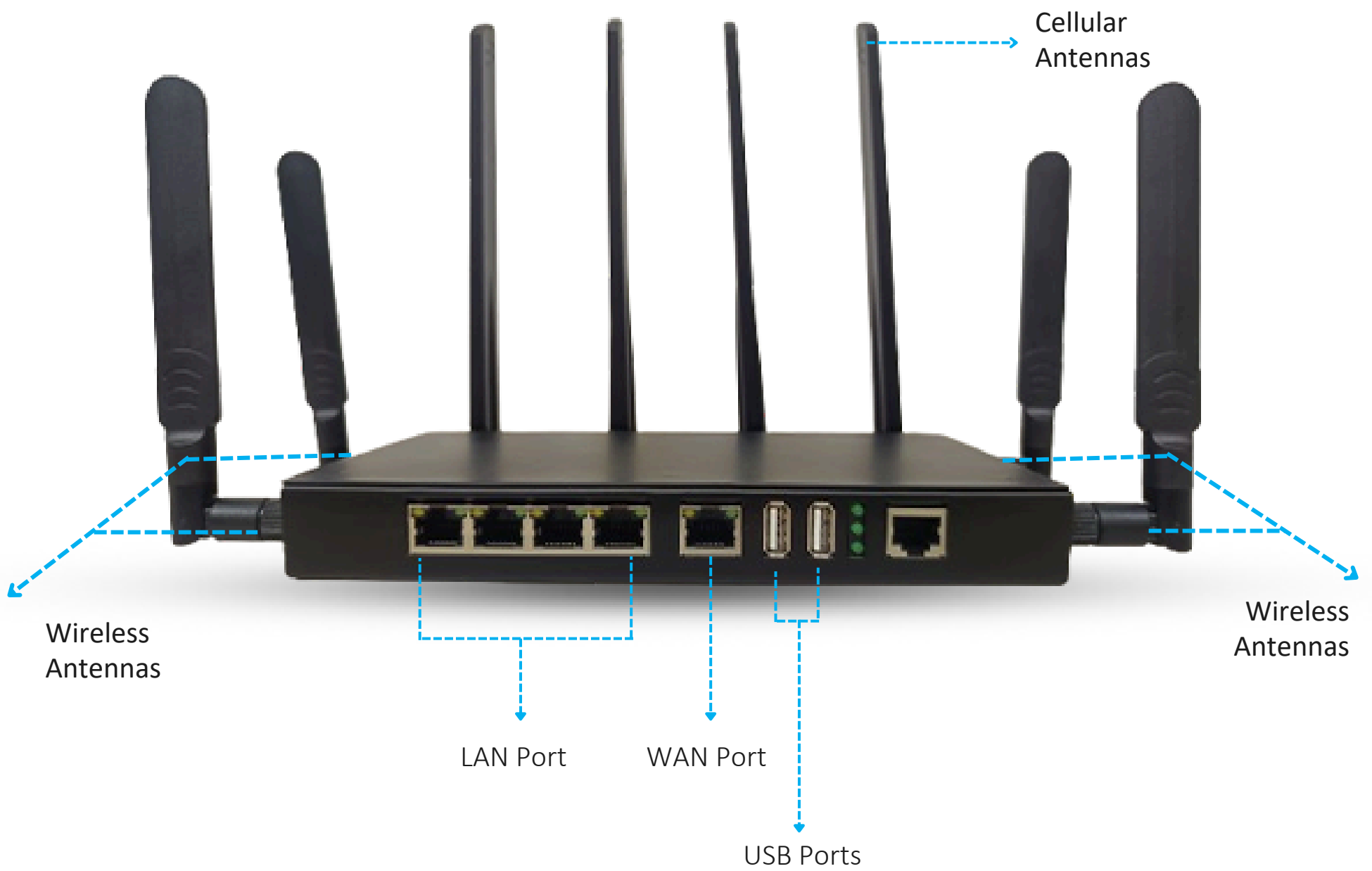


# KRO-110-D4G User Manual

# CONTENTS

Appearance.....	1
Router Setup.....	2
Configuration.....	3
LOGS.....	4
Stats.....	5
Update.....	6
Administration.....	7

## Appearance



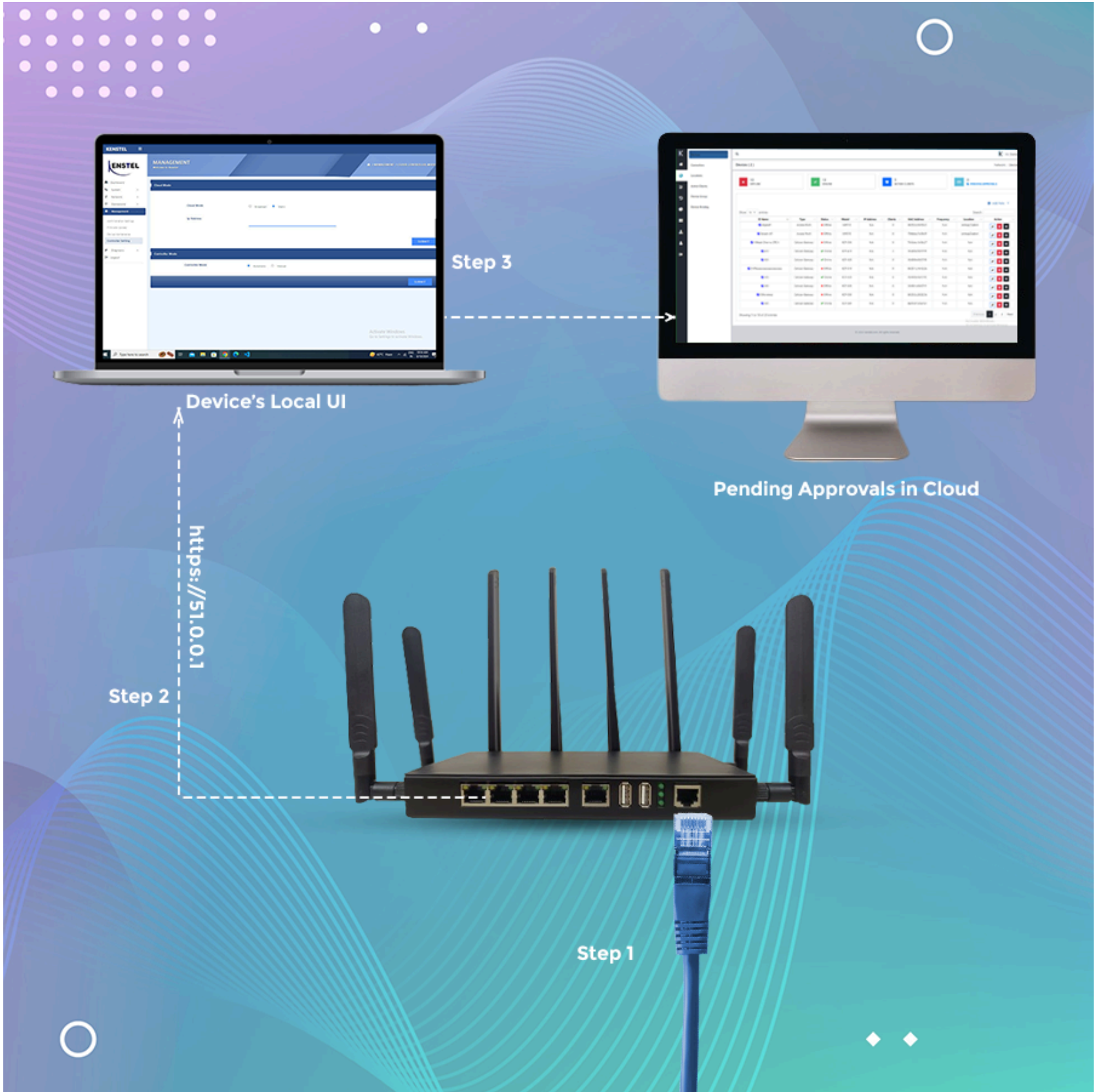


**LAN/WAN Port:** It can be switch into LAN or WAN.

**DC Adapter :** DC Adapter is the port where you plug in the power adapter to supply electrical power to the device.

**Reset Button:** Push for 10 Seconds and release for reset. You can do the same at least 2 minutes after KCP510 Power-up.

**SIM Slot:** This is the port where you should insert the SIM.



Device can run on two modes one is Local and another is Cloud.

If you want to run the Device with local mode you just simply Connect your Device via LAN Port → Then open with the IP, https://51.0.0.1 → Signup and Signin

And if you want to run the Device with Cloud mode you just simply Connect your Device via LAN Port → Then open with the IP, https://51.0.0.1 → Signup and Signin

And then go to Management → Controller Setting

**Status:** Enable the Status.

**Cloud Mode:** There are two cloud modes one is Broadcast and another one is Static. If you enable Static mode then input the ip address.

**Controller Mode:** There are two controller modes one is Automatic and another one is Manual. In Automatic mode device will get the IP automatically from cloud while in manual you have to input the IP manually.

The screenshot shows the 'Controller Settings' page with three main sections: Status, Cloud, and Controller. The Status section has 'Enable' selected. The Cloud section has 'Static' selected and an empty 'Ip Address' input field. The Controller section has 'Automatic' selected. A 'SUBMIT' button is at the bottom right.

Section	Option	Selected
Status	Enable	Yes
	Disable	No
Cloud Mode	Broadcast	No
	Static	Yes
Ip Address	Input Field	Empty
Controller Mode	Automatic	Yes
	Manual	No

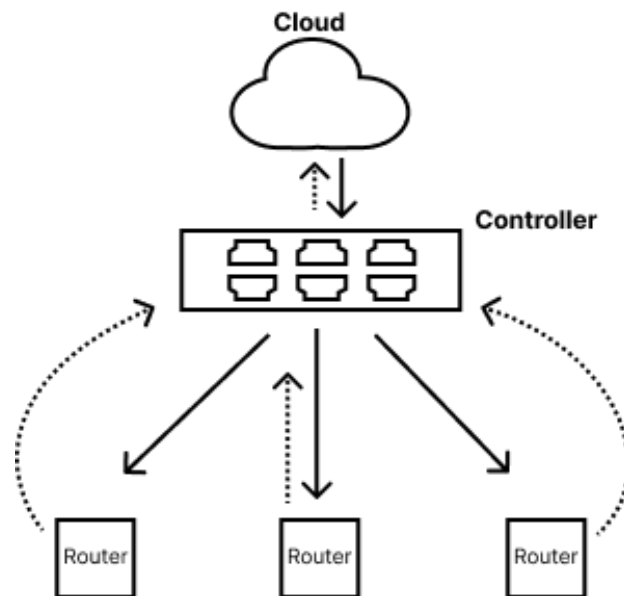
## Router Setup.....2

Controller.....	2.1
Device.....	2.2
Device Groups.....	2.3
Device Binding.....	2.4

**Note:** In this document you will find '**Rule Type**' where it is mentioned as **By group** or **By Name**. For that, refer to the below lines.

If you select By group then the features will apply to all the Router devices within the selected Router group. And if you select By name then the features will apply to the selected Router device only. Here, you can choose multiple groups or devices. By default, the most recently created rule will apply to a new device. And if you delete the newly created rule type then it will switch to the earlier added rule type whether it is By Group or By Name.

# Controller



Controller acts like a bridge to connect to all the Access Points with Cloud. Controller takes incoming messages from cloud and sends them to all the AP's and also collects all the information from AP's and sends them back to the cloud.

To reach this Page go to Network → Controllers

Here you can add Controllers to the Cloud by clicking on the Add New Button.

**Controllers ( 5 )** Dashboard / Wireless / Controllers

Show  entries Add New

Search:

Controller	Type	Model	Serial Number	IP	Active AP	Action
ashu	Local	KC100	4c4c4544-0052-5310-8030-b6c04f395833	192.168.1.3	5	<a href="#">Edit</a> <a href="#">Delete</a>
Controller03	Local	KC100	4c4c4544-0052-4b10-8044-b5c04f305833	192.168.5.63	0	<a href="#">Edit</a> <a href="#">Delete</a>
dinesh	Local	KC100	4c4c4544-004b-5010-8053-b4c04f4c3733	192.168.1.7	5	<a href="#">Edit</a> <a href="#">Delete</a>
ShivanshuController	Local	KC100	4c4c4544-0043-5610-8030-b5c04f4c4b33	172.16.229.1	0	<a href="#">Edit</a> <a href="#">Delete</a>
ShivanshuController02	Local	KC100	7AA0BE80-A813-11E8-B86D-1E5608733900	192.168.5.95	2	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1 to 5 of 5 entries Previous **1** Next

(You able to see this page when it is in Basic mode.)

Controller can operate on Local Routing, Centralized forwarding and Bridging.

Local routing: In the case of Local routing, Captive Portal, Network rate limit and user by the rate limit are all features operated on Access Point itself.

Centralized forwarding: But, in the case of Centralized forwarding, all the above features are implemented on controller.

[Click here to open the Edit Controller Page](#)

## Controller

Edit Controller page when controller type is in Local.

### Update Your Controller Setting ×

#### General Settings

Controller Name	<input type="text" value="anjali"/>
Controller Type	<input type="radio"/> Cloud <input checked="" type="radio"/> Local
Operating Mode	<input type="text" value="Local Routing"/>
Controller Model	<input type="text" value="KC100"/>
Controller Serial Number	<input type="text" value="4c4c4544-004b-5010-8053-b4c04f4c3733"/>
Controller LAN IP	<input type="text" value="22.0.0.46"/>
Backup Controller	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Backup Controller Serial Number	<input type="text" value="Enter Serial Number"/>

Here you can edit your controller Settings.

## Controller

Edit Controller page controller type is in Cloud.

### Update Your Controller Setting ✕

#### General Settings


Controller Name	<input type="text" value="ShivanshuController"/>
Controller Type	<input checked="" type="radio"/> Cloud <input type="radio"/> Local
Cloud Controller	<input checked="" type="radio"/> Physical <input type="radio"/> Virtual
Operating Mode	<input type="text" value="Local Routing"/>
Controller Model	<input type="text" value="KC100"/>
Controller Serial Number	<input type="text" value="Serial Number"/>
Controller Static IP	<input type="text" value="Static IP (Optional)"/>
Backup Controller	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Backup Controller Serial Number	<input type="text" value="Enter Serial Number"/>

Here you can edit your controller Settings.

# Controller


Controllers ( 1 ) Network / Controllers

Show  entries Search:

Controller	Type	Model	Serial Number	IP	Active AP	Action
ubuntu	Local	KC100	4c4c4544-0043-5610-8030-b4c04f4c4b33	192.168.5.74	9	

Showing 1 to 1 of 1 entries Previous **1** Next

(You able to see this page when it is in Mixed mode.)

Click here to open the edit controller page. 

# Controller

Edit Controller page.

### Update Your Controller Settings

#### General Settings

Controller Name: ubuntu

Controller Type: local

Controller Model: KC100

Controller Serial Number: 4c4c4544-0043-5610-8030-b4c04f4c4b33

Controller LAN IP: 192.168.5.74

Mac Address: 00:25:82:00:84:32

Operating Mode: Local Routing

Backup Controller:  Enable  Disable

#### Controller Settings

##### Wan IP Settings

Wan Ip Settings:  DHCP  Static

IP Address: 192.168.5.22

Netmask: 255.255.255.0

Gateway: 192.168.5.10

Primary DNS Server: 192.168.5.10

Secondary DNS Server: 192.168.5.10

##### Management Settings

IP Address: 50.0.0.1

Netmask: 255.255.255.0

##### Tools

Tool: Reboot

##### Controller Upgrade

Controller Update: Choose File Browse Install Update

Backup Controller  Enable  Disable

Backup Controller Serial Number: Enter Serial Number

#### Wan IP Settings

Wan Ip Settings:  DHCP  Static

IP Address: Ip Address

Netmask: Netmask

# Controller

There can be two types of controller: 1. Cloud  
2. Local

**Add Controller** Dashboard / Wireless / Controllers / Add Controller

---

**General Settings**

Controller Name	<input type="text" value="Enter controller Name"/>
Controller Type	<input checked="" type="radio"/> Cloud <input type="radio"/> Local
Cloud Controller	<input checked="" type="radio"/> Physical <input type="radio"/> Virtual
Operating Mode	<input type="text" value="--Please-Select--"/>
Controller Model	<input type="text" value="KC100"/>
Controller Serial Number	<input type="text" value="Serial Number"/>
Controller Static IP	<input type="text" value="Static IP (Optional)"/>

Cloud :-In the case of Cloud controller, there can be two cases, first case is the one in which controller is physical device, here this controller can have a static IP and this IP can be binded to multiple user and can be binded with multiple locations.

# Controller

**Add Controller** Dashboard / Wireless / Controllers / Add Controller

---

**General Settings**

Controller Name	<input type="text" value="Enter controller Name"/>
Controller Type	<input checked="" type="radio"/> Cloud <input type="radio"/> Local
Cloud Controller	<input type="radio"/> Physical <input checked="" type="radio"/> Virtual
Operating Mode	<input type="text" value="--Please-Select--"/>
Controller Model	<input type="text" value="KC100"/>
Controller Serial Number	<input type="text" value="Serial Number"/>

Virtual, here this controller can be binded to multiple users and it is a EC2 instance.

# Controller

**Add Controller** Dashboard / Wireless / Controllers / Add Controller

---

**General Settings**

Controller Name	<input type="text" value="Enter controller Name"/>
Controller Type	<input type="radio"/> Cloud <input checked="" type="radio"/> Local
Operating Mode	<input type="text" value="--Please-Select--"/>
Controller Model	<input type="text" value="--Please-Select--"/>
Controller Serial Number	<input type="text" value="Serial Number"/>
Controller LAN IP	<input type="text" value="LAN IP (Optional)"/>

Local :-In the case of local controller, one user can access that controller and also local controller can be binded to only one location.

# Devices

A router in a cloud controller directs network traffic within a cloud environment, facilitating communication between different resources. It forwards packets, uses routing protocols for optimal path selection, enables network segmentation and security policies, supports load balancing, VPN connectivity, and ensures high availability through redundancy and failover mechanisms.

There are two ways to Add Router

To reach this Page go to Network → Devices → Pending Approvals

Name	Type	Status	Model	IP Address	Clients	MAC Address	Frequency	Location	Action
Kenstel Router	Router	Online	KRO-110-D4G	192.168.5.70	0	bc7:43:98:be:fc	N.A	N.A	[Edit] [Delete] [Overview]

Click here to check the overview of the Router.

Name	TYPE	Model	MAC Address	IP Address	Country Code	Location	Action
Kenstel Router	router	KRO-110-D4G	bc7:43:98:be:fc	192.168.5.70	IN	Live	[Delete]

Router will be visible when it is added to the Cloud. To add the Router to the Access Point select the router and Location then Click on Approve.

# Devices

Here you can get the overview of the Router

Router Details Network / Devices / De:30:D7:E3:E1:A3

Summary Tools Vpn

123659 DEVICE NAME	de:30:d7:e3:e1:a3 MAC ADDRESS	ONLINE STATUS	N.A CLIENTS	N.A UPTIME	N.A DOWNTIME
-----------------------	----------------------------------	------------------	----------------	---------------	-----------------

Total Memory N.A	Free Memory N.A	Hardware Version N.A	Software Version N.A
---------------------	--------------------	-------------------------	-------------------------

Device Location Map View Satellite View

General Details

Name	123659
Model	KRO-110-D4G
MAC	de:30:d7:e3:e1:a3
IP Address	N.A
Controller	N.A
Controller Type	N.A
Controller Model	N.A
Controller Serial Number	N.A

Router Details Network / Devices / 7a:A3:E3:Eb:41:85

Summary Tools Vpn

Ping

Reboot Device

Traceroute

```
(K|E|N|S|T|E|L)
This interface is only to show ping and traceroute results.
© 2019 kenstel.com All Rights Reserved.
```

You can Ping or Reboot here.

# Device

Router Details Network / Devices / 7a:A3:E3:Eb:41:85

---

Summary Tools **Vpn**

<b>PPTP Server</b>	<b>Disabled</b>
<b>L2TP</b>	<a href="#">Show Connection</a>
<b>OpenVpn</b>	<a href="#">Show Connection</a>
<b>Active tunnels in L2TPV3</b>	<a href="#">Show Connection</a>
<b>Active tunnels in GRE</b>	<a href="#">Show Connection</a>
<b>Active tunnels in Ipsec</b>	<a href="#">Show Connection</a>

# Device

Another way to Add Router.

To reach this Page go to Network → Devices → Add New → Router

**Add Router** Network / Devices / Add Router

**General Settings**

Router Name:

Router Model:

Router Mac Address:

Router Description:

SSH:

Telnet:

Honey Trap:

LLDP:

Location:  Fixed  Live  
 Pin Point  Auto Suggestion

**Advance Settings**

Radio 0 Radio 1

Radio Status:

Operating Frequency:

Mode:

Channel:

Width:

Transmit Power:

RSSI Threshold:  Enable

RSSI:

## General Settings

1. **Router Name:** You can add any name.
2. **Router Model:** You can choose Router model from dropdown button.
3. **Router Mac Address:** You find router Mac on the back of your Device.
4. **Router Description:** Description is optional.
5. **SSH:** SSH, which stands for Secure Shell, is a cryptographic network protocol used for secure communication over an unsecured network. It is commonly used for remote administration of servers and secure file transfers. Enable the button if you want to activate SSH.

6. **Telnet:** Telnet is used on the internet or local area networks to provide a bidirectional interactive text- oriented communication facility using a virtual terminal connection. Enable the button if you want activate Telnet.

7. **Honey Trap:** Ahoney trap is set up to identify and mitigate potential threats or attacks. . Enable the button if you want activate Honey Trap.

8. **LLDP:** LLDP plays a crucial role in facilitating the automatic discovery and mapping of network topologies, making it easier to manage and troubleshoot network configurations, especially in diverse and multivendor environments. Enable the button if you want activate LLDP.

9.**Location :** Set the location either on Live or Fixed. In Fixed mode you have to set the device's location manually and in Live mode the device will automatically set its location.

Then click on Add router button.

## Advanced Settings

1. **Radio0 and Radio1:** These are the network bands. 0 indicates 2.4GHz and 1 indicates 5GHz.

2. **Mode:** Different Router has its different Modes(N ,AC, AX and Legacy).

**N Mode (802.11n):** Offers improved speed and range over older standards. It operates in both 2.4 GHz and 5 GHz bands and uses multiple antennas (MIMO) for better data rates.

**AC Mode (802.11ac):** Operates exclusively in the 5 GHz band. It provides even higher speeds and performance than 802.11n, utilizing advanced MIMO technology and wider channel bandwidths.

**AX Mode (802.11ax):** Also known as Wi-Fi 6, this standard improves efficiency in crowded environments. It operates in both 2.4 GHz and 5 GHz bands, supporting higher data rates, increased device capacity, and better performance in congested areas.

**Legacy Mode:** Supports older standards like 802.11a/b/g, allowing compatibility with older devices. However, using legacy mode can limit the network's potential speed and capabilities.

3. **Channels:** Essentially, these are the two supported network frequencies of our Routers. You can select options from the dropdown button. When you are on Radio0, the 2.4GHz frequencies are displayed and when you are on Radio1, the 5GHz frequencies are displayed.

4. **Width:** It determines the amount of frequency spectrum the Router occupies. The channel width can impact data transfer rates, capacity, and interference in the network. You need to select the appropriate width based on the Router you have chosen. Radio0 supports only 20MHz and 40 MHz. And Radio1 supports all the frequencies mentioned below.

**20 MHz:**This is the standard channel width and provides good compatibility and lower interference. It's commonly used in environments where there are many overlapping Wi-Fi networks.

**40 MHz:**This wider channel width can provide higher data rates but may also introduce more interference in crowded environments. It's usually used in networks with fewer neighboring networks.

**80 MHz:**This wider channel width offers even higher data rates but requires a relatively clean spectrum to operate effectively without causing interference to other networks.

**160 MHz:**This is an even wider channel width option, providing very high data rates. However, it requires a significant portion of clear spectrum to operate properly and is more commonly used in less congested environments.

5. **Transmit Power:** It is the signal strength of the Device. Transmit power is usually measured in decibels milliwatts(dBm) or milliwatts (mW). Higher power can extend range but might cause interference. Lower power reduces interference but limits range. It's regulated to prevent disruption. Adjusting it affects coverage and signal quality. Our Routers support dynamic power control, where the device automatically adjusts its transmit power based on factors like distance to connected devices and interference levels.

5. **RSSI:** Received Signal Strength Indication (RSSI) is the minimum signal strength a device needs to maintain a reliable connection to a network. It prevents weak connections that could lead to slow or unstable data transmission. It helps devices make decisions like roaming between Routers and avoiding interference. Configuring this threshold ensures a stable and efficient wireless network.

## Device Groups

To create a group of Router go to Network → Device Group → Add New → Router

Enter the given fields and select the router with which you want to create a group then click on Add Router Group Button.

The screenshot shows the 'Add Router Group' form. It has a breadcrumb trail: Network / Device Group / Add Router Group. The form includes a blue header 'Create Routers Group'. Below it are two input fields: 'Name' with a placeholder 'Enter Group Name' and 'Description' with a placeholder 'Group Description...'. There is a 'Show 10 entries' dropdown and a 'Search:' input field. A table lists four routers with columns for Router Name, MAC Address, and Model. At the bottom, there is a 'Showing 1 to 4 of 4 entries' indicator and 'Previous 1 Next' navigation buttons. A blue button labeled 'Add Router Group' is at the bottom left.

<input type="checkbox"/>	Router Name	MAC Address	Model
<input type="checkbox"/>	123659	de:30:d7:e3:e1:a3	KRO-110-D4G
<input type="checkbox"/>	d4g	92:99:0c:56:57:f5	KRO-110-D4G
<input type="checkbox"/>	demo_by_name	92:69:0c:56:57:f2	KRO-110
<input type="checkbox"/>	kro 4g	7a:a3:e3:eb:41:85	KRO-110-4G

Creating Router groups within a cloud controller can enhance the efficiency, security, and manageability of on-premises resources, contributing to a smoother and more effective cloud computing environment.

To create a group of Routers go to Network → Device Groups

The screenshot shows the 'Device Groups (8)' list. It has a breadcrumb trail: Networks / Device Groups. There is an 'Add New' button and a 'Search:' input field. A table lists three device groups with columns for Group Name, Type, Description, Total Device's, and Action. At the bottom, there is a 'Showing 1 to 8 of 8 entries' indicator and 'Previous 1 Next' navigation buttons.

Group Name	Type	Description	Total Device's	Action
540	CPE Group		1	
SgRouter	Router Group		1	
apGrp	AP Group		1	

To edit the group, click on any edit icon, choose the appropriate options, and finally, click the 'Update' button.

# Device Binding

For Router Device binding go to Network → Device Binding

Device Group	Controller Name	Action
Kenstel CPE Grp	ip-172-31-21-162	

Add New → Router

Please select the Router Group and controller which you want to bind then click on Add Binding.

**Router Binding Settings**

Router Group:

Controller:

Binding a Router group with a controller enhances the management, security, automation, and integration capabilities of the cloud infrastructure, leading to improved efficiency, reliability, and scalability for the organization.

## Configuration.....3













Wireless.....	3.1		
Network.....	3.1.1		
Network Group.....	3.1.2		
Network Binding.....	3.1.3		
User Group.....	3.1.4		
Access Control.....	3.1.5		
Airtime Fairness.....	3.1.6		
Common Device Setting.....	3.1.7		
Cellular .....	3.2		
Cellular Config.....	3.2.1		
APN Setting.....	3.2.2		
Lock-Bands.....	3.2.3		
Operator Selection.....	3.2.4		
Captive Portal.....	3.3		
Captive User Management.....	3.3.1		
Voucher Management.....	3.3.2		
Network.....	3.4		
IPV4.....	3.4.1		
IPV6.....	3.4.2		
WAN.....	3.4.3		
VLAN.....	3.4.4		
Address Reservation.....	3.4.5		
Port Setup.....	3.4.6		
SDN.....	3.4.7		
VPN.....	3.5		
PPTP.....	3.5.1		
L2TP.....	3.5.2		
GRE.....	3.5.3		
IPsec.....	3.5.4		
OpenVpn.....	3.5.5		
Neighbour.....	3.5.6		
Routing.....	3.6		
Static Route.....	3.6.1		
RIP.....	3.6.2		
OSPF.....	3.6.3		
BGP.....	3.6.4		
Firewall.....	3.7		
Port Forwarding.....	3.7.1		
IP Filter.....	3.7.2		
Mac Filter.....	3.7.3		
Port Filter.....	3.7.4		
URL Filter.....	3.7.5		
NAT.....	3.7.6		
IPS.....	3.7.7		
Attack Defense.....	3.7.8		

# Networks

To create Networks go to Configuration → Wireless → Networks

Networks ( 4 ) Configuration / Wireless / Networks

Show 10 entries Search:  [+ Add](#)

Network Name	Description	Security Mode	Created At	Action
Kenstel--1		open	<a href="#">Tue Apr 02 2024 10:20:09 GMT+0000 (Coordinated Universal Time)</a>	  
Kenstel--2		open	<a href="#">Wed Apr 03 2024 06:13:14 GMT+0000 (Coordinated Universal Time)</a>	  
Kenstel--3		open	<a href="#">Wed Apr 03 2024 06:13:40 GMT+0000 (Coordinated Universal Time)</a>	  
Kenstel--4		open	<a href="#">Wed Apr 03 2024 06:13:56 GMT+0000 (Coordinated Universal Time)</a>	  

Showing 1 to 4 of 4 entries Previous **1** Next



View here the already added networks.



You can edit the network by clicking on this button.



You can delete the network by clicking on this button.

# Networks

For Adding Networks go to Configuration → Wireless → Networks → Add New

The screenshot displays the 'Add New Network' configuration page. It is divided into two main sections: 'Basic Info' and 'Advanced Settings'.  
**Basic Info:** Contains fields for 'Network Name' (with a placeholder 'Enter Network Name / SSID'), 'Description' (with a placeholder 'Network Description...'), and 'Security Mode' (set to 'Open'). An 'Add Network' button is located at the bottom left of this section.  
**Advanced Settings:** Contains various toggle and dropdown options:

- Status: Radio buttons for 'Auto' (selected) and 'Manual'.
- SSID Broadcast: Checked 'Enable'.
- WPA3-OWE: Unchecked 'Enable'.
- Rate Limit: Unchecked 'Enable'.
- ACL Rule: Dropdown menu set to 'None'.
- User Group: Dropdown menu set to 'None'.
- Enable Bridging: Unchecked 'Enable'.
- VLAN ID: Input field with '(0-100)' placeholder.
- Airtime Fairness: Unchecked toggle.
- Wifi Multimedia: Checked toggle with a play icon.
- MFP: Radio buttons for 'Enable (Not Required)', 'Enable (Required)', and 'Disable' (selected).
- Hotspot 2.0: Unchecked 'Enable'.
- Roaming: Checked 'Enable'.
- Band Steering: Unchecked 'Enable'.
- Layer2 User Isolation: Unchecked 'Enable'.
- STP: Unchecked 'Enable'.


Enter the given fields and click on Add Network

Here you can choose the options of Security Mode from the dropdown button.

1. **Radius MAC:** In Radius MAC we add the Server IP, in Authentication Server Port we have to add Server Port and in Authentication Server Password we put Server Credentials.
2. **Status:** If we set the status in Auto the default IP will display and if we set the status in Manual then we have to input the details manually.
3. **SSID Broadcast:** If we enable SSID Broadcast then only our created networks will visible publicly.
4. **Rate limit:** By Enable Rate limit we can set the download and upload speed limit.
5. **ACL Rule:** An "ACL rule" is a directive within an Access Control List (ACL), specifying what is allowed or denied for specific sources, destinations, protocols, and conditions in a network, system, or application. ACLs are used to control access to resources and enforce security policies. We have to add MAC Address of an individual device and then we can edit in Whitelisting or Blacklisting(only one at time).
6. **User Group:** User group settings are essential for authentication and authorization processes. When users log in, the system checks their group membership to determine what they can access. User group settings are a way to organize and manage users within a network efficiently. They help maintain security, optimize network performance, and ensure that users have appropriate access to network resources based on their roles and responsibilities. We have to go the User Group Setting and 1. Set a group name 2. Add user's MAC Address 3. Set rate limit(Download) 4.Set rate limit(Upload) and finally add this user group with the network.
7. **Bridging:** Bridging is commonly used in scenarios where Ethernet LANs need to be extended or connected, especially in large enterprise networks. It allows for the creation of larger and more flexible network topologies, helps reduce network congestion, and simplifies network management. If we enable bridging then the individual network is not shown in the Captive Portal. If we don't provide specific ID to VLAN then VLAN ID will by default get the LAN ID. Here, in case of Router device Bridging is not working.
8. **VLAN ID:** A VLAN ID (Virtual LAN Identifier) in a network is a numerical tag that is assigned to a Virtual LAN (VLAN) to uniquely identify it within a larger network infrastructure. VLANs are used to logically segment a physical network into multiple virtual networks, allowing network administrators to control traffic, improve network security, and manage network resources more efficiently. VLAN IDs are a critical part of network segmentation and management, helping organizations optimize their network resources, enhance security, and simplify network administration in complex environments. If we enable bridging then only we can add VLAN ID.

**9. Airtime Fairness:** Airtime fairness helps to optimize the use of the wireless spectrum and ensure that all devices receive a fair share of airtime, leading to better performance and reliability in Wi-Fi networks.

**10. Wi-Fi Multimedia:** Wi-Fi Multimedia (WMM) is a feature in Wi-Fi networks that prioritizes traffic types, such as voice and video, to improve the quality of service for multimedia applications. It categorizes traffic into four access categories, uses Enhanced Distributed Channel Access (EDCA) for prioritization, and defines quality of service parameters to ensure smoother and more reliable performance for time-sensitive applications.

You can edit by clicking on edit icon. 

**11. MFP:** Management Frame Protection (MFP) is a Wi-Fi security feature that safeguards against attacks targeting management frames. It uses message integrity checks (MICs) to ensure the integrity and authenticity of management frames, particularly deauthentication frames, helping to mitigate potential security threats in Wi-Fi networks. You can choose the options as per your requirement.

**12. Hotspot 2.0:** Hotspot 2.0 improves the usability, security, and performance of Wi-Fi networks, making it easier for users to connect to and roam between Wi-Fi hotspots while maintaining high levels of security and privacy.

**13. Roaming:** Roaming allows your devices to roam freely between multiple Router networks without losing their connection.

**14. Band Steering:** Band steering is a Wi-Fi optimization technique that encourages client devices to connect to the less congested 5 GHz frequency band instead of the 2.4 GHz band when possible. It aims to improve performance, maximize throughput, and balance client distribution across bands for a better overall user experience in wireless networks.

**15. Layer 2 User Isolation:** Layer 2 user isolation, achieved through VLAN segmentation, enhances network security, control, and performance by restricting communication between devices within the same VLAN while allowing for efficient routing and communication between VLANs.

**16. STP:** STP stands for Spanning Tree Protocol. It is a network protocol used to prevent loops in Ethernet networks, which can cause broadcast storms and lead to network instability.

# Networks

The screenshot displays a network configuration interface with two main sections: Basic Info and Advanced Settings.

**Basic Info:**

- Network Name: Enter Network Name / SSID
- Description: Network Description...
- Security Mode: WEP
- Key Selected: Key1
- Key-Value 1: Enter Key Value
- Buttons: Add Network

**Advanced Settings:**

- Type:  Auto  Open System  Shared Key
- WEP Key Format:  ASCII  Hexadecimal
- Key Type:  64Bit  128Bit
- Status:  Auto  Manual
- SSID Broadcast:  Enable
- Rate Limit:  Enable
- ACL Rule: None
- User Group: None
- Enable Bridging:  Enable
- VLAN ID: (0-100)
- Airtime Fairness:  Enable
- Wifi Multimedia:  Enable
- MFP:  Enable (Not Required)  Enable (Required)  Disable
- Hotspot 2.0:  Enable
- Roaming:  Enable
- Band Steering:  Enable
- Layer2 User Isolation:  Enable
- STP:  Enable

WEP was designed to provide a level of privacy and security for wireless networks that was supposed to be equivalent to that of a wired network. It used a shared key authentication system and encryption to protect data transmitted over the wireless network. However, several vulnerabilities were discovered in WEP over the years, making it relatively easy for attackers to crack the encryption and gain unauthorized access to a network.

Due to these vulnerabilities, WEP has been widely replaced by more secure protocols such as WPA (Wi-Fi Protected Access) and its successors, including WPA2 and WPA3, which offer much stronger security features.

**Key Selected:** In Key Selected, you can choose Key options from the dropdown button. And then set a password in Key 1 and the same password should be used in Key 2 Key 3 and Key 4.

**WEP Key Format:** ASCII and Hexadecimal keys typically refer to different types of encryption keys used to secure wireless networks. ASCII keys are typically made up of letters (both uppercase and lowercase), numbers, and other special characters. These keys are usually easier to remember but may be less secure compared to hexadecimal keys. A hexadecimal key, on the other hand, is a key composed of hexadecimal digits, which include the numbers 0-9 and the letters A-F (or a-f). Hexadecimal keys are often used when a stronger level of security is required for a wireless network.

**Key Type:** A 64-bit key is relatively short and provides relatively low encryption strength. And a 128-bit key is much stronger than a 64-bit key and is considered secure for most applications.

# Networks

The screenshot displays a network configuration interface with two main sections: 'Basic Info' and 'Advanced Settings'.

**Basic Info:**

- Network Name: Enter Network Name / SSID
- Description: Network Description...
- Security Mode: WPA-Enterprise
- Radius Server IP: 0.0.0.0
- Radius Port: (0-65535)
- Radius Password: [password field]
- Radius Accounting:  Enable
- Interim Update:  Enable
- Buttons: Add Network

**Advanced Settings:**

- Status:  Auto  Manual
- SSID Broadcast:  Enable
- Version:  Auto  WPA  WPA2  WPA3 SuiteB
- Encryption:  Auto  TKIP  AES
- Group Key Update Period: seconds(30-8640000, 0 means no upgrade)
- Rate Limit:  Enable
- ACL Rule: None
- User Group: None
- Enable Bridging:  Enable
- VLAN ID: (0-100)
- Airtime Fairness:  Enable
- Wifi Multimedia:  Enable
- MFP:  Enable (Not Required)  Enable (Required)  Disable
- Hotspot 2.0:  Enable
- Roaming:  Enable
- Band Steering:  Enable
- Layer2 User Isolation:  Enable
- STP:  Enable

## Version:-

**WPA (Wi-Fi Protected Access):** An older Wi-Fi security standard that improved upon WEP but is now considered insecure due to vulnerabilities. **WPA2 (Wi-Fi Protected Access 2):** A widely used Wi-Fi security standard that uses AES encryption and provides enhanced security compared to WPA.

**WPA3 (Wi-Fi Protected Access 3):** The latest Wi-Fi security standard with even stronger encryption and improved security features, making it the most secure choice.

**Suite B:** A set of cryptographic standards approved for securing sensitive information, including encryption algorithms, but not specific to Wi-Fi security standards.

## Encryption:-

**TKIP:** For encryption, Temporal Key Integrity Protocol is more secure than WEP but still had some vulnerabilities.

**AES:** Advanced Encryption Standard on the other hand, is considered highly secure.

**Group key Update Period:-** The Group Key Update Period determines how often the group key used for encrypting multicast and broadcast traffic in Wi-Fi networks is refreshed. This periodic rotation helps enhance security by reducing the risk of key compromise while balancing the impact on network performance.

# Networks

The image shows a network configuration interface with two main sections: 'Basic Info' and 'Advanced Settings'.

**Basic Info:**

- Network Name: Enter Network Name / SSID
- Description: Network Description...
- Security Mode: WPA-PSK
- Wireless Password: [Redacted]
- Buttons: Add Network

**Advanced Settings:**

- Status:  Auto  Manual
- SSID Broadcast:  Enable
- Version:  Auto  WPA  WPA2  WPA3 SAE  WPA3 SAE+PSK
- Encryption:  Auto  TKIP  AES
- Group Key Update Period: seconds(30-8640000, 0 means no upgrade)
- Rate Limit:  Enable
- ACL Rule: None
- User Group: None
- Enable Bridging:  Enable
- VLAN ID: (0-100)
- Airtime Fairness:  Enable
- Wifi Multimedia:  Enable
- MFP:  Enable (Not Required)  Enable (Required)  Disable
- Hotspot 2.0:  Enable
- Roaming:  Enable
- Band Steering:  Enable
- Layer2 User Isolation:  Enable
- STP:  Enable




**WPA3 SAE:** SAE is a key exchange protocol used in WPA3 for securing the initial connection between a device and a Wi-Fi network. SAE ensures that both the client device and the access point mutually authenticate each other, preventing man-in-the-middle attacks during the initial connection setup.

**PSK (Pre-Shared Key):** PSK is a passphrase or shared secret key that is used to authenticate and encrypt the connection between the client device and the access point. It is more convenient for home and small office networks as it eliminates the need for a complex and individualized key setup for each device.

But when you use WPA3 SAE+PSK security, you get the robust security benefits of WPA3 SAE during the initial connection setup while still using a pre-shared key for convenience, especially in small-scale network deployments.

# Network Groups

To create Network Groups go to Configuration → Wireless → Networks Groups

Group Name	Description	Created At	Action
Bikash Network Group		Tue Apr 02 2024 10:20:51 GMT+0000 (Coordinated Universal Time)	  

Here you able to see the history of already created groups.

Enter the required fields, then select the Networks with which you want create a group and select the network band then click on Add Network Group button.

Select	Interface	Network	Band
<input checked="" type="checkbox"/>	1	Select Network	Select Band
<input type="checkbox"/>	2	Select Network	Select Band
<input type="checkbox"/>	3	Select Network	Select Band
<input type="checkbox"/>	4	Select Network	Select Band
<input type="checkbox"/>	5	Select Network	Select Band
<input type="checkbox"/>	6	Select Network	Select Band
<input type="checkbox"/>	7	Select Network	Select Band
<input type="checkbox"/>	8	Select Network	Select Band

**Bands:** Choose bands from the dropdown according to your preference. Select bands to 2.4 GHz or 5 GHz or both.

Creating network groups or similar constructs in cloud controllers helps with resource organization, security, scalability and overall management

of your cloud infrastructure. It allows you to logically group related resources, control their communication, and apply policies consistently.

# Network Binding

To create Network Groups go to Configuration → Wireless → Networks Binding

Device Group	Network Group Name	Action
Bikash CPE Group	Bikash Network Group	

Here you able to see the already binded Networks.

Please select the Device Group and Network Group which you want to bind then click on Add Binding.

**Network Binding Settings**

Device Group

Network Group

Add Binding

Binding Device groups and network groups together in a cloud controller offers simplified management, consistent configuration, network segmentation, load balancing, event reporting, scalability, policy enforcement, and flexibility in handling access points and their associated network segments.

# User Group

To create User Groups go to Configuration → Wireless → User Group

Monitor User Group ( 0 ) Dashboard / Account / User Group

Show 10 entries Search:  [+ Add New](#)

User Group Name	Action
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

A user group refers to a logical grouping or categorization of users with similar characteristics, permissions, or access levels. These groups make it easier to manage and control access to resources, services, and applications within the cloud infrastructure.

Add User Group Dashboard / Account / User Group / Add User Group

**Add a User**

User Group Name

User Mac Address  [+ Add New](#)

Rate Limit (Download)

Rate Limit (Upload)

[Add Group](#)

**User Group Name:** Input a name for the group identification.

**User MAC Address:** Input the MAC Address of the user with which you want to make a User Group. Here you can multiple MAC Addresses.




**Rate Limit:** Here you can set the rate limit of download and upload speed within 0 to 10000.

# Access Control

Configuration → Wireless → Access Control

Access Control Rules ( 1 ) Dashboard / Wireless / Access Control

Show  entries Search:  [+ Add New](#)

Rule Name	Action
cdcv	  

Showing 1 to 1 of 1 entries Previous **1** Next

Access control is a fundamental security measure that involves managing and regulating access to resources (such as systems, applications, data, or physical locations) within an organization. The goal of access control is to ensure that only authorized individuals or systems can access and interact with specific resources, while unauthorized access is prevented or restricted.



Click to view the settings.



Click to edit the settings.



Click to delete the settings.

Add Access Control Rules Dashboard / Wireless / Access Control / Add Access Control

**Add a rule**

Rule Name

Mode  Blacklist  Whitelist \* Only one mode will work at a time.

Blacklist

Whitelist

**Rule name:** A rule name refers to a descriptive identifier assigned to a specific access control rule or policy. A rule name is a human- readable label that helps administrators, security personnel, and other stakeholders easily identify and understand the purpose of a particular access control rule within a system or security infrastructure.

**Mode:** Enable the mode either in Blacklist or Whitelist

**Blacklist:** Enter the MAC Address which you want to block. Here you can add multiple MAC Addresses by clicking on

**Whitelist:** Enter the MAC Address which you want to allow . Here you can add multiple MAC Addresses by clicking on



















# Airtime Fairness

Configuration → Wireless → Airtime Fairness

Airtime Fairness refers to a feature that ensures fair distribution of available airtime (communication time) among connected devices. This is particularly important in wireless networks to prevent certain devices from dominating the available airtime and causing performance issues for other devices.

Airtime Fairness ( 6 ) Configuration / Wireless / Airtime Fairness

Show  entries Search:  [+ Add](#)

Rule Type	Group/Network Name	Action
Client	Austin-1	  
Client	wpa+psk1	  
Network	Shivang+Network+Group	  
Network	A--[ Bikash Network Group ]	  
Network	wireless test	  
Network	Prabhash	  

Showing 1 to 6 of 6 entries Previous **1** Next



Click to view the settings.



Click to edit the settings.



Click to delete the settings.

If you want to add more networks then click on [+ Add](#) button.

Here, you can add more networks/ network groups.

The image shows a dialog box titled "Airtime Fairness" with a close button (X) in the top right corner. Below the title bar is a blue header with the text "Configure Airtime Fairness". The main area contains three rows of configuration options, each with a label on the left and a dropdown menu on the right:

- Rule Type:** The dropdown menu shows "Network".
- Group:** The dropdown menu shows "SMITA Network".
- Network:** The dropdown menu shows "Select SSID" with a downward arrow.

At the bottom right of the dialog box, there are two buttons: "Cancel" and "Apply".

**Rule Type:** Select network from the drop down.

**Group:** Select network group from the drop down.

**Network:** Select networks that are present within the above network group.

## Common Device Setting

Configuration → Wireless → Common Device Settings

**Settings**

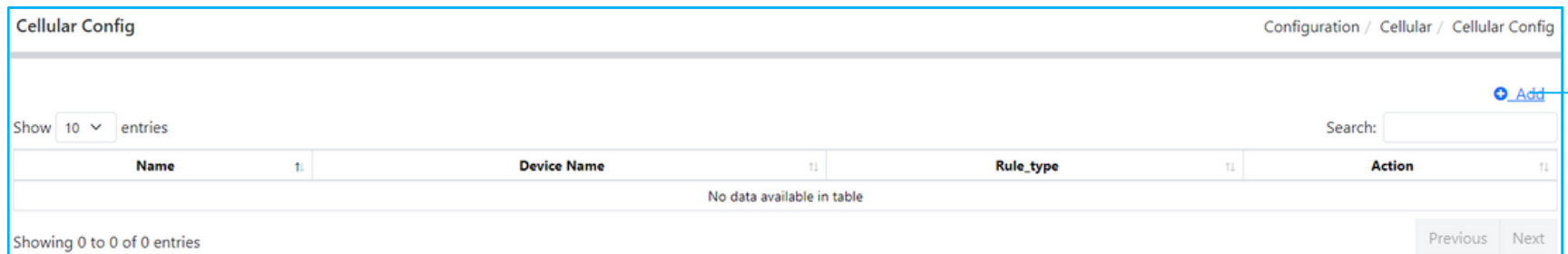
Device Group

Common Setting

Select both the options from the drop down and click on Apply.

## Cellular Setting - Cellular Config

For Cellular Setting go to Configuration → Cellular → Cellular Config



Cellular Config

Configuration / Cellular / Cellular Config

Show 10 entries

Search:

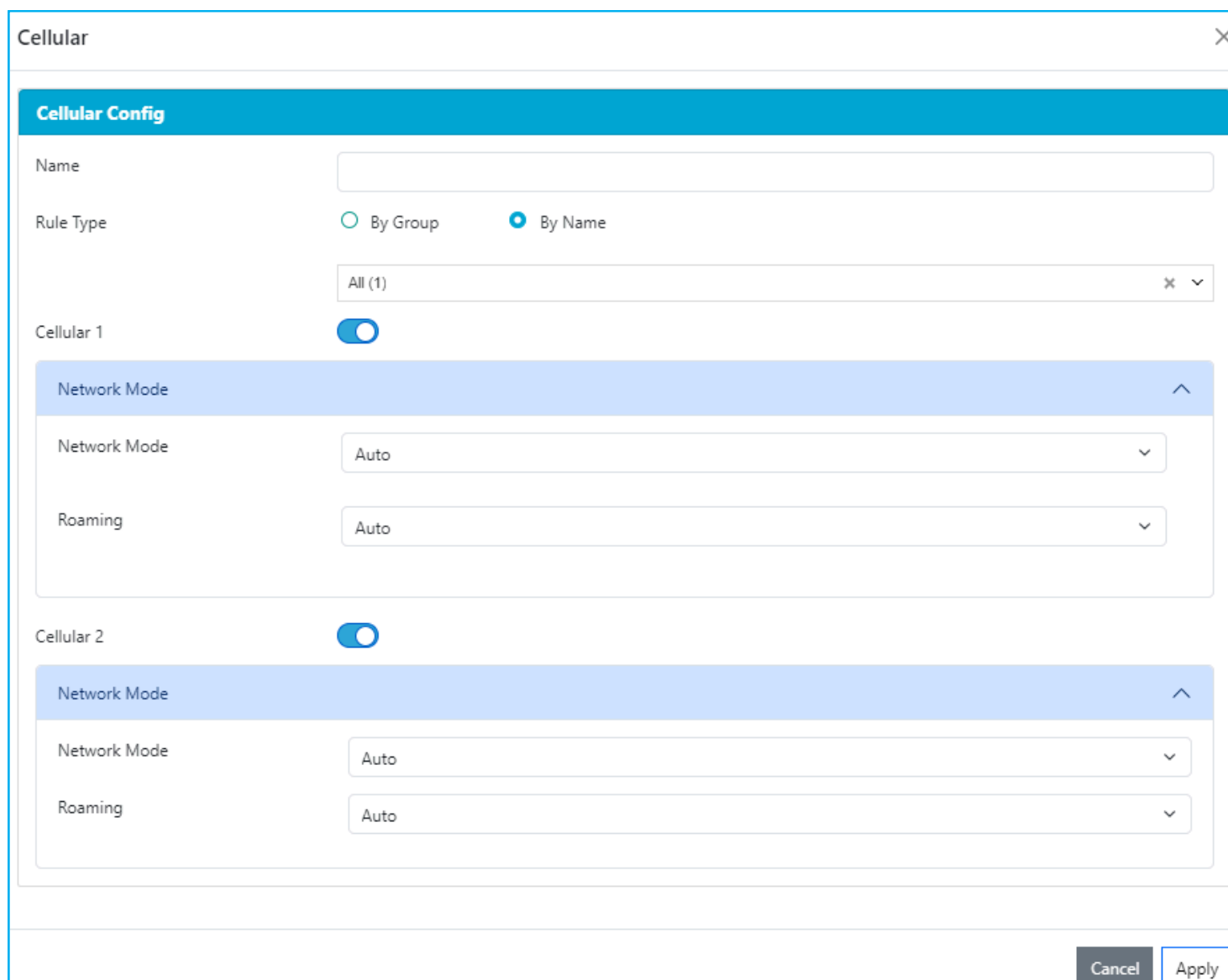
[Add](#)

Name	Device Name	Rule_type	Action
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

Cellular configuration typically refers to the setup and management of cellular connectivity for devices within the cloud environment. This could include configuring devices to connect to cellular networks, managing data plans, monitoring usage, and ensuring reliable connectivity.



Cellular

**Cellular Config**

Name

Rule Type  By Group  By Name

All (1)

Cellular 1

Network Mode

Network Mode

Roaming

Cellular 2

Network Mode

Network Mode

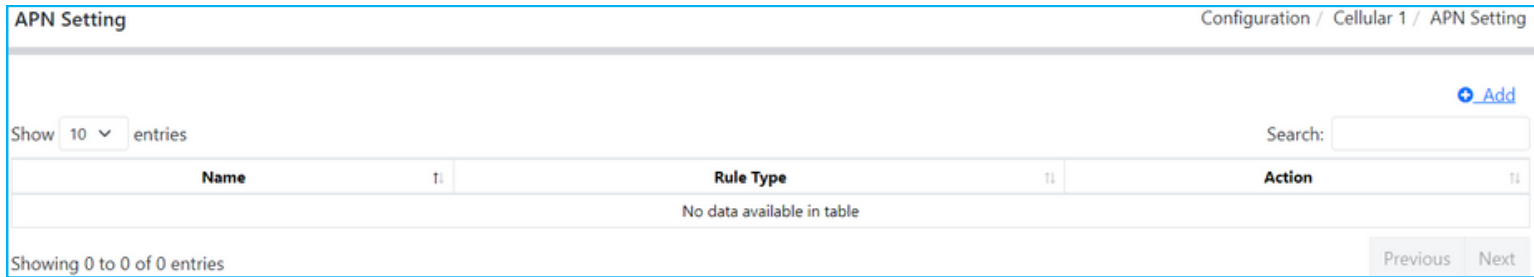
Roaming

Cancel Apply

Select the Options from the dropdown button and click on Apply Button.

# Cellular Setting - APN Setting

For Cellular Setting go to Configuration → Cellular → APN Setting



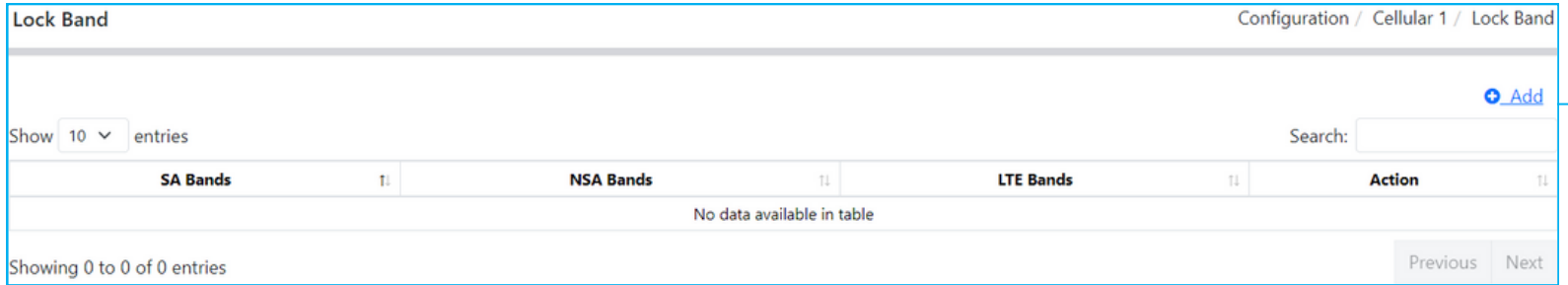
Configuring the Access Point Name (APN) settings is crucial for establishing the connection between the device and the cellular network. The APN acts as a gateway between the mobile network and the internet or a private network, depending on the specific requirements of the application.

The screenshot shows a 'Cellular' configuration dialog box. It has a title bar with a close button. Below the title bar is a section for 'APN Setting' with a blue header. The 'Name' field is empty. The 'Rule Type' section has two radio buttons: 'By Group' (unselected) and 'By Name' (selected). Below this is a dropdown menu showing 'All (1)'. There are two sections for cellular settings, 'Cellular 1' and 'Cellular 2', each with a toggle switch that is turned on. Each section has a 'Configuration' header and four input fields: 'APN Name', 'Username', 'Password', and 'Authentication'. The 'Authentication' dropdown is currently set to 'NONE'. At the bottom right, there are 'Cancel' and 'Apply' buttons.

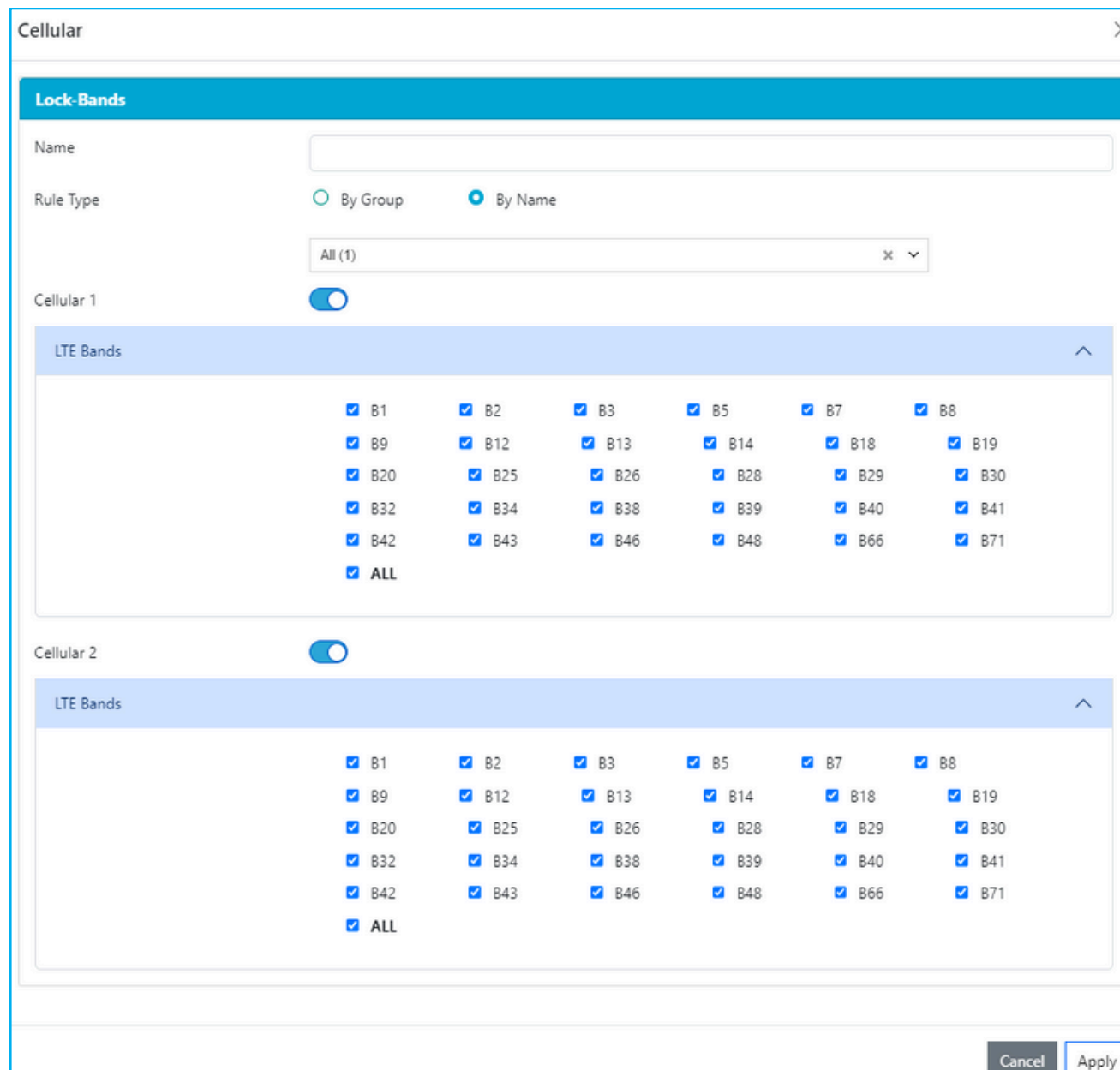
Fill the credential and Select the authentication mode from the dropdown button and click on Apply Button.

# Cellular Setting - Lock Band

For Cellular Setting go to Configuration → Cellular → Lock Band



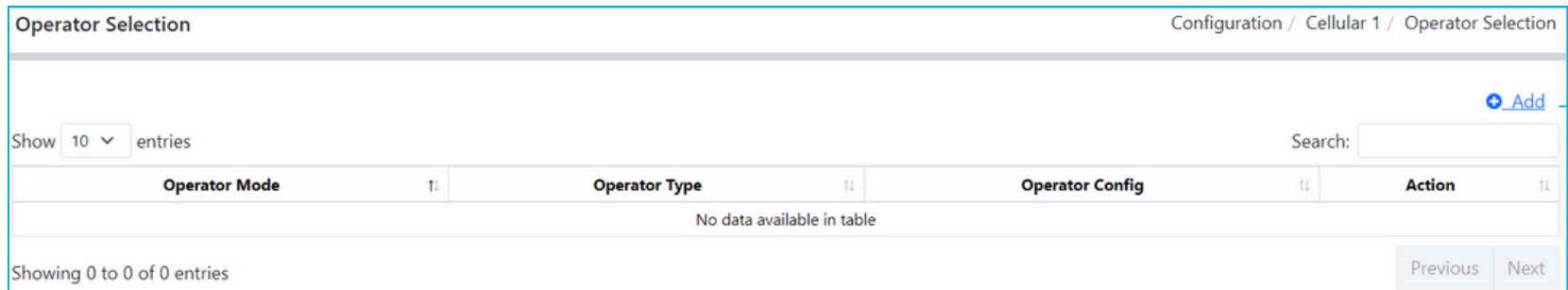
By locking bands in cellular configurations managed by a cloud controller, organizations can optimize the performance, reliability, and regulatory compliance of their cellular deployments, ensuring seamless communication and connectivity for their devices.



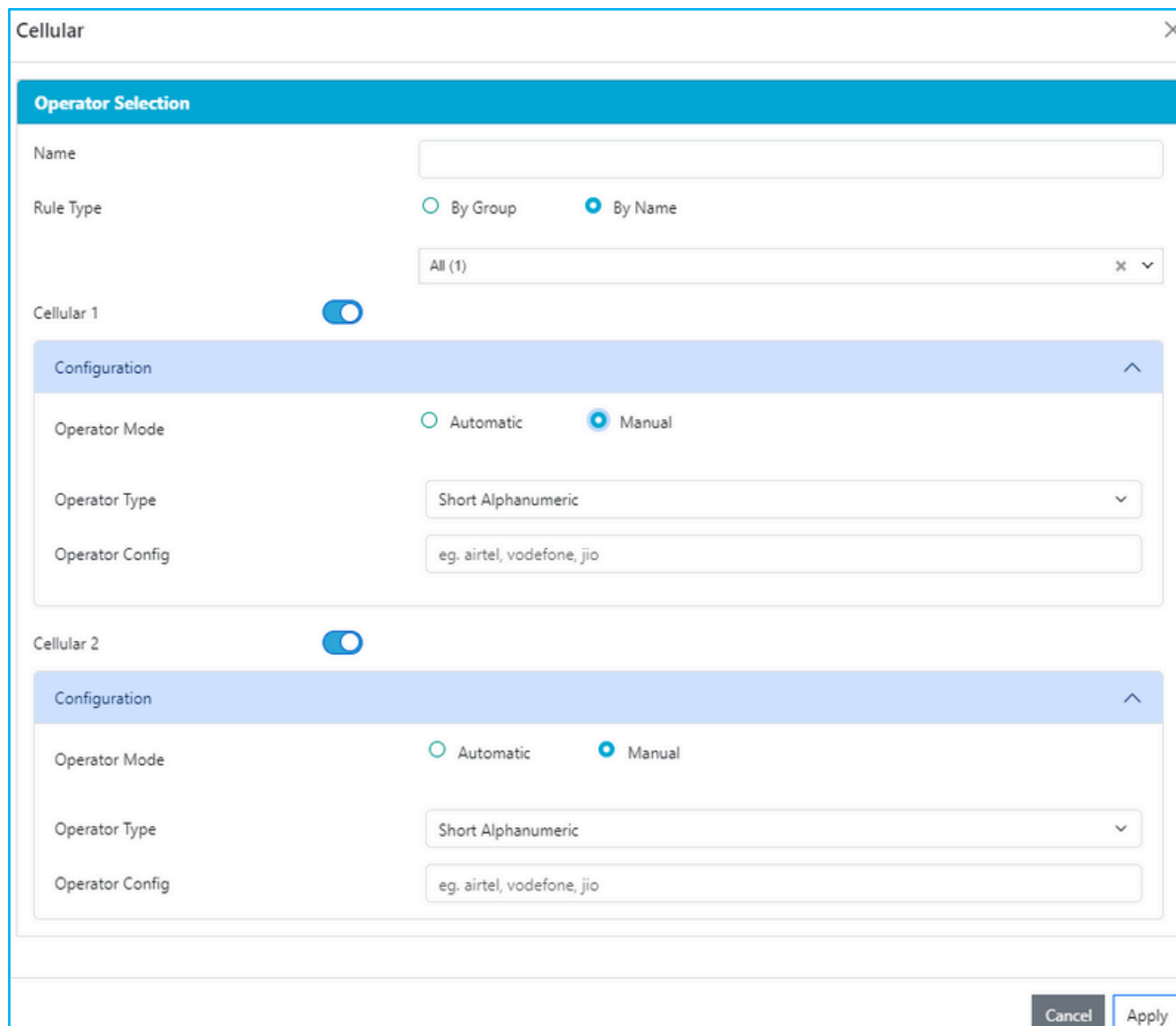
**LTE Bands:** LTE (Long-Term Evolution) is a 4G wireless standard that provides increased network capacity and speed for cellphones and other cellular devices compared with 3G technology. An LTE network employs the multiuser variant of the orthogonal frequency-division multiplexing (OFDM) modulation scheme, called orthogonal frequency-division multiple access (OFDMA), for its downlink signal.

# Cellular Setting - Operator Selection

For Cellular Setting go to Configuration → Cellular → Operator Selection

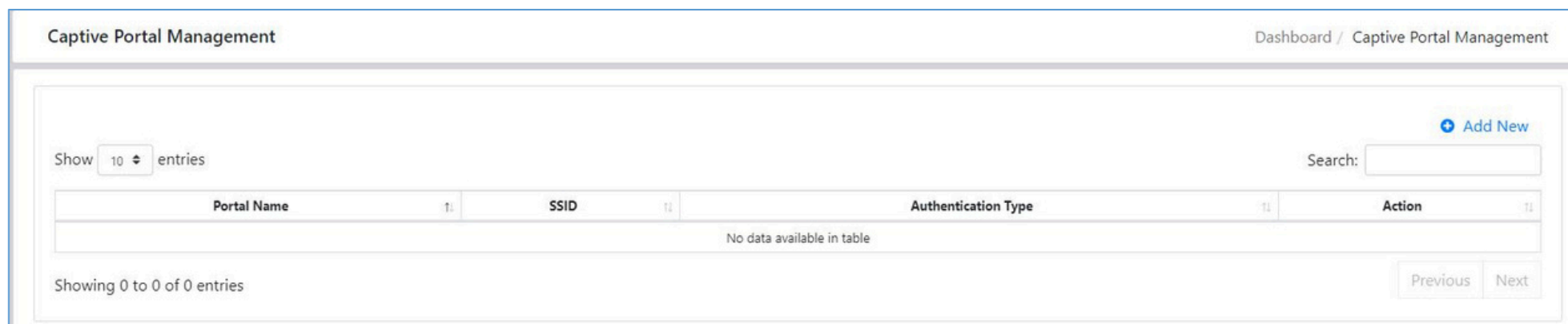


A network operator is responsible for the implementation, configuration, and management of TCP/IP protocols across a Cellular network infrastructure. They also ensure reliable data transmission by establishing and maintaining TCP connections between Router devices and Network.



# Captive Portal

To Add Captive Portal go to Configuration → Captive Portal



A captive portal in the context of a cloud controller typically refers to a network security feature used to authenticate and manage access to a wireless or wired network. Captive portals are commonly used in public Wi-Fi networks, such as in hotels, airports, coffee shops, or other public places, to control access to the internet or network resources.

## Benefits of Captive portal:

1. **Access Control:** Ensures that only authorized users can access the network or internet resources.
2. **Security:** Requires users to authenticate or accept terms of use, reducing the risk of unauthorized access.
3. **User Tracking:** Monitors user activity and enforces network policies.
4. **Customization:** Can display branding, advertisements, or specific messages.
5. **Compliance:** Helps organizations meet legal requirements, such as providing terms of use agreements.

# Captive Portal

Configuration → Captive Portal → Add New → General Settings

The screenshot shows the 'Add Captive Portal' configuration interface. The 'General Settings' tab is selected. The 'Authentication Type' dropdown menu is open, showing options: 'Simple Password', 'No Authentication', 'Local User', 'Local User (Active Directory)', 'Voucher', 'SMS', 'Facebook', 'External Radius Server', and 'Mbps (0-10000)'. The 'HTTPS Redirect' checkbox is checked. On the right side, there are two storage status indicators: '9.17 MB AVAILABLE' and '0.12 MB IN USE'.

Select the network, enter the selected network name in the 'Portal Name,' and then choose the authentication type from the dropdown menu. Select the option according to your preference. The details of the authentication type differ with every option, so fill them in. Set the login page and then click on the 'Apply' button.

## Authentication Type

**Simple Password:** Here you can put any kind of password.

This screenshot shows the configuration for 'Simple Password' authentication. The 'Authentication Type' dropdown is set to 'Simple Password'. Below it is a 'Password' input field with a toggle for visibility.

**Local User:** Once you fill all the details click on Apply button then click Radius Management to go Radius Management Settings.

This screenshot shows the configuration for 'Local User' authentication. The 'Authentication Type' dropdown is set to 'Local User'. Below it is a 'Radius Management' button with a user icon.

# Captive Portal

## Radius Management

Configuration → Radius Management

Radius Management Dashboard / Radius Management

Show  entries

[Add New](#) [Upload CSV](#)

Search:

Name	Username	Telephone	Action
No data available in table			

Showing 0 to 0 of 0 entries

Add RADIUS User Dashboard / Radius Management / Add RADIUS User

**RADIUS Settings**

Username:

Password:

Authentication Timeout:

Maximum Users:

Name:

Telephone:

Rate Limit (Download):  Enable

Rate Limit (Download):

Rate Limit (Upload):  Enable

Rate Limit (Upload):

Traffic Limit:  Enable

Traffic Limit (In MBs):

Fill the credentials and click on Add User button.

Local User (Active Directory): Fill the credentials below.

Authentication Type	<input type="text" value="Local User (Active Directory)"/>
IP	<input type="text"/>
Active Directory DNS Name	<input type="text"/>
Active Directory Domain Name	<input type="text"/>

**Voucher:** Once you fill all the details click on Apply button then click on Voucher Management to go Voucher management Settings.

Authentication Type	<input type="text" value="Voucher"/>
Captive User Rate Limit	<input type="checkbox"/> Enable
Rate Limit (Download)	<input type="text" value="Mbps (0-10000)"/>
Rate Limit (Upload)	<input type="text" value="Mbps (0-10000)"/>
<a href="#">Voucher Management</a>	

# Captive Portal

## Voucher Management

Configuration → Voucher Management

Voucher Management Dashboard / Voucher Management

Show 10 entries Delete Print Add New

Search:

<input type="checkbox"/>	Code	Created Time	Notes	Duration	Status	Action
<input type="checkbox"/>	149095	Tue Aug 29 2023 18:23:59 GMT+0530 (India Standard Time)		1 Hour	Valid for single use	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	210672	Tue Sep 12 2023 15:07:39 GMT+0530 (India Standard Time)		1 Hour	Valid for 2 users	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 to 2 of 2 entries Previous 1 Next

Fill the details and click on Apply to Create voucher.

### Create Vouchers

**Voucher Settings**

Code Length:

Amount:

Type:

Duration:

Rate Limit (Download):  Enable

Rate Limit (Upload):  Enable

Traffic Limit:  Enable

Note:

## Captive Portal


**SMS:** Go to TwilioWebsite, generate your TwilioSID and AuthToken then put it below. Also put the Mobile number. Lastly set the user limit and country code then Apply.

Authentication Type	SMS
We provide Twilio Messaging Service. Please provide us the twilio account details.	
Twilio SID	<input type="text"/>
Auth Token	<input type="text"/>
Mobile Number	+919044XXXXXX
Maximum User	(0-10, 0 means no limit)
Preset Country Code	(E.g., +91)

**Facebook:** After filling all the details click on Apply button. And then click on Configuration to go to Facebook Page.

Authentication Type	Facebook
Facebook Page Configuration	<a href="#">Configuration</a>

## External Radius Server:

Authentication Type	External Radius Server
Authentication Timeout	1 Hour
RADIUS Server IP	
RADIUS Port	1812
RADIUS Password	<input type="password"/> 
Authentication Mode	PAP
NAS ID	Kenstel
RADIUS Accounting	<input type="checkbox"/> Enable
Portal Customization	External Web Portal
External Web Portal URL	


# Captive Portal

Configuration → Captive Portal → Add New → Login Page

### Login Page

Background  Solid Color  Picture

Background Color



Logo Picture   
Max Size: 50 kB

Welcome Information   
(1-31 characters)

Welcome Text Color

Button Background Color

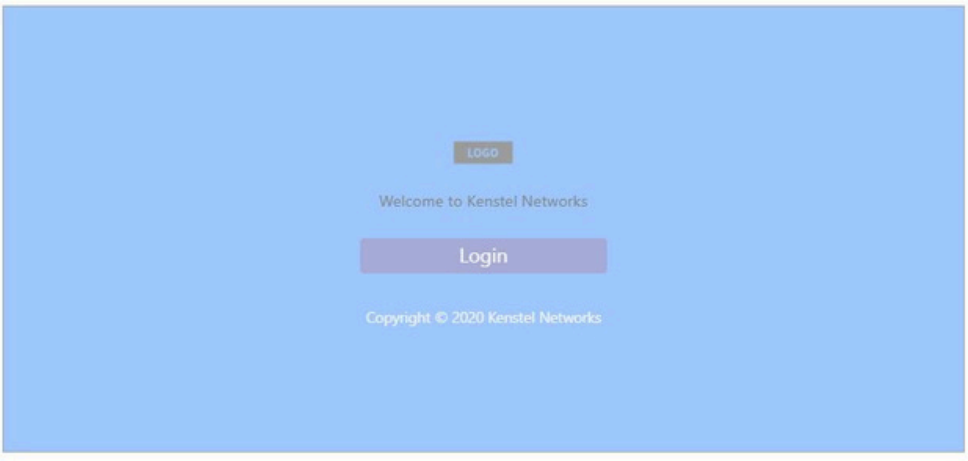
Button Text Color

Copyright   
(1-70 characters)

Copyright Text Color

Terms of Service  Enable

### Captive Portal View

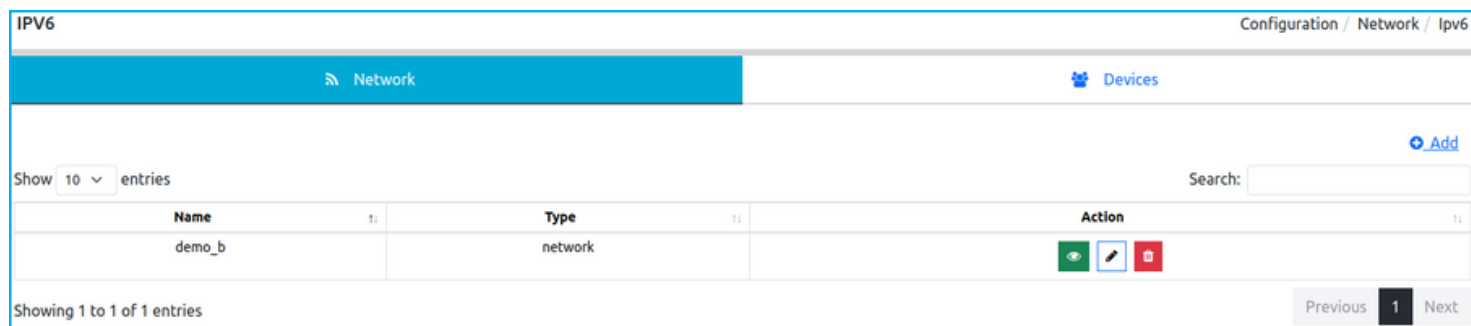


When you connects to a network with a captive portal, then you redirected to a login page. In the above showing page you can edit your login page UI.

# Network - IPv6

Configuration → Network → IPv6

IPv6, or Internet Protocol version 6, is the latest version of the Internet Protocol designed to overcome the limitations of IPv4. It has a much larger address space using 128 bits for addressing (compared to IPv4's 32 bits), simplified header format, improved security with built-in IPsec, automatic address configuration, enhanced multicast and anycast capabilities, and supports backward compatibility with IPv4. IPv6 is essential for accommodating the growing number of devices on the internet and ensuring its continued development.



To add IPv6 to any Networks click on Add

The 'Network' dialog box is open, showing the 'IPv6' section. It has three input fields:

- Name:** A text input field with the placeholder 'Enter Name'.
- Select Networks:** A dropdown menu with the placeholder 'Select Networks'.
- Assigned Type:** A dropdown menu with the placeholder 'None'.

At the bottom right, there are 'Cancel' and 'Apply' buttons.

**Name:** Enter a specific name for identification and select a Network from the dropdown button.

**Assigned Type:** Choose assigned type from the dropdown button. Options are DHCPv6, SLAAC + Stateless DHCP and SLAAC + RDNS.

IPV6 Configuration / Network / Ipv6

Network Devices

Show 10 entries Search:

Name	Type	Action
No data available in table		

Showing 0 to 0 of 0 entries Previous Next

To add IPv6 to any Device click on Add

**Network** ✕

**IPv6**

Name

Rule Type  By Group  By Name

Assigned Type

**Name:** Enter a specific name for identification

**Rule Type:** Choose any option and select device or device group to which you want to add IPv6.

**Assigned Type:** Choose assigned type from the dropdown button. Options are DHCPv6, SLAAC + Stateless DHCP and SLAAC + RDNS.

### Assigned Type

**DHCPv6:** DHCPv6 (Dynamic Host Configuration Protocol for IPv6) automates IPv6 address and network configuration for devices. It provides IPv6 addresses, network parameters, and security features, facilitating efficient network management. DHCPv6 operates in stateful (assigns unique IPv6 addresses) and stateless (provides configuration details without assigning specific addresses) modes, catering to diverse network needs. It also supports prefix delegation for router address assignment. Relay agents assist in DHCPv6 message forwarding, and security mechanisms ensure data integrity and authenticity. Overall, DHCPv6 streamlines IPv6 network setup and administration.

**IPv6 address:** IPv6 addresses are represented as a sequence of 128 bits, typically written in hexadecimal format and separated into eight groups of 16 bits each, separated by colons. This is known as the colon-hexadecimal format. Here's a general representation of the IPv6 address format:

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Each "x" represents a hexadecimal digit (0-9, A-F). For example, an IPv6 address might look like this:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

**Prefix:** Prefix refers to an IPv6 address prefix, especially in DHCPv6. DHCPv6 uses prefix delegation to assign blocks of IPv6 addresses to routers, enabling efficient address management within networks. Routers request prefixes from DHCPv6 servers, which then delegate them for address assignment within the network.

Set the Prefix at 64

**DHCP Range:** The DHCP range, also known as the DHCP address pool, refers to a specific range of IP addresses that a DHCP (Dynamic Host Configuration Protocol) server is configured to assign to devices on a network. When a device connects to the network and requests an IP address using DHCP, the DHCP server selects an available IP address from the DHCP range and assigns it to the device for a specified lease duration.

For example, a typical DHCP range might be defined as:

Starting IP address: 192.168.1.100

Ending IP address: 192.168.1.200

**Lease Time:** Lease time in DHCP refers to the duration an IP address is temporarily assigned to a device. It's like a 'rental period' for IP addresses, during which the device can use the assigned IP. When the lease time elapses, the device can either renew the lease to keep the same IP or request a new one. The lease time is a crucial aspect of IP address management, allowing flexibility and efficient use of IP addresses in dynamic network environments.

**DNS Address:** A DNS (Domain Name System) address, often referred to as a DNS server address, is the network address of a server that hosts a DNS service. The DNS system translates user-friendly domain names (e.g., [www.example.com](http://www.example.com)) into IP addresses (e.g., 192.168.1.1) that computers and network devices use to communicate over the internet. There are two types of DNS addresses:

**Primary DNS Server Address:** The address of the primary DNS server that the device will use to resolve domain names into IP addresses. This server is the first choice for DNS resolution.

**Secondary DNS Server Address:** An alternative DNS server address that the device will use if the primary DNS server is unavailable or does not respond. Having a secondary DNS server provides redundancy and ensures continued DNS resolution even if the primary server is down.

Here you can choose either Auto or Manual DNS. If you choose Manual DNS then you have to put the address manually.

**Assigned Type:-**

**SLAAC + Stateless DHCP:** SLAAC (Stateless Address Autoconfiguration) and Stateless DHCP (Dynamic Host Configuration Protocol) are used in combination to achieve comprehensive network configuration in IPv6 environments. This hybrid approach combines the benefits of both SLAAC and Stateless DHCP, providing devices with not only IPv6 addresses but also additional network configuration parameters. Here's how SLAAC and Stateless DHCP can work together:

**SLAAC for Address Assignment:**

Devices use SLAAC to autonomously generate IPv6 addresses based on the network prefix advertised by IPv6 routers via Router Advertisement (RA) messages. The interface identifier part of the address is typically derived from the device's MAC address.

**Stateless DHCP for Additional Configuration Parameters:**

While SLAAC handles address assignment, Stateless DHCP can be used to provide additional network configuration parameters such as DNS server addresses, domain names, NTP (Network Time Protocol) servers, and other relevant details.

Note: For rest of the fields refer to page no. 52 and 53.

**Network**

**IPv6**

Name: Enter Name

Rule Type:  By Group  By Name

Assigned Type: Select Groups (dropdown menu)

Assigned Type: SLAAC+RDNS (dropdown menu)

Address Prefix: Enter Address Prefix

Address Prefix Range: 64

DNS Address:  Auto  Manual DNS

Primary DNS: Enter Primary DNS

Secondary DNS: Enter Secondary DNS

Cancel Apply

**Assigned Type:-**

**SLAAC + RDNS:** When a device uses SLAAC to configure its IPv6 address, it generates the interface identifier portion of the address (usually based on its MAC address).

An organization can set up their DNS servers to automatically create reverse DNS records (PTR records) mapping these IPv6 addresses to corresponding hostnames.

This allows for efficient reverse lookups where given an IPv6 address, you can determine the associated hostname

**SLAAC:**

Devices use SLAAC to autonomously generate IPv6 addresses based on the network prefix advertised by IPv6 routers via Router Advertisement (RA) messages. The interface identifier part of the address is typically derived from the device's MAC address.

**RDNS:**

RDNS is the process of converting an IP address back into a domain name, providing a way to look up the domain associated with an IP address. It's a crucial part of network infrastructure, often used for troubleshooting, logging, and security purposes. RDNS helps identify the hostnames corresponding to IP addresses.

Note: For rest of the fields refer to page no. 52 and 53.

# Network - IPv4

Configuration → Networks → IPv4 → Add

Pv4 is a connectionless protocol, and operates on a best-effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

### Network

#### Ipv4

Name

Rule Type  By Group  By Name

#### LAN IPV4

IP Address

IP Netmask

Dns (Optional)

#### DHCPV4 Server

DHCP Server  Enable  Disable

DHCP Pool Start  Limit

Fill the details and click on Apply button

PV4 Configuration / Network / IPV4

how  entries [Add](#)

Search:

Name	Rule Type	Action
123vipul12342312	By Name	<input type="button" value="View"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 to 1 of 1 entries Previous **1** Next



Click to view the settings.



Click to edit the settings.



Click to delete the settings.

# Network - WAN

Configuration → Network → WAN → IPv6

The screenshot shows the WAN IPv6 configuration page. At the top, there are tabs for IPv4 and IPv6, with IPv6 selected. Below the tabs, there is a search bar and an 'Add New' button. A table displays one entry with the following details:

Name	Type	Action
12345	By Group	

Below the table, it says 'Showing 1 to 1 of 1 entries'. There are also 'Previous' and 'Next' navigation buttons.

The screenshot shows the configuration form for IPv6. It has two main sections: 'Ipv6' and 'WAN 1'.

**Ipv6 Section:**

- Name:
- Rule Type:  By Group  By Name
- 

**WAN 1 Section:**

- Get IPv6 Address:  Auto  DHCPv6  SLAAC+Stateless DHCP
- Prefix Delegation:  Auto  Custom  Disable
- Dns Address:  Get Dynamically From ISP  Use the following address

At the bottom right, there are 'Cancel' and 'Apply' buttons.

**Name:** Enter a specific name for identification.

**Rule type:** Select either By Group or By Name. And choose Device group if you selected rule type as By Group or Device name if you selected rule type as By Name.




Note: For rest of the fields refer to page no. 52 and 53.

Configuration → Network → WAN → IPv4

WAN Configuration / Network / WAN

IPv4 IPv6

Show 10 entries Search:

Name	Rule Type	Action
anjali12	By Group	  

Showing 1 to 1 of 1 entries Previous 1 Next

Networks

Ipv4

Name: anjali12

Rule Type:  By Group  By Name

anjaliGrp

WAN 1

Connection Type: Static IP

VLAN:

IP Address: 192.168.5.179

Netmask: 255.255.255.0

Gateway: 192.168.5.10

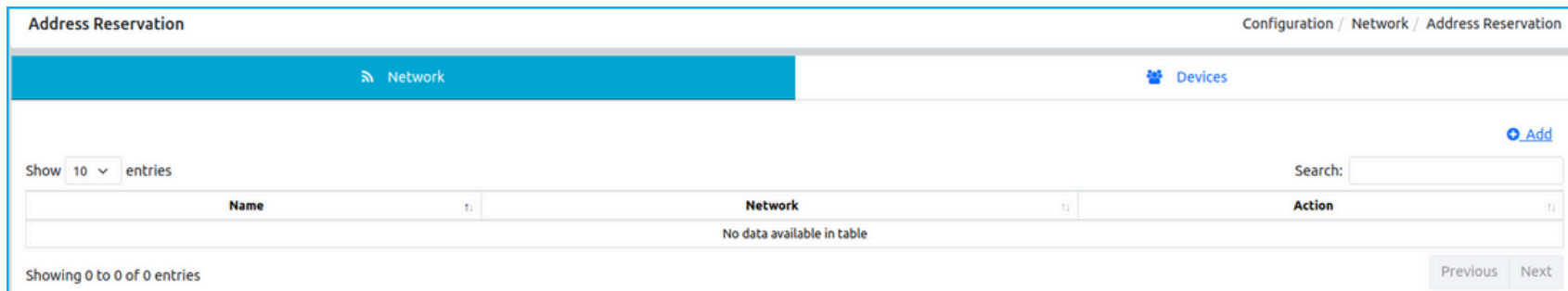
Primary Dns (Optional): N/A

Secondary Dns (Optional): N/A

Cancel Apply

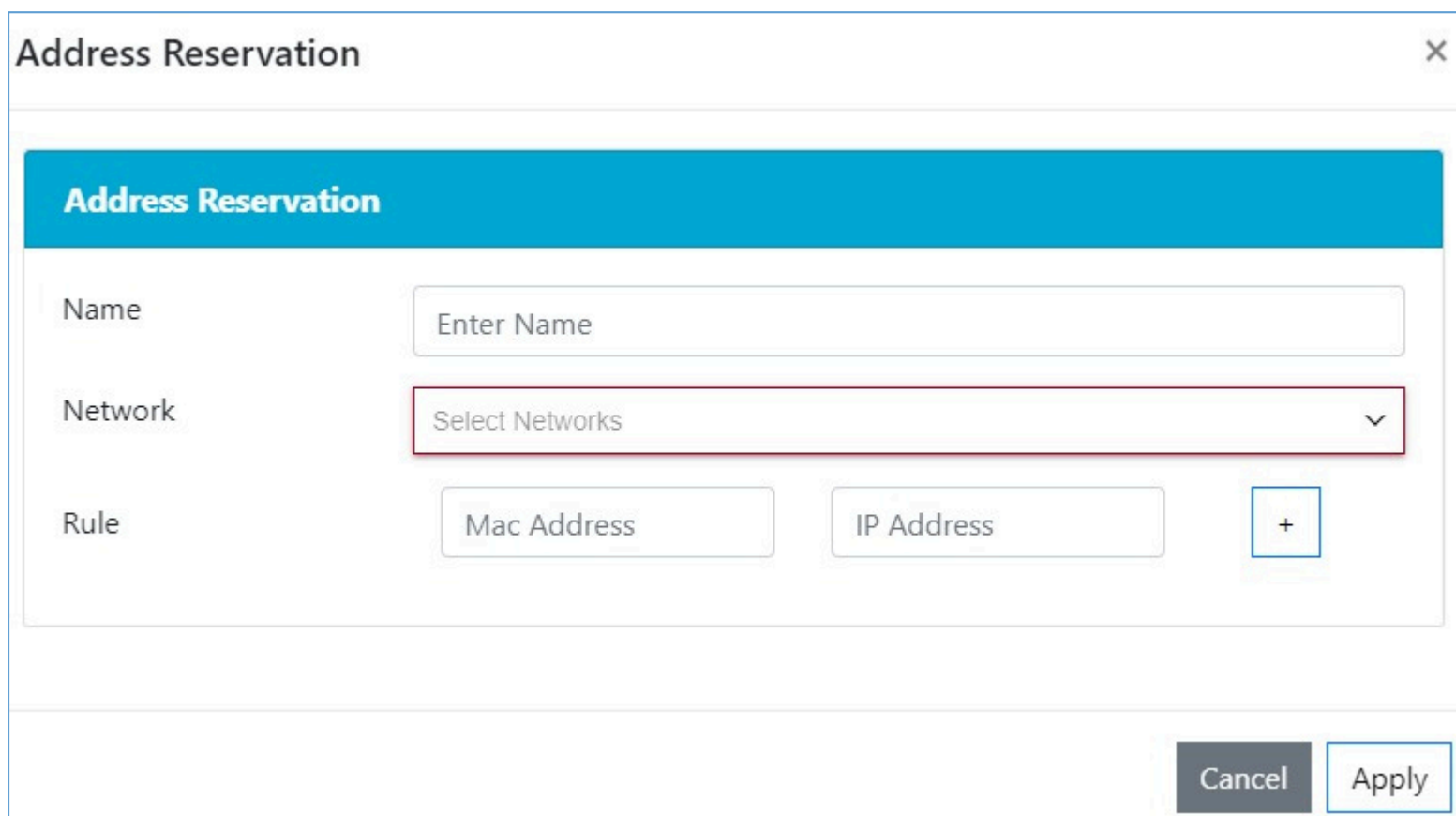
## Network - Address Reservation

Configuration → Network → Address Reservation → Network



The screenshot shows the 'Address Reservation' configuration page. At the top, there is a breadcrumb trail: 'Configuration / Network / Address Reservation'. Below this, there are two tabs: 'Network' (selected) and 'Devices'. A search bar is located on the right side. The main content area contains a table with the following columns: 'Name', 'Network', and 'Action'. The table is currently empty, with the message 'No data available in table' displayed. At the bottom of the table, it says 'Showing 0 to 0 of 0 entries'. There are 'Previous' and 'Next' navigation buttons at the bottom right.

**Address Reservation:** Address reservation, also known as DHCP reservation, is a feature in DHCP (Dynamic Host Configuration Protocol) where the DHCP server allocates a specific IP address to a device based on its MAC (Media Access Control) address. This ensures that the device consistently receives the same IP address whenever it connects to the network.



The screenshot shows the 'Address Reservation' configuration dialog box. It has a title bar with 'Address Reservation' and a close button (X). The dialog is divided into three sections: 'Name', 'Network', and 'Rule'. The 'Name' section has a text input field with the placeholder 'Enter Name'. The 'Network' section has a dropdown menu with the placeholder 'Select Networks'. The 'Rule' section has two text input fields: 'Mac Address' and 'IP Address', followed by a plus sign (+) button. At the bottom right of the dialog, there are 'Cancel' and 'Apply' buttons.

**Name:** Enter a specific name for identification.

**Network:** Select network from the dropdown button.

**Rule:** Input your MAC Address and IP Address. Here you can input multiple MAC and IP Addresses by clicking on



Configuration → Network → Address Reservation → Devices

The screenshot shows the 'Address Reservation' configuration page. At the top, there is a breadcrumb trail: Configuration / Network / Address Reservation. Below this, there are two tabs: 'Network' (selected) and 'Devices'. The main content area features a table with the following columns: Name, Rule Type, and Action. The 'Name' column contains a single entry with a grid icon. The 'Rule Type' column shows 'By Group'. The 'Action' column contains three icons: a green eye, a pencil, and a red trash can. Above the table, there is a search bar and a '+ Add' button. Below the table, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' navigation buttons.

Name	Rule Type	Action
	By Group	

The screenshot shows the 'Address Reservation' configuration form. It has a title bar 'Address Reservation' with a close button. The form is divided into several sections: 'Name' with a text input field containing 'Enter Name'; 'Rule Type' with two radio buttons, 'By Group' (selected) and 'By Name'; 'Devices' with a dropdown menu showing 'Select Groups'; and 'Rule' with two text input fields, 'Mac Address' and 'IP Address', and a '+' button to add more rules. At the bottom right, there are 'Cancel' and 'Apply' buttons.

**Name:** Enter a specific name for identification.

**Rule Type:** Set Rule type as per your requirement.




**Devices:** Select device group if you set the rule type as By Group or device name if you set the rule type as By Name from the dropdown button.

**Rule:** Input your MAC Address and IP Address. Here you can input multiple MAC and IP Addresses by clicking on

# Network - VLAN

Configuration → Network → VLAN

The screenshot shows a web interface for VLAN configuration. At the top, there is a breadcrumb trail: Configuration / Network / VLAN. Below this, there is a search bar and an 'Add' button. A table displays the current VLAN configuration. The table has four columns: Name, Type, device & id, and Action. The first row contains the following data: Name: ambuj1, Type: By Name, device & id: LAN2 & 27, and Action: (represented by three icons: a green eye, a pencil, and a red trash can). Below the table, it says 'Showing 1 to 1 of 1 entries'. On the right side, there are navigation buttons: 'Previous', '1', and 'Next'.

Name	Type	device & id	Action
ambuj1	By Name	LAN2 & 27	  

VLANs allow you to segment a network into smaller, virtual sub-networks, which can be used to isolate traffic and improve network performance. VLANs are often used in enterprise networks to separate different departments or groups, or to segment different types of traffic (such as voice, data, and video).

The screenshot shows the 'VLAN' configuration form. It is divided into several sections. The first section is 'VLAN' and contains the following fields: 'Name' (text input with placeholder 'Enter Name'), 'Rule Type' (radio buttons for 'By Group' (selected) and 'By Name'), 'Interface' (dropdown menu with placeholder 'Select Groups'), and 'VLAN ID' (text input with placeholder '1-4096'). The second section is 'Assign IP Address' and contains: 'Assign IP Address' (radio buttons for 'Enable' (selected) and 'Disable'), 'IP Address' (text input with placeholder 'X . X . X . X'), 'NetMask' (text input with placeholder 'X . X . X . X'), and 'Subnet-Type' (dropdown menu with 'None' selected). The third section is 'Enable DHCP Server' and contains: 'DHCP Server' (radio buttons for 'Enable' (selected) and 'Disable') and 'IP Address Pool' (text input with 'start' and 'limit' separated by a hyphen). At the bottom right, there are 'Cancel' and 'Apply' buttons.

# Network - Port Setup

Configuration → Network → Port Setup

Name	Rule Type	Action
530	By Name	
admin	By Name	
kro	By Name	

By default KRO-110-D4G device has five port which can be switch LAN to WAN or WAN to LAN. Here you can do the same in Port Setup.

Port Number	Name	Mode	Service Type
1	LAN/WAN		
2	LAN/WAN		
3	LAN/WAN		
4	LAN/WAN		
5	LAN/WAN		

Here you can set the mode of port whether it is on or off and also can set the service type of LAN and WAN by clicking on the buttons.

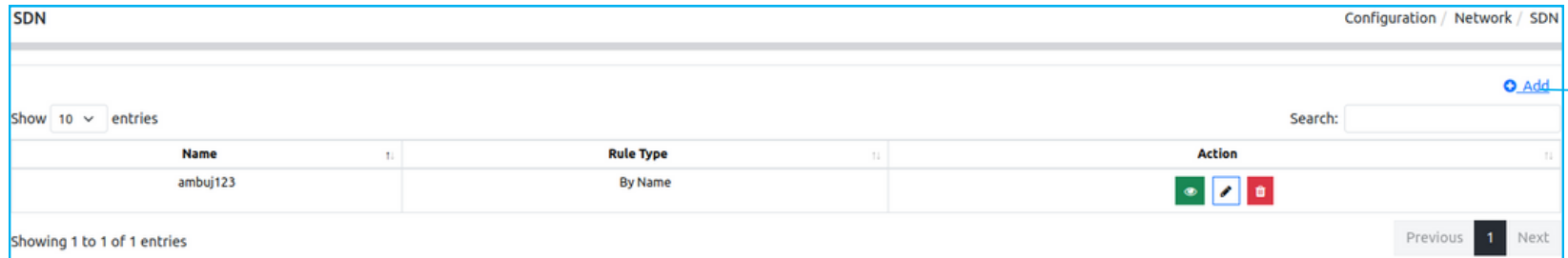
Configuration → Network → Port Setup → Add

The screenshot shows a web interface for "Port Setup Configuration". At the top right, there is a breadcrumb trail: "Network / Port Setup / Port Setup Configuration". Below this is a blue header bar labeled "Basic Configuration". Underneath, there are two main sections: "Name" with a text input field containing "Enter Name", and "Rule Type" with two radio buttons: "By Group" (which is selected) and "By Name". Below the radio buttons is a dropdown menu with the text "Select Groups" and a downward arrow. At the bottom of the form, there is a table with four columns: "Port Number", "Name", "Mode", and "Service Type". Below the table is a light blue bar with a button labeled "Add" with a plus icon.

Here you can add Device Group or Device in which you want to apply port setup feature by simply choosing from the dropdown button. Select Device Group or Device name and click on Add.




# Network - SDN

Configuration → Network → SDN



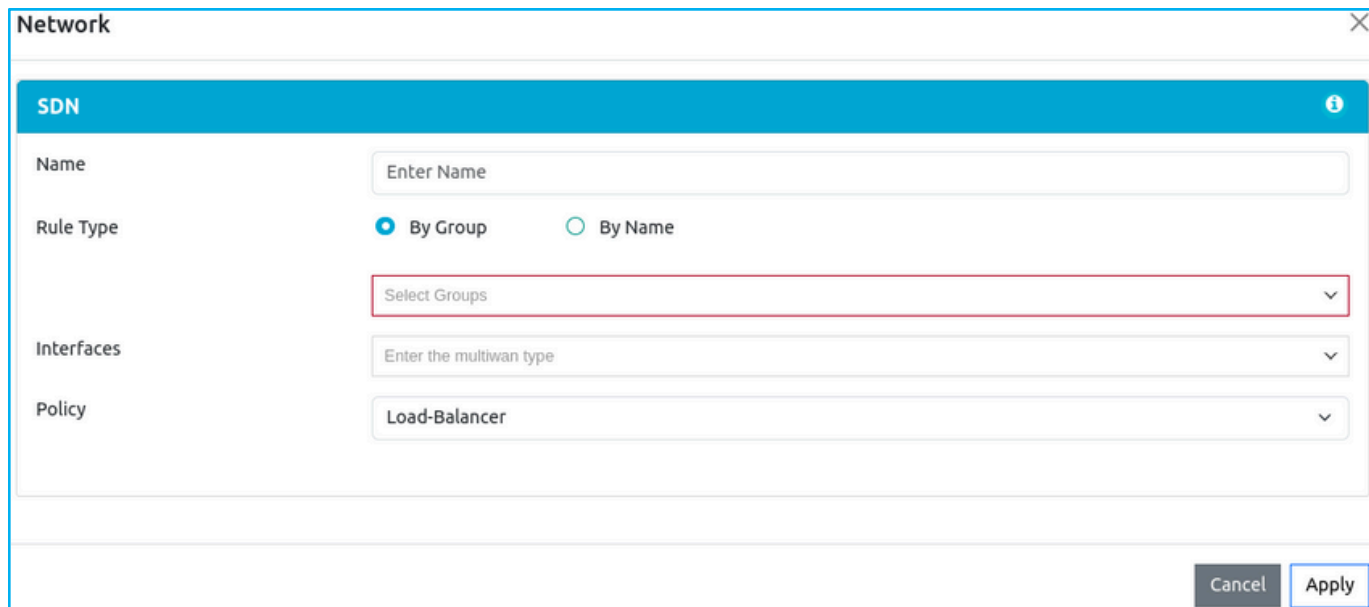
SDN Configuration / Network / SDN

Show 10 entries Search:

Name	Rule Type	Action
ambuj123	By Name	  

Showing 1 to 1 of 1 entries Previous 1 Next

Software-defined networking (SDN) is an architecture that makes networks more flexible and easier to manage by separating the data forwarding function from the control plane in individual networking devices.



Network

**SDN**

Name

Rule Type  By Group  By Name

Interfaces

Policy

**Network** ✕

---

**SDN** i

Name

Rule Type  By Group  By Name

✕ ▾

Interfaces  ✕ ▾

Policy  ▾

	Metric	Weight
<input type="text" value="WAN1"/>	<input type="text" value="2"/>	<input type="text" value="2"/>

# VPN - PPTP

---

Configuration → VPN → PPTP

PPTP (Point-to-Point Tunneling Protocol) is a networking protocol that was commonly used to establish virtual private network (VPN) connections over the internet or other untrusted networks. It's important to note that PPTP has some security vulnerabilities, and it's generally considered less secure than more modern VPN protocols like L2TP/IPsec, OpenVPN, or IKEv2/IPsec.




## Some key points about PPTP:

**Security:** VPNs provide a secure and encrypted connection, ensuring that data transmitted between the remote location and the cloud infrastructure is protected from unauthorized access.

**Access Control:** VPNs enable organizations to control who has access to their cloud resources, ensuring that only authorized users or networks can connect.

**Privacy:** VPNs help maintain the privacy of data as it traverses public networks, making it difficult for eavesdroppers to intercept sensitive information.

**Connectivity:** VPNs enable seamless and secure connectivity to cloud resources, regardless of the physical location of the user or network.

Name	Rule Type	Action
ambujdwđwq	By Name	  

Configuration → VPN → PPTP → New

The screenshot shows a configuration window titled "VPN" with a close button in the top right corner. Below the title bar is a blue header with the text "PPTP" and an information icon. The main area contains the following fields:

- Name:** A text input field with the placeholder text "Enter Name".
- Rule Type:** Two radio buttons: "By Group" (selected) and "By Name".
- Select Groups:** A dropdown menu with the text "Select Groups" and a downward arrow.
- Tunnel IP:** A text input field with the placeholder text "xxx.xxx.xxx.xxx".
- Client IP Range:** Two text input fields. The first is labeled "X.X.X.X" and contains "0". The second is labeled "X.X.X.X" and contains "255".

At the bottom right of the window are two buttons: "Cancel" and "Apply".

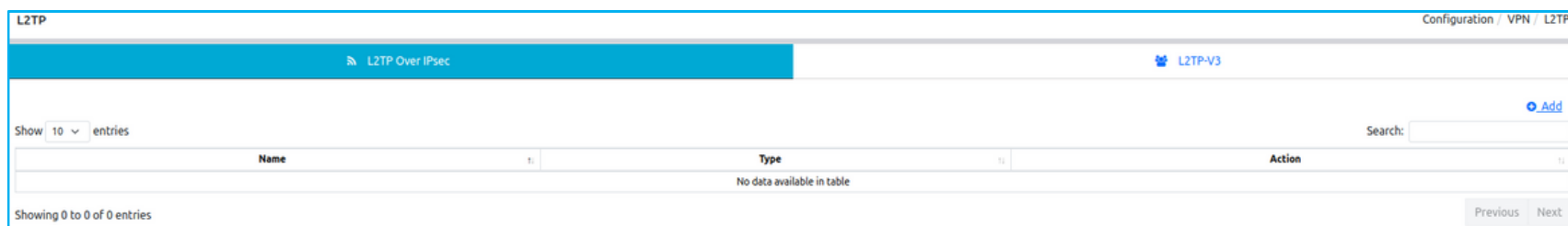
Tunnel IP: It is an encrypted connection between a device and a VPN server that hides a user's IP address and encrypts their data.

Client IP Range: The client IP range refers to the range of IP addresses that the VPN server assigns to connected clients when they establish a VPN connection. When you connects to the PPTP VPN server, The server assigns an IP address from the specified client IP range to you. This IP address is used for the duration of the VPN session.

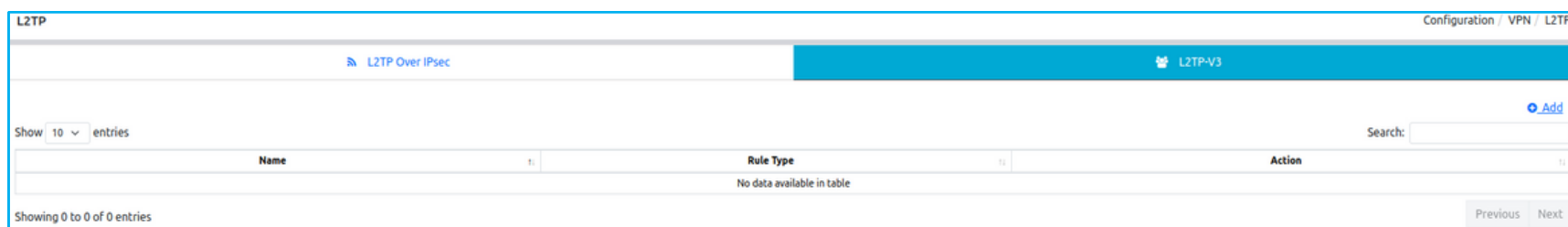
## VPN - L2TP

Configuration → VPN → L2tp

L2TP (Layer 2 Tunneling Protocol) is a networking protocol used for creating secure virtual private network (VPN) connections. It's often combined with IPsec for added security. L2TP is known for its compatibility, support for various operating systems, and flexibility in traversing different network configurations. It's commonly used in remote access, site-to-site, and mobile VPN scenarios. However, its security relies on the additional use of IPsec, and more modern VPN protocols are often preferred for their enhanced security features.



**L2TP/IPsec:** L2TP/IPsec, or Layer 2 Tunneling Protocol over Internet Protocol Security, is a combination of two networking protocols used to establish secure virtual private network (VPN) connections. This combination provides a higher level of security compared to using L2TP or IPsec individually.



**L2TPv3:** L2TPv3 (Layer Two Tunneling Protocol Version 3) is a point-to-point layer two over IP tunnel. This means you can tunnel L2 protocols like Ethernet, Frame-relay, ATM, HDLC, PPP, etc. over an IP network. This can be pretty useful...For example, let's say you have two remote sites and an application that requires that hosts are on the same subnet. With L2TPv3, it's no problem to "bridge" two remote sites together, putting them in the same broadcast domain/subnet.

Configuration → VPN → L2tp → Add

VPN

**L2tp**

Type  Server  Client

Name

Rule Type  By Group  By Name

Auth

Pre-Shared-Key

NAT  Enable

Tunnel IP

Client IP Range ⓘ X.X.X.X  X.X.X.X

Cancel Apply

VPN

**L2tp**

Type  Server  Client

Name

Rule Type  By Group  By Name

Auth

Pre-Shared-Key

NAT  Enable

Server IP

Username

Password

Cancel Apply

**Auth:** Authentically refers to the authentication mechanism used to verify the identity of users or devices attempting to establish a VPN (Virtual Private Network) connection. L2TP is often used in conjunction with other authentication protocols to secure VPN connections. The four authentication methods used with L2TP are: PAP, CHAP, MS-CHAP and MS-CHAPv2

**PAP (Password Authentication Protocol):** PAP is a simple authentication protocol that requires the client (the device or user trying to connect to the VPN) to send a username and password to the server (the VPN endpoint) in plain text. The server then compares the provided credentials with its database to authenticate the client. PAP is considered less secure because it transmits passwords in plain text, making it vulnerable to eavesdropping.

**CHAP (Challenge Handshake Authentication Protocol):** CHAP is a more secure authentication method used with L2TP. It involves a challenge-response mechanism where the server sends a random challenge to the client. The client then uses a one-way hash function to combine the challenge and its password, sending the result back to the server for verification. Since the password is never sent in plain text, CHAP provides a higher level of security compared to PAP.

**MS-CHAP:** MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) is a widely used authentication protocol in the context of VPN connections and remote access authentication. It is developed by Microsoft and is an extension of the standard CHAP (Challenge Handshake Authentication Protocol). MS-CHAP enhances CHAP with additional security features and compatibility with Microsoft Windows-based systems.

**MS-CHAPv2:** MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) is also an authentication protocol used primarily in VPN and remote access scenarios. It was also developed by Microsoft to address security concerns and improve upon the earlier version, MS-CHAPv1. MS-CHAPv2 is designed to provide stronger security and protection against certain vulnerabilities.

**Pre-Shared Key:** A pre-shared key (PSK) is a shared secret phrase or string of characters used to authenticate and secure the VPN connection. The PSK is known to both the client and the VPN server, allowing them to establish a secure communication channel.

**NAT:** NAT is a technique used to map private IP addresses to a single public IP address, typically used in routers and firewalls to allow multiple devices within a local network to share a single public IP address when accessing resources on the internet.

**NAT for L2TP Servers:** In some cases, L2TP servers may be behind a NAT device, such as a router or firewall. This scenario is common when you have a private network with L2TP VPN servers, and you want to allow remote clients to connect to them from the internet. The NAT device maps the public IP address and port number to the internal private IP address of the L2TP server.

Configuration → VPN → L2tpv3 → Add New

The screenshot shows the 'L2TP-V3' configuration window. It includes a title bar with 'L2TP' and a close button. The main content area has a blue header 'L2TP-V3'. Below this, there are several configuration fields: 'Name' (text input with placeholder 'Enter Name'), 'Remote Wan-IP' (text input with placeholder 'Enter Remote Wan-IP'), 'Rule Type' (radio buttons for 'By Group' (selected) and 'By Name'), a dropdown menu for 'Select Groups', 'Tunnel-IP' (text input), 'CIDR' (text input), 'Tunnel-ID' (text input), 'Remote Tunnel-ID' (text input), 'Session-ID' (text input with placeholder 'xxx.xxx.xxx.xxx'), and 'Remote Session-ID' (text input with placeholder 'xxx.xxx.xxx.xxx'). At the bottom right are 'Cancel' and 'ADD Server' buttons.

**Remote Wan-IP:** You need to configure the WAN IP address of remote router or device that is going to establish the L2TPv3 tunnel. This IP address is used to identify the endpoint of the tunnel.

**Tunnel-IP:** In L2TPv3 tunnels, each endpoint of the tunnel is identified by its own tunnel IP address. L2TPv3 is used to transport Layer 2 frames over an IP network. Example: Tunnel IP at Local Endpoint: 192.168.1.1

**CIDR:** CIDR (Classless Inter-Domain Routing) is a method for representing IP addresses and network prefixes. It uses a notation that includes an IP address followed by a forward slash and a number (e.g., 192.168.1.0/24). This number indicates the length of the network prefix, allowing for more flexible and efficient allocation of IP address blocks compared to the older classful IP addressing scheme. CIDR is widely used in networking for specifying network addresses and routing policies.

**Tunnel-ID and Remote Tunnel-ID:** In L2TPv3 (Layer 2 Tunneling Protocol Version 3), tunnel IDs are used to uniquely identify and manage virtual tunnels. Each L2TPv3 tunnel has both a local and remote tunnel ID. These IDs are configured during tunnel setup and negotiation, ensuring that data frames are properly routed through the tunnel. Tunnel IDs play a crucial role in differentiating and directing traffic within L2TPv3 tunnels, especially in networks with multiple tunnels.

Note: The ID must be unique.

**Session ID:** A Session ID is a unique identifier used to distinguish and manage individual data sessions. It ensures that data frames are correctly routed to the appropriate session within the tunnel, allowing multiple sessions to share the same tunnel without interference. Session IDs are assigned during session setup and negotiation between the local and remote endpoints and play a key role in multiplexing data sessions.

**Remote Session ID:** In L2TPv3 (Layer 2 Tunneling Protocol Version 3), the "remote session ID" refers to the session identifier assigned to the remote end of an individual data session. The remote session ID is used in conjunction with the local session ID to uniquely identify and manage data sessions within the tunnel.

# VPN - GRE

Configuration → VPN → GRE

**GRE:** GRE (Generic Routing Encapsulation) is used to create a point-to-point or site-to-site virtual network connection over an existing network, typically the internet. GRE itself does not provide encryption or security features, so it is often used in conjunction with other protocols such as IPsec (Internet Protocol Security) to create secure VPN connections.

Name	Rule Type	Action
No data available in table		

**GRE**

Name: Enter Name

Rule Type:  By Group  By Name

Select Groups: [Dropdown]

Protocol: GRE Over IPv4 [Dropdown]

Remote IP: [Text Input]

Tunnel IP Type:  IPV4  IPV6

Tunnel IP: xxx.xxx.xxx.xxx

Netmask: 32

Cancel Apply

#### GRE over IPv4

- The original IP packet is encapsulated by adding a GRE header followed by a new IPv4 header.
- The GRE header contains control information and protocol type.
- The new IPv4 header has the source and destination addresses of the GRE tunnel endpoints.
- The encapsulated packet is then transmitted over the IPv4 network.
- At the receiving end, the GRE and new IPv4 headers are removed, leaving the original IP packet, which is then forwarded to its final destination based on the original IP header.
- GRE doesn't provide encryption or security, often requiring additional security protocols like IPsec for secure communication.

#### GRE over IPv6

GRE can be used over IPv6 to create private point-to-point connections. The process is similar to GRE over IPv4, but encapsulation occurs within IPv6 packets. The original IP packet is encapsulated with a GRE header and a new IPv6 header. The GRE header contains control information, and the new IPv6 header has the source and destination IPv6 addresses of the tunnel endpoints. The encapsulated packet is transmitted over the IPv6 network and, upon reaching the endpoint, is decapsulated for further processing. As with GRE over IPv4, GRE over IPv6 doesn't provide encryption or security, often requiring additional security protocols like IPsec for secure communication.

#### GRE Tap over IPv4

When utilizing GRE (Generic Routing Encapsulation) over IPv4, you can create a virtual point-to-point network interface, commonly referred to as a "GRE tap," that allows for encapsulation and tunneling of various network protocols. This setup enables the creation of private communication channels over a public IPv4 network.

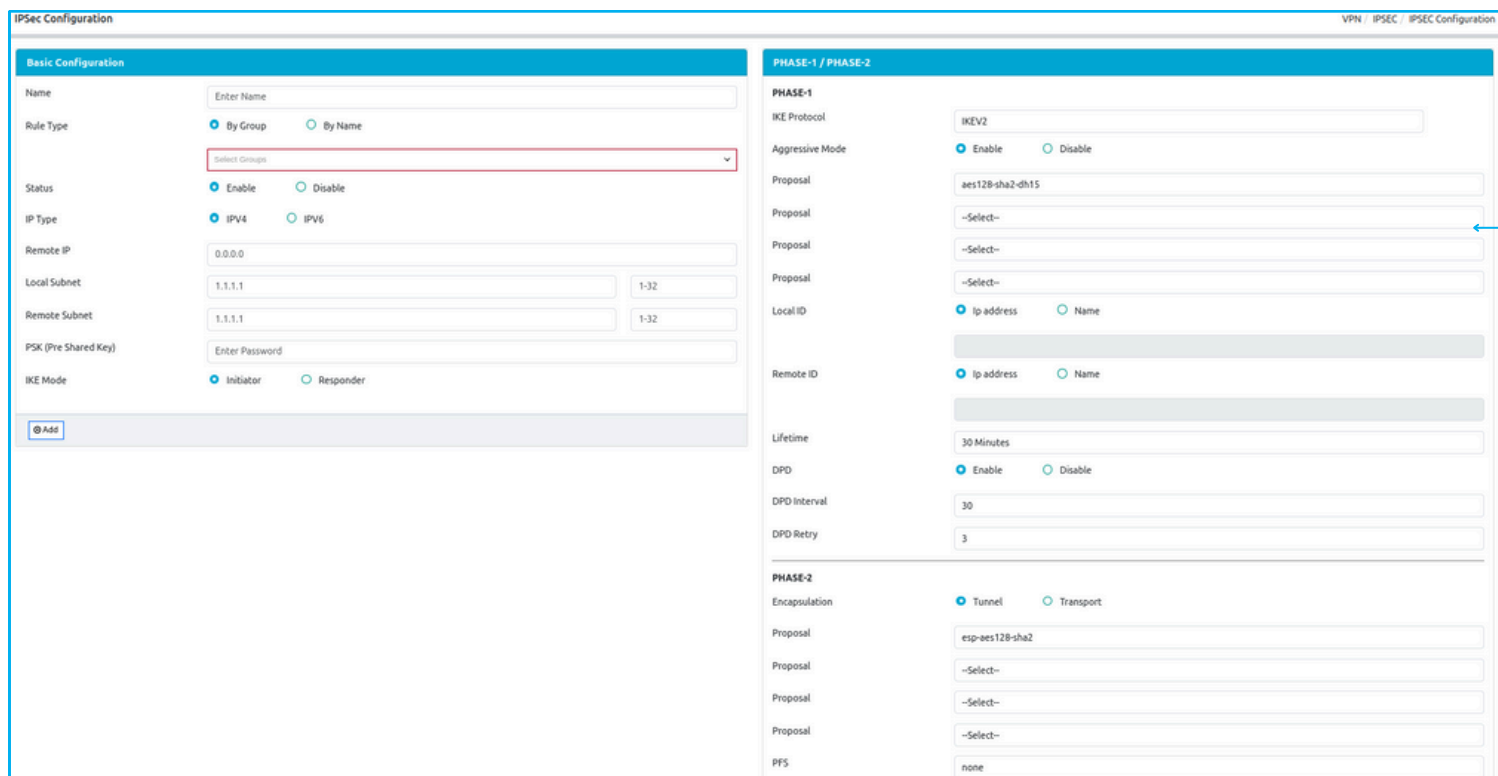
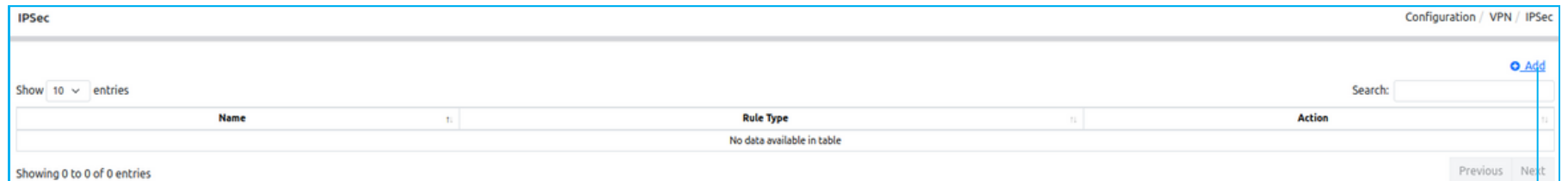
#### GRE Tap over IPv6

"GRE tap over IPv6" refers to the usage of Generic Routing Encapsulation (GRE) to create a virtual point-to-point network interface, often referred to as a "GRE tap," over an IPv6 network. This allows for the encapsulation and tunneling of various network protocols within IPv6 packets, enabling private communication channels over a public IPv6 network.

# VPN - IPSec

Configuration → VPN → IPSec

IPsec (Internet Protocol Security) is a suite of protocols and standards that provide security services for communication at the network layer of the OSI model. It's widely used to secure communication over IP networks, including the internet. IPsec operates by encrypting and authenticating data to ensure confidentiality, integrity, and authenticity. IPsec provides a robust framework for securing data communication, making it a fundamental tool for network security in the modern digital landscape.



**IKE(Internet Key Exchange):** IKE establishes a secure, authenticated communication channel between two parties. IKE negotiates security associations (SAs), which are a set of mutually agreed-upon keys and algorithms used by both parties trying to establish a VPN connection. Here you can select proposals from the drop down. You can select upto four proposals at a time

**DPD(Dead Peer Detection):** Dead Peer Detection (DPD) is a method that network devices use to detect the availability of peer devices. It uses IPsec traffic patterns to reduce the number of messages needed to confirm a peer's availability.



**DPD Intervals:** The Dead Peer Detection (DPD) interval for IPsec is 30 seconds by default. This means that the router Device will send DPD packets every 30 seconds when there is no traffic over the IPsec tunnel. If the peer doesn't respond the device will then disconnect the IPsec tunnel.

**PFS:** Perfect Forward Secrecy (PFS) prevents third parties from discovering a key value.

# VPN - OpenVpn

Configuration → VPN → OpenVpn

OpenVPN is an open-source Virtual Private Network (VPN) software that allows for secure point-to-point or site-to-site connections. It provides a secure tunnel for data transmission over an insecure network, typically the internet. OpenVPN is known for its robustness, security, and flexibility, making it a popular choice for creating secure VPN connections.

OpenVpn			Configuration / VPN / OpenVpn		
Name	OpenVpn Type	Action			
vipul	server	 			

Showing 1 to 1 of 1 entries

### Openvpn Config

Type  Server  Client

Name

Device

Service Port

Service IP

Service Netmask

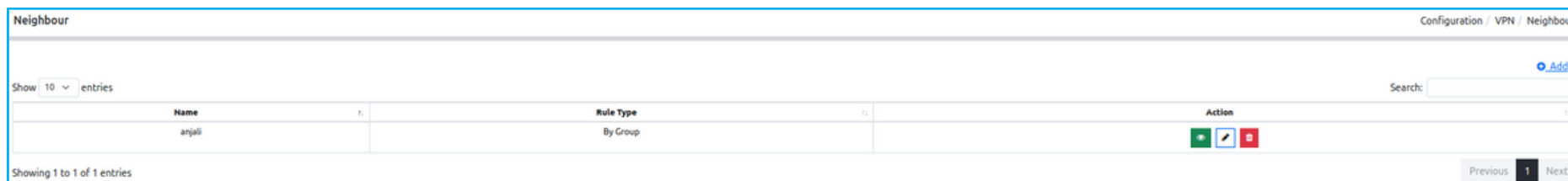
Service Protocol  TCP  UDP

Service Type  TUN  TAP




# VPN - Neighbour

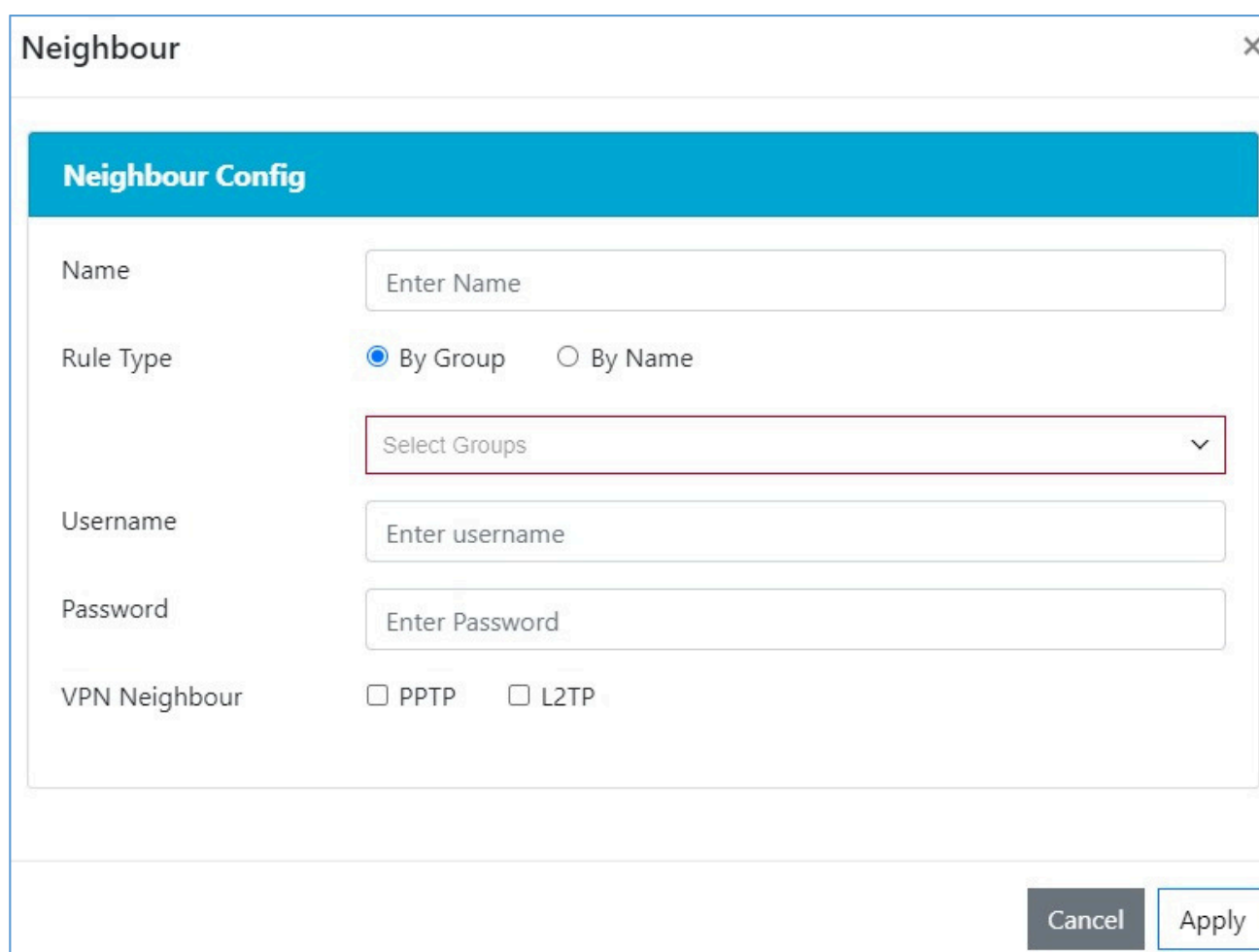
Configuration → VPN → Neighbor

The Neighbor is a remote network or device that connects to the PPTP server/ L2TP server. using a username and a password for authentication. The PPTP Neighbor is essentially a user or client trying to establish a secure tunnel to the PPTP server/ L2TP server, and their username and password are used to Authenticate and gain access to the VPN.



The screenshot shows a web interface for configuring VPN neighbors. At the top right, the breadcrumb is "Configuration / VPN / Neighbour". Below the breadcrumb, there is a search bar and an "Add" button. A table displays the current configuration for a neighbor named "anjali". The table has three columns: "Name", "Rule Type", and "Action". The "Name" column contains "anjali", the "Rule Type" column contains "By Group", and the "Action" column contains three icons: a green plus sign, a blue pencil, and a red minus sign. Below the table, it says "Showing 1 to 1 of 1 entries".

Name	Rule Type	Action
anjali	By Group	  



The screenshot shows a "Neighbour Config" dialog box. It has a blue header with the text "Neighbour Config". Below the header, there are several fields and options:

- Name:** A text input field with the placeholder text "Enter Name".
- Rule Type:** Two radio buttons: "By Group" (selected) and "By Name".
- Select Groups:** A dropdown menu with the placeholder text "Select Groups" and a downward arrow.
- Username:** A text input field with the placeholder text "Enter username".
- Password:** A text input field with the placeholder text "Enter Password".
- VPN Neighbour:** Two checkboxes: "PPTP" and "L2TP", both of which are currently unchecked.

At the bottom right of the dialog box, there are two buttons: "Cancel" and "Apply".

VPN Neighbor: If you enable PPTP, you have to use the same username and password that you set in the PPTP VPN. If you enable both PPTP and L2TP, you must use the usernames and passwords that are set for both the PPTP and L2TP VPNs.

# Routing - Static Route

Configuration → Routing → Static Route

A static route in a cloud controller is a manually configured path for network packets to reach a specific destination. It's setup within the cloud controller's networking or network configuration section, involving specifying the destination IP address or network and the next hop (router or gateway). Once configured, the static route directs traffic along the defined path.

Routing			Configuration / Routing / Static Routing
Name	Type	Action	
No data available in table			

Showing 0 to 0 of 0 entries

Search:

[Add](#)

Previous Next

Configuration → Routing → Static Route → Add

The screenshot shows a 'Routing' window with a 'Static Route' tab. The form contains the following fields and options:

- Name:** A text input field with the placeholder 'Enter Name'.
- Rule Type:** Two radio buttons: 'By Group' (selected) and 'By Name'.
- Destination IP:** A text input field with the placeholder 'xxx.xxx.xxx.xxx'.
- Netmask / CIDR:** A dropdown menu with the placeholder 'Select Netmask/CIDR'.
- Gateway:** A text input field with the placeholder 'xxx.xxx.xxx.xxx'.
- Interface:** A dropdown menu.

At the bottom right of the window are 'Cancel' and 'Apply' buttons.

**Destination IP:** The destination IP refers to the specific IP address, IP address range, or subnet that the static route is intended to direct traffic towards. When a packet is being sent to a destination IP address, the static route specifies how that packet should be forwarded to reach that particular IP address or IP range.

**Netmask:** A netmask (or subnet mask) is used to define the network portion of an IP address. It allows for the logical separation of an IP address into a network part and a host part. When configuring a static route, you specify the destination IP address or IP address range and its corresponding netmask. The netmask helps the router or networking device determine which packets should be sent along the static route based on the network portion.

**Gateway:** The gateway in a static route is the IP address of the next device, typically a router or Layer 3 switch, that the traffic is sent to in order to reach the specified destination IP address or subnet. This intermediary device then handles the further routing of the traffic towards the final destination based on the information in its routing table.

# Routing - RIP

Configuration → Routing → RIP

RIP, or Routing Information Protocol, is one of the oldest and most basic distance vector routing protocols used in computer networking. It's designed to help routers dynamically share information about the paths or routes they know about in order to efficiently reach various network destinations. While RIP is a straightforward and easy-to-configure routing protocol, it's generally not the best choice for large or complex networks due to its slow convergence and limitations. More modern protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) are often preferred for larger, more scalable networks.

RIP				Configuration / Routing / RIP
Name	Type	version	Action	
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next



Click to view RIP settings



Click to Edit RIP settings



Click to Delete RIP settings

Configuration → Routing → RIP → Add

The screenshot shows a configuration window titled "RIP" with a close button in the top right corner. Below the title bar is a blue header labeled "General Configuration". The form contains the following fields and controls:

- Name:** A text input field with the placeholder "Enter Name".
- Rule Type:** Two radio buttons: "By Group" (selected) and "By Name".
- Select Groups:** A dropdown menu with a red border and a downward arrow.
- Default Distance:** A text input field with the value "1-15".
- Default Metric:** A text input field with the value "1-255".
- Network:** A text input field with the placeholder "A . B . C . D / M" and a blue "+" button to its right.
- Version:** A text input field with the value "2".
- Interface:** A dropdown menu.
- Advance Configuration:** A checked checkbox.
- Rip Timer:** An unchecked checkbox.
- Updated Timeout:** A range slider set to "5-30".
- Timeout Time:** A range slider set to "5-180".
- Garbage Timeout:** A range slider set to "5-120".
- Rip Authentication:** A checked checkbox.
- Key Identity Number:** A text input field with the placeholder "Key Identity Number".
- Auth Mode:** A dropdown menu with the value "md5".
- Key String:** A text input field with the placeholder "Key string".

At the bottom right of the window are "Cancel" and "Apply" buttons.

**Default Distance:** Routing Information Protocol (RIP), the default administrative distance is 120. Administrative distance (AD) is a metric used by routers to determine the trustworthiness of a routing source. Lower AD values indicate higher trust. when a router receives routing information from multiple sources (e.g., RIP, OSPF, EIGRP), it uses the administrative distance to determine which route to include in its routing table. Lower administrative distances are preferred, so a route with a lower administrative distance will be chosen over one with a higher administrative distance.

**Default Metric:** The default metric used is hop count. The hop count is a simple metric that indicates the number of routers (hops) a packet must traverse to reach a destination network. Each hop represents a router the packet goes through. For RIP, the maximum hop count allowed for a route is 15. If a route has a hop count of 16 or higher, it is considered unreachable (infinity) in RIP terminology.

**Network:** Input IP and Netmask (0.0.0.0/255.255.255.255). Here you can add multiple network by clicking on the "+" button.

**Version:** Two Versions of RIP are here you can choose any one. The above page is showing when you choose version 1. If you choose version 2 the page will extend with some more features.

**More:** Enable the check box of Advance Configuration for further settings of version 1.

**RIP Timer:** Enable the check box of RIP timer to set the Updated Timeout, Timeout Time and Garbage Timeout

**Updated Timeout:** RIPv1 has a simple operation without features like authentication, subnet masks, or updated timeout mechanisms. Updates are sent every 30 seconds regardless of whether there have been changes in the network or not. The "timeout" in RIPv1 refers to the time after which a route is considered invalid if no update is received for that route.

**Timeout Timeout Time:** The "timeout" refers to the time it takes for a route to be considered invalid or expired if no updates are received for that route. There are typically two timeout intervals associated with RIP: the "route timeout" and the "holddown timeout."

**Key Identity Number:** The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed on that interface. Define the key or keys on the key chain and specify the password or key-string to be used in the key.

**AuthMode:** Choose the AuthMode options from the dropdown button. The options are md5 and Text.

**Md5:** Message Digest Algorithm 5 Authentication: This mode uses MD5, a cryptographic hash function, to generate a digest (hash) based on the key string and parts of the RIP packet. The digest is sent along with the RIP packet. This provides a more secure way of authenticating the RIP packets because the key string itself is not transmitted in the clear.

**Text:** In this mode, the key string is sent in plain text along with the RIP packet. It is important to ensure that the key string is kept confidential as it's sent in an unencrypted form.

**Key String:** The "key string" is a shared secret, essentially a password or passphrase, that is configured on the routers participating in RIPv2 authentication. This key string is used to authenticate the routing updates. Both sending and receiving routers must have the same key string configured to authenticate and accept RIPv2 updates.

# Routing - OSPF

Configuration → Routing → OSPF

Name	Type	Action
No data available in table		

Open Shortest Path First (OSPF) is a link-state routing protocol used for finding the shortest path in a network. It maintains detailed network topology information, divides networks into areas for scalability, uses cost metrics to determine optimal paths, employs Hello packets for neighbor relationships, and allows for fast network convergence. OSPF is widely used in large networks due to its efficiency and scalability.


Configuration → Routing → OSPF → Add

The screenshot shows a configuration window titled "OSPF" with a "General Configuration" tab. The fields are as follows:

- Name:** A text input field with the placeholder "Enter Name".
- Rule Type:** Two radio buttons: "By Group" (selected) and "By Name".
- Select Groups:** A dropdown menu with a red border and a downward arrow.
- Router Id:** A text input field with the placeholder "xxx.xxx.xxx.xxx".
- Network:** A text input field with the placeholder "A . B . C . D / M" and a blue "+" button to its right.
- Interface:** A dropdown menu with a downward arrow.
- Advance Configuration:** A checked checkbox.
- Connected:** An unchecked checkbox.
- Static:** An unchecked checkbox.
- RIP:** An unchecked checkbox.
- BGP:** An unchecked checkbox.

At the bottom right, there are "Cancel" and "Apply" buttons.

**Router ID:** The Router ID (RID) is a unique identifier assigned to each router participating in the OSPF routing domain. It's a 32-bit number, often represented in dotted-decimal format (e.g., 192.168.0.1). The RID is crucial for several OSPF operations, including neighbour establishment, database synchronisation, and SPF (Shortest Path First) tree calculation.

**Network:** Input IP and Netmask (0.0.0.0/255.255.255.255). Here you can add multiple network by clicking on the  Button.

# Routing - BGP

Configuration → Routing → BGP

The screenshot shows the 'General' tab of the BGP configuration page. At the top, there are three tabs: 'General' (selected), 'Neighbors', and 'Network'. Below the tabs, there is a search bar and an 'Add' button. A table lists two entries:

Name	Rule Type	Action
cvgv	By Group	
Microsoft11	By Group	

At the bottom, it says 'Showing 1 to 2 of 2 entries' and has 'Previous', '1', and 'Next' navigation buttons.

BGP, or Border Gateway Protocol, is a standardized exterior gateway protocol used to exchange routing and reachability information between autonomous systems (ASes) on the internet. It's a path vector protocol, which means it's designed to make routing decisions based on the shortest path, policies, and rule sets.

The screenshot shows the 'Neighbors' tab of the BGP configuration page. At the top, there are three tabs: 'General', 'Neighbors' (selected), and 'Network'. Below the tabs, there is a search bar and an 'Add' button. A table lists two entries:

Name	Rule Type	Action
cfvcv	By Group	
Microsoft	By Group	

At the bottom, it says 'Showing 1 to 2 of 2 entries' and has 'Previous', '1', and 'Next' navigation buttons.

BGP establishes neighbor relationships with other BGP-speaking routers. These peerings are essential for exchanging routing information.

The screenshot shows the 'Network' tab of the BGP configuration page. At the top, there are three tabs: 'General', 'Neighbors', and 'Network' (selected). Below the tabs, there is a search bar and an 'Add' button. A table lists one entry:

Name	Rule Type	Action
dfg	By Group	

At the bottom, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' navigation buttons.

Network generally refers to a specific IP network or subnet that an autonomous system (AS) advertises to its BGP neighbors. When a network is advertised in BGP, it informs other BGP routers about the reachability of that network through the advertising router.

Configuration → Routing → BGP → General → Add

The screenshot shows a 'BGP' configuration window with a 'General Configuration' section. The fields are as follows:

- Name:** Enter Name
- Rule Type:**  By Group,  By Name
- Devices:** Select Groups
- Autonomous system No.:** 1-4294967295
- Redistribute local routes:**  Enable,  Disable
- Redistribute connected routes:**  Enable,  Disable

Buttons: Cancel, Apply

**Devices:** Select a Device Group or a Device in which you want to create BGP Server.

**Autonomous System No:** In Border Gateway Protocol (BGP), an Autonomous System Number (ASN) is a unique numeric identifier assigned to an autonomous system (AS). An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet.

**Redistribute local routes.:** The redistribute local routes refers to the process of advertising routes that are locally generated or exist within the router's routing table into the BGP routing table. This allows these routes to be propagated to BGP neighbors and potentially further into the BGP network. Remember to exercise caution when redistributing routes into BGP, as it can have significant impacts on your network's routing behavior. Make sure to consider the implications on route selection, routing policy, and potential routing loops.

Also, ensure that proper filtering and route policies are in place to control the routes being redistributed and to ensure that only the intended routes are advertised into the BGP network.

**Redistributing connected routes:** It is a common practice when you want to advertise routes from interfaces that are directly connected to a BGP router into the BGP routing table. Keep in mind that redistributing connected routes into BGP should be done with caution, and you should consider the implications on route selection, routing policy, and potential routing loops. It's important to have a good understanding of your network's requirements and design before redistributing routes into BGP.

Configuration → Routing → BGP → Neighbor → Add

**BGP**

**Neighbors Configuration**

Name: Enter Name

Rule Type:  By Group  By Name

Devices: Select Groups

IP Address: IP Address

AS Number: 1 - 4294967295

Nexthop:  Enable  Disable

Multihop:  Enable  Disable

Cancel Apply

**Devices:** Select a Device Group or a Device in which you want to create BGP Server.

**IP Address:** The IP address is crucial in BGP for defining the neighbors with whom the BGP router will establish TCP connections and establish BGP neighbor relationships for the exchange of routing information.

**AS Number:** An Autonomous System Number (ASN) plays a significant role in establishing BGP neighbor relationships and routing information exchange. An ASN is a unique identifier assigned to an autonomous system, which is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet. When configuring a BGP neighbor relationship, you need to specify the ASN of both the local router (your own ASN) and the remote router (the neighbor's ASN).

**Next hop:** The next-hop is a crucial attribute associated with a BGP route. It specifies the IP address of the next router or hop that should be used to reach the destination network for a particular BGP route. This information is essential for the proper forwarding of packets in a BGP network.

**Multihop:** The "multihop" feature allows for the establishment of a BGP neighbor relationship over a non-directly connected path, spanning multiple hops. This feature is used when you need to set up a BGP neighbor relationship with a router that is not on a directly connected subnet. The typical BGP behavior is to establish a neighbor relationship directly with an adjacent router on a shared network segment. However, in certain scenarios, you may want to establish a BGP neighbor relationship with a router that is more than one hop away, perhaps on a different subnet. The multihop feature enables this by allowing you to specify the number of hops (routers) between your BGP router and the remote BGP router.

Configuration → Routing → BGP → Network → Add

**BGP**

**Network Configuration**

Name: Enter Name

Rule Type:  By Group  By Name

Devices: Select Group

Prefix: 0.0.0.0

Prefix Length: 0 - 32

Cancel Apply

**Devices:** Select a Device Group or a Device in which you want to create BGP Server.

**Prefix:** A prefix refers to a unique identifier for a route in an IP network. It consists of an IP address and a prefix length, expressed in CIDR (Classless Inter-Domain Routing) notation.

**Prefix Length:** The prefix length indicates the number of bits in the network address that are fixed (representing the network portion) and the number of bits that can vary (representing the host portion). It is denoted using CIDR notation (e.g., /24), where the number after the slash (/) indicates the length of the network prefix in bits.

For example, a BGP prefix could be expressed as "192.168.0.0/24", where: "192.168.0.0" is the IP address.

"/24" denotes the prefix length, indicating that the first 24 bits of the IP address represent the network portion.

# Firewall - Port Forwarding

Configuration → Firewall → Port forwarding

Port Forwarding Configuration / Firewall / Port Forwarding

Show 10 entries Search:

Name	Rule Type	Action
No data available in table		

Showing 0 to 0 of 0 entries Previous Next

Port forwarding is a networking technique used to redirect network traffic from one port on a network device to another port on a different device. It allows incoming traffic to reach a specific service or application hosted on a private network, which is behind a network address translation (NAT) or firewall. Port forwarding is a powerful tool that helps optimize network traffic flow, enhance accessibility, and efficiently manage services within a network. However, it's important to configure it securely to maintain network security.

Port Forwarding

Name

Rule Type  By Group  By Name

Select Groups

Protocol  TCP  UDP  ICMP  TCP+UDP

Source Port

Destination IP

Destination Port

Cancel Apply

**Protocol:** The term protocol refers to the specific networking protocol being used for forwarding traffic from one port to another.

**TCP:** TCP or Transmission Control Protocol, is one of the core protocols of the Internet Protocol (IP) suite. It operates at the transport layer (Layer 4) of the OSI model and is responsible for providing reliable, connection-oriented communication between devices over an IP network. TCP is widely used for various applications and services on the internet. TCP is used by a wide range of applications, including web browsing, email, file transfers (e.g., FTP), remote administration (e.g., SSH), and more. It forms the basis for reliable data transmission over the internet and is a critical protocol for modern network communication.

**UDP:** UDP, or User Datagram Protocol, is a connectionless and lightweight transport layer (Layer 4) protocol in the Internet Protocol (IP) suite. Unlike TCP, UDP does not provide mechanisms for reliable, ordered, or error-checked delivery of data. It is designed for fast and efficient data transmission, making it suitable for applications where speed and low latency are more critical than data reliability. UDP is faster and more efficient than TCP, it lacks features such as reliability and error correction. Therefore, applications using UDP must implement their own error detection and correction mechanisms if needed. The choice between UDP and TCP depends on the specific requirements of the application, balancing speed versus reliability.

**ICMP:** ICMP, or Internet Control Message Protocol, is an integral part of the Internet Protocol (IP) suite and operates at the network layer (Layer 3). It's primarily used for diagnostics and error reporting in IP networks, providing a means to communicate error and control messages between devices. ICMP is an essential protocol for network troubleshooting, diagnostics, and management. It provides valuable information about the network's health and assists in identifying and resolving various network-related issues. However, due to its critical role, ICMP messages should be handled carefully to avoid misuse or potential security risks.

**TCP+UDP:** You can use both TCP and UDP simultaneously, depending on the requirements. For instance, a VoIP application may use UDP for real-time audio transmission (low latency), while using TCP for signaling and control (reliability).

**Source Port:** The source port refers to the port number from which the incoming connection or data packet originates. When a client initiates a connection to a server or service, it typically selects a source port as part of the communication process. In the context of port forwarding, the source port is important because it helps determine which specific port on the client side is making the initial request. The source port is often dynamically assigned by the client's operating system or application.




**Destination IP:** The destination IP address is the specific IP address to which data packets are directed and where they are intended to be delivered within a network.

**Destination Port:** The destination port refers to the port number on a network device (such as a computer, server, or network appliance) to which incoming network traffic is directed. It helps determine which specific service or application running on the destination device should receive the incoming packets.

# Firewall - IP Filter

Configuration → Firewall → IP Filter

The screenshot shows the IP Filter configuration page. At the top, there is a breadcrumb trail: Configuration / Firewall / IP - Filter. Below this, there is a search bar and a dropdown menu set to '10' entries. A table lists the filter entries. The table has three columns: Name, Rule Type, and Action. The first entry is 'anjali12' with Rule Type 'By Group'. The Action column contains three icons: a green eye, a pencil, and a red trash can. At the bottom of the table, it says 'Showing 1 to 1 of 1 entries'. On the right side, there are 'Previous', '1', and 'Next' navigation buttons.

Name	Rule Type	Action
anjali12	By Group	  

IP filtering, often referred to as packet filtering, is a technique used in networking and network security to control the flow of network traffic based on specific criteria related to IP addresses, ports, protocols, or other attributes present in the headers of datapackets. It allows or denies network traffic based on a predefined set of rules or policies.

The screenshot shows the IP-Filter configuration dialog box. It has a title bar 'IP-Filter' with a close button. The dialog is divided into several sections. The first section is 'IP - Filter' with a blue header. Below this, there are several fields and options: 'Name' (text input), 'Rule Type' (radio buttons for 'By Group' and 'By Name'), 'Rule Mode' (radio buttons for 'Black-list' and 'White-list'), 'Protocol' (radio buttons for 'All', 'ICMP', 'TCP', 'UDP', 'TCP+UDP'), 'Source Zone' (radio buttons for 'LAN' and 'WAN'), 'Source IP' (text input), 'Destination Zone' (radio buttons for 'LAN' and 'WAN'), and 'Destination Port' (text input). At the bottom right, there are 'Cancel' and 'Apply' buttons.

**Rule Mode:** Rule mode refers to the operational state or behavior of a rule within a firewall or other network security device. A rule typically defines a specific action or set of actions to be taken based on defined criteria such as source/destination addresses, ports, protocols, and more.

The appropriate mode is selected based on the desired outcome, whether it's allowing specific traffic, denying unwanted traffic, logging traffic for analysis, triggering alerts, or closely inspecting traffic for security purposes.

Enable Blacklist if you want to deny unwanted traffic and enable Whitelist if you want to allow specific traffic.

Protocol: For protocol refer to Page nos. 89 and 90.

**Source Zone:** A source zone refers to a specific network segment, area, or domain from which network traffic originates. It is part of the broader concept of network segmentation and is commonly used in firewall and security policies to define rules based on the source of the traffic.

Choose LAN or WAN according to your choice.

**Source IP:** The source IP (Internet Protocol) address is a fundamental component of network communication. It identifies the origin or sender of a packet or data transmission in a network. Each device connected to a network, whether it's a computer, server, router, or any other networked device, is assigned a unique source IP address.

**Destination Zone:** A destination zone refers to a designated area or grouping of network segments, devices, or systems within a network where incoming traffic is directed or intended to reach. It is an important aspect of access control and traffic management.

Choose LAN or WAN according to your choice.

**Destination Port:** The "destination port" is a port number used in networking to identify the intended recipient or service on a device to which incoming network traffic is directed. In the context of the transport layer protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), the destination port is an essential component of network communication.

Port Numbers Range:

Destination port numbers range from 0 to 65535.

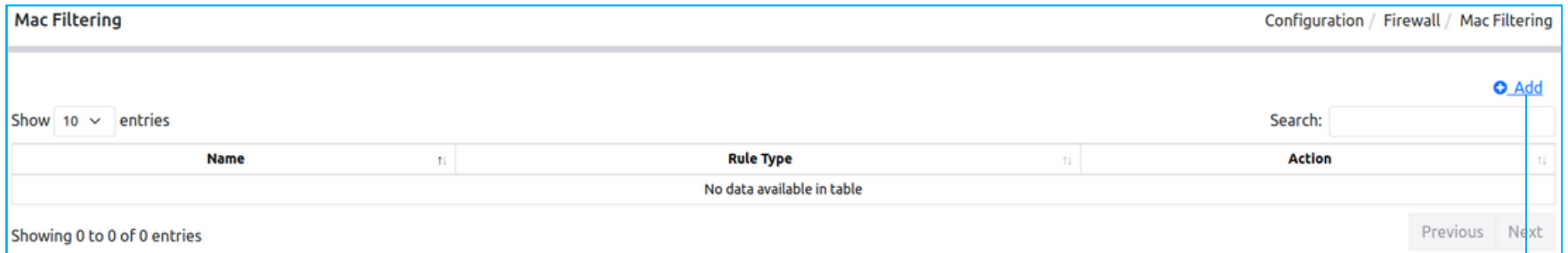
Ports from 0 to 1023 are well-known ports and are reserved for system services or protocols (e.g., HTTP uses port 80, SMTP uses port 25).

Ports from 1024 to 49151 are registered ports and can be used by user applications and protocols.

Ports from 49152 to 65535 are dynamic or private ports and are available for temporary use by client applications.

# Firewall - MAC Filter

Configuration → Firewall → MAC Filter



MAC filtering is a security feature that allows or denies devices from accessing a network based on their MAC address. It can be used to improve security, provide access control, and improve network management.

The screenshot shows the 'Firewall' configuration dialog box. The 'Mac Filtering' section is highlighted in blue. It contains the following fields and options:

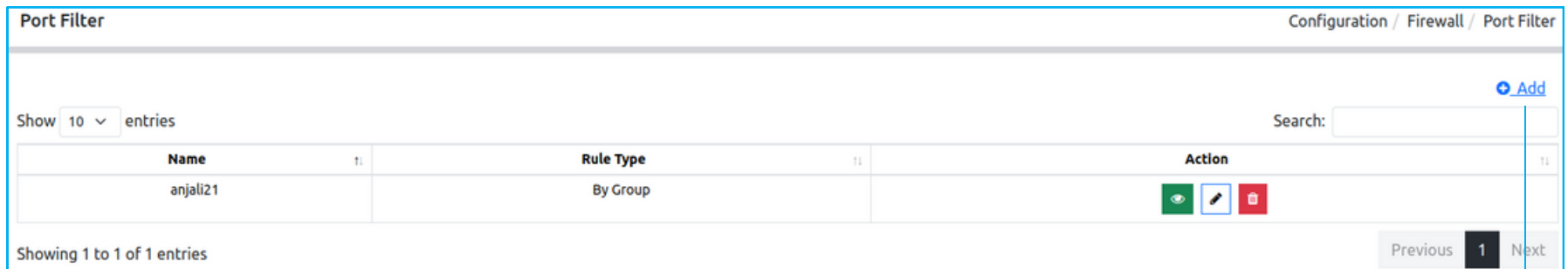
- Name:** A text input field with the placeholder 'Enter Name'.
- Rule Type:** Two radio button options: 'By Group' (selected) and 'By Name'.
- Devices:** A dropdown menu with the placeholder 'Select Groups'.
- Mac Address:** A text input field with the placeholder 'Enter Mac Address'.

At the bottom right of the dialog box, there are 'Cancel' and 'Apply' buttons. A blue arrow points from the 'Add' button in the previous screenshot to the 'Mac Filtering' section of this dialog box.

Select Device or Device Group and enter the MAC Address then click on Apply Button.




# Firewall - Port Filter

Configuration → Firewall → Port Filter



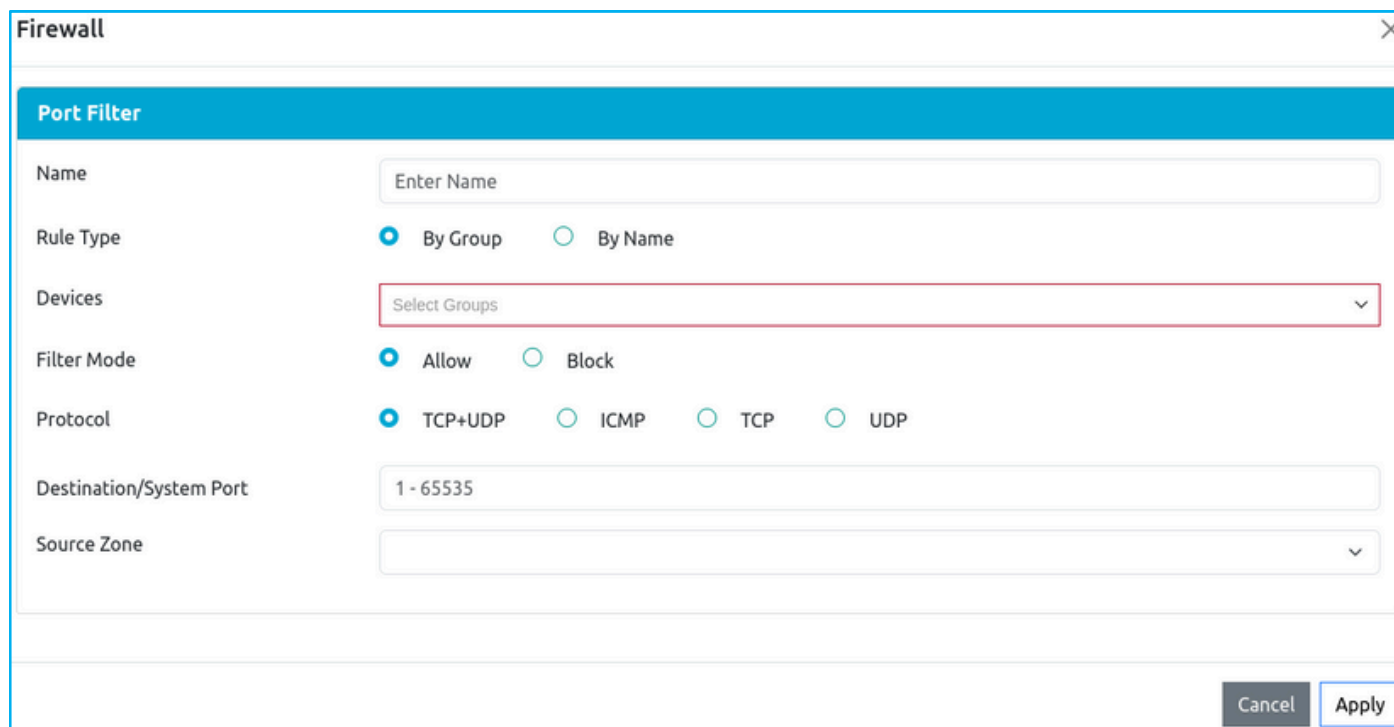
Port Filter Configuration / Firewall / Port Filter

Show 10 entries Search:

Name	Rule Type	Action
anjali21	By Group	  

Showing 1 to 1 of 1 entries Previous 1 Next

Port filtering is a network security measure that involves controlling or restricting access to specific network ports on a device or network. A port is a virtual endpoint for communication, and filtering ports helps regulate incoming and outgoing network traffic based on predefined rules and policies.



Firewall Port Filter

Name:

Rule Type:  By Group  By Name

Devices:

Filter Mode:  Allow  Block

Protocol:  TCP+UDP  ICMP  TCP  UDP

Destination/System Port:

Source Zone:

Cancel Apply

**Filter Mode:** Filter mode" in networking and network security refers to the behavior and action taken by a filtering system, such as a firewall or security device, when a data packet or network traffic matches a specific filtering rule. The mode determines what action is applied to the traffic based on the rules defined in the filter.

Enable the appropriate filter mode. There are two filter modes Allow and Block.

**Allow:** In "allow" mode, the filtering system allows traffic that matches the specified rules to pass through or be processed. Traffic that does not match any rules might be implicitly denied.

**Block:** In Block mode, the filtering system blocks or rejects traffic that matches the specified rules. Traffic that does not match any rules might be implicitly allowed or dropped.

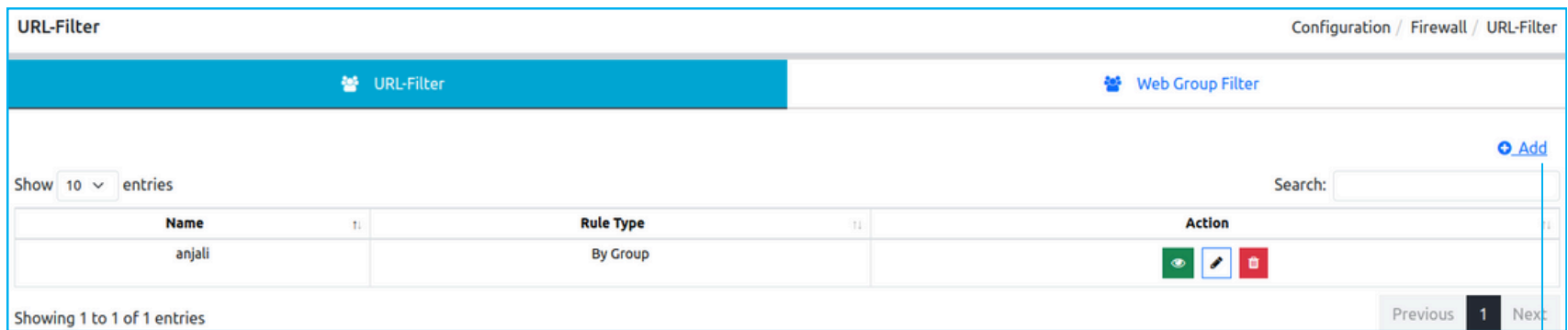
Protocol: Refer to page no 89 and 90.

Source Zone: Refer to page no 92.




Destination/ System Port: Refer to page no 92.

# Firewall - URL Filter

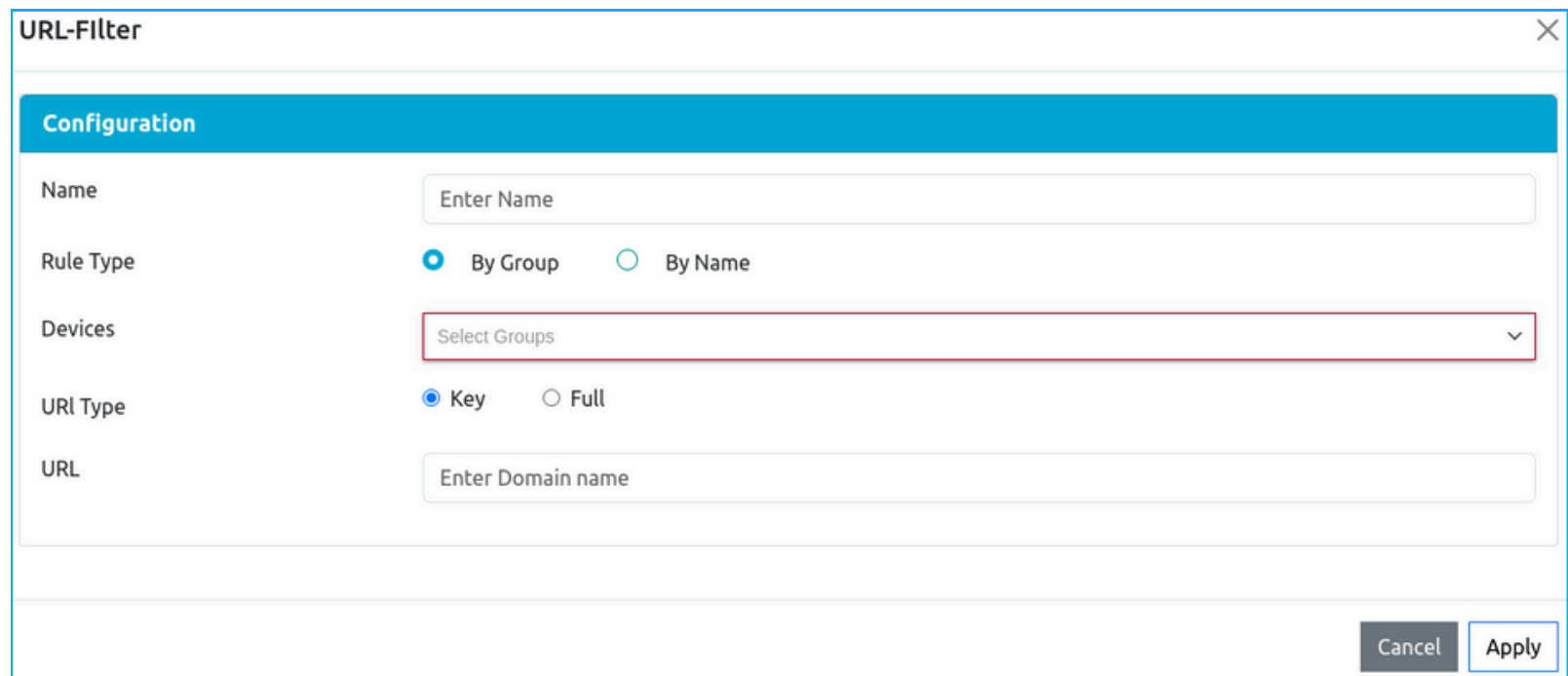
Configuration → Firewall → URL Filter



The screenshot shows the 'URL-Filter' configuration page. At the top, there are tabs for 'URL-Filter' (selected) and 'Web Group Filter'. Below the tabs, there is a search bar and a table of entries. The table has columns for 'Name', 'Rule Type', and 'Action'. One entry is visible with the name 'anjali' and 'By Group' as the rule type. The action column contains icons for enable, edit, and delete. At the bottom, there are 'Previous', '1', and 'Next' navigation buttons.

Name	Rule Type	Action
anjali	By Group	  

URL filtering is a network security measure that involves controlling or restricting access to specific websites or web resources based on their URLs (Uniform Resource Locators). It's a common approach used to enforce security policies, improve productivity, and protect against potential security threats in networks.



The screenshot shows the 'URL-Filter' configuration form. It has a 'Configuration' header. The form contains the following fields and options:

- Name:** Enter Name
- Rule Type:**  By Group  By Name
- Devices:** Select Groups
- URI Type:**  Key  Full
- URL:** Enter Domain name

At the bottom right, there are 'Cancel' and 'Apply' buttons.

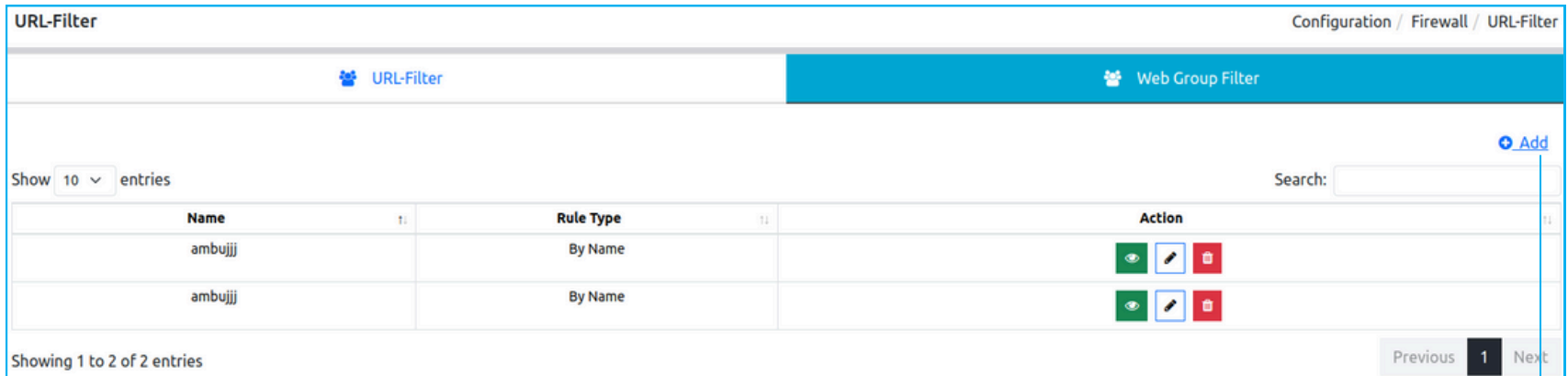
**Devices:** Select the device group if you selected the Rule type as By Group or select a device group if you selected the Rule type as By Name in which you want add URL Filter.

**URL Type:** URL type refers to the classification or categorization of URLs (Uniform Resource Locators) based on their content, purpose, or characteristics. URLs can be categorized into various types to help manage, control, and filter access to websites or web resources based on specific criteria. URL categorization is a fundamental component of URL filtering and content filtering systems.







**Key URL:** Key URL types provide a summarized or high-level categorization of URLs based on their broad content, purpose, or characteristics.

**Full URL:** Full URL types offer a more detailed and granular categorization of URLs, often including subcategories or more specific classifications.

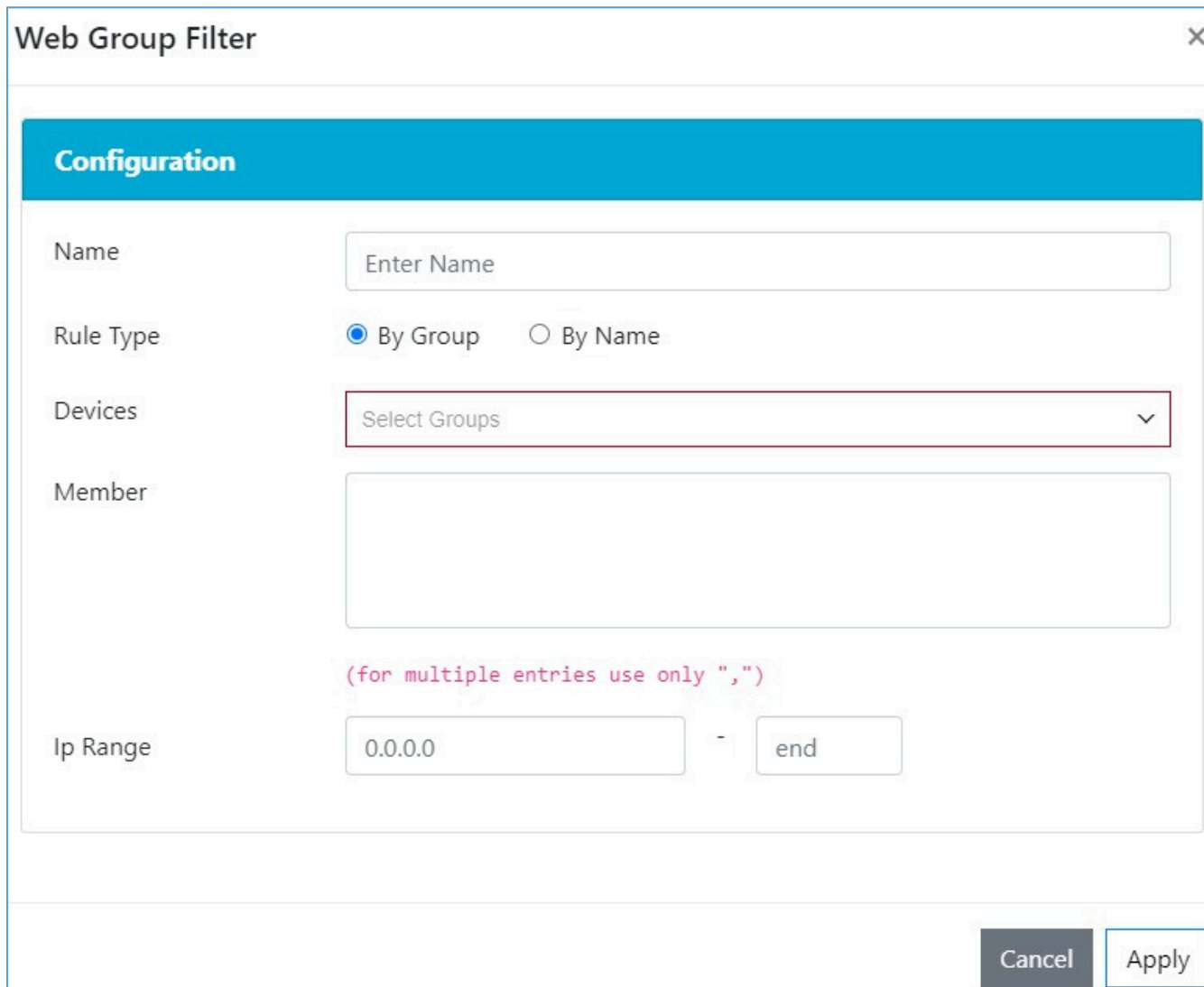
Configuration → Firewall → URL Filter → Web Group Filter



The screenshot shows the 'URL-Filter' configuration page. At the top, there are tabs for 'URL-Filter' and 'Web Group Filter'. Below the tabs, there is a search bar and a table with two entries. The table has columns for 'Name', 'Rule Type', and 'Action'. The first entry has 'ambujjj' as the name and 'By Name' as the rule type. The second entry also has 'ambujjj' as the name and 'By Name' as the rule type. The 'Action' column contains icons for view, edit, and delete. At the bottom, there are 'Previous' and 'Next' buttons, with '1' indicating the current page.

Name	Rule Type	Action
ambujjj	By Name	  
ambujjj	By Name	  

A web group filter typically refers to a feature or mechanism within network security tools, such as firewalls or web filtering solutions, that allows the categorization and management of websites or web content into groups for easier control and access management. This functionality is commonly used to enforce security policies and improve network productivity.



The screenshot shows the 'Web Group Filter' configuration dialog box. It has a 'Configuration' tab. The fields are: 'Name' (text input with placeholder 'Enter Name'), 'Rule Type' (radio buttons for 'By Group' and 'By Name'), 'Devices' (dropdown menu with 'Select Groups'), 'Member' (text area), and 'Ip Range' (text input with '0.0.0.0' and 'end' fields). There is a note '(for multiple entries use only ",")' below the 'Member' field. At the bottom, there are 'Cancel' and 'Apply' buttons.

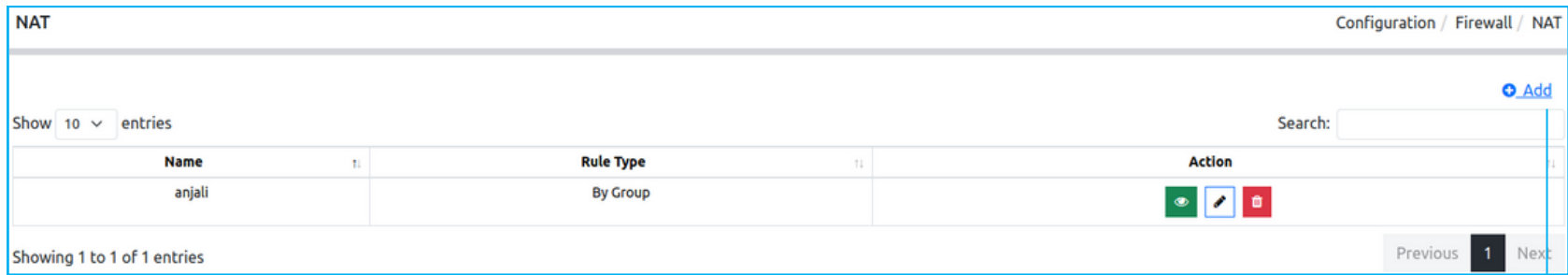
**Devices:** Select the device group if you selected the Rule type as By Group or select a device name if you selected the Rule type as By Name in which you want add Web GroupFilter.




**Member:** In Member you have to input the URL or group of URLs those you want to Block. Use coma “ , “ if you input multiple URLs.

**IP Range:** An IP range refers to a set of IP addresses or a range of IP addresses that are specified for filtering or controlling access to a web group or specific content on the web. This is a common practice in network and security management to control who can access certain services, websites, or resources based on their IP address. For example, an IP range like "192.168.1.0 -192.168.1.255" includes all the possible IP addresses starting from 192.168.1.0 up to 192.168.1.255 will blocked.

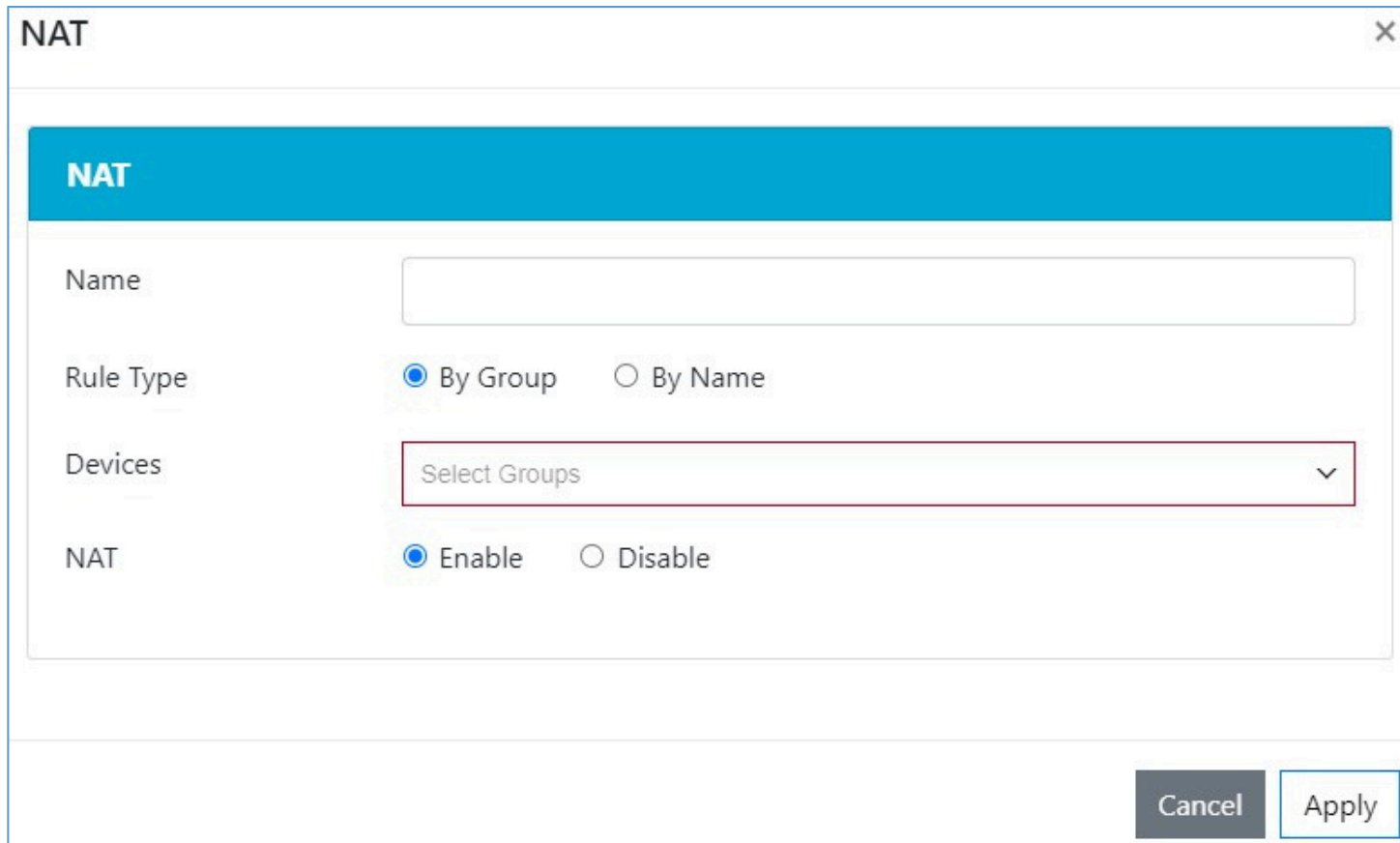
## Firewall - NAT

Configuration → Firewall → NAT



Name	Rule Type	Action
anjali	By Group	  

NAT, or Network Address Translation, is a crucial component of firewalls and network security. NAT operates at the network layer(Layer 3) of the OSI model and is primarily used to map private IP addresses to public IP addresses. NAT in a firewall is a fundamental tool used to manage and secure communication between a private network and the internet by translating private IP addresses to public IP addresses, thus ensuring efficient and secure data transfer.



**NAT**

Name

Rule Type  By Group  By Name

Devices

NAT  Enable  Disable




Cancel Apply

**Devices:** Select the device group if you selected the Rule type as By Group or select a device name if you selected the Rule type as By Name in which you want add Web GroupFilter.

**NAT:** Enable NAT if you want to apply NAT service to the selected Devices or Disable it if don't .

# Firewall - IPS

Configuration → Firewall → IPS

Name	Rule Type	Action
anjali	By Group	  

IPS, or Intrusion Prevention System, is an advanced security technology commonly integrated into firewalls. It's designed to detect and prevent malicious activities and attacks in a network. It is like having a security guard at the entrance of your network. It constantly checks who's coming in, verifies their credentials (the network packets), and takes action if it detects anything suspicious or malicious, providing an additional level of security and threat prevention.

**IPS**

Name:

Rule Type:  By Group  By Name

Select Groups:

**Per Ip Address**

Total allow incoming connection number:

Max incoming connection retry number:   during  sec.

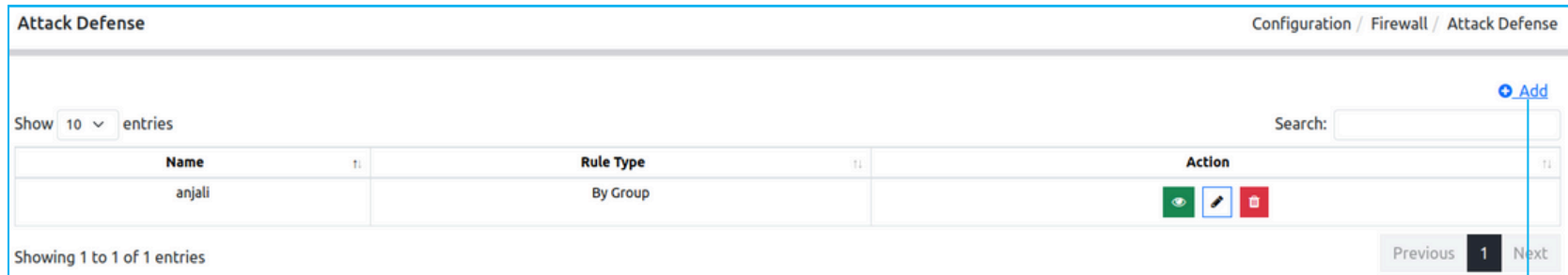
Cancel Apply

**Total Allow incoming connection number:** The "Total Allow Incoming Connection Number" refers to the maximum permitted number of incoming connections that are considered safe or allowed based on the security policies and configurations set within the IPS. Enable the check box and input your number between 1 to 60.




**Max incoming connection retry number:** The "Max Incoming Connection Retry Number" typically refers to the maximum number of attempts allowed for establishing a connection with a specific service or resource. When a connection attempt fails, the system or application may retry a certain number of times before considering the connection unsuccessful. Enable the check box and input the number and time. The number should be within 1 to 60 and time should be within 1 to 300 Sec.

# Firewall - Attack Defense

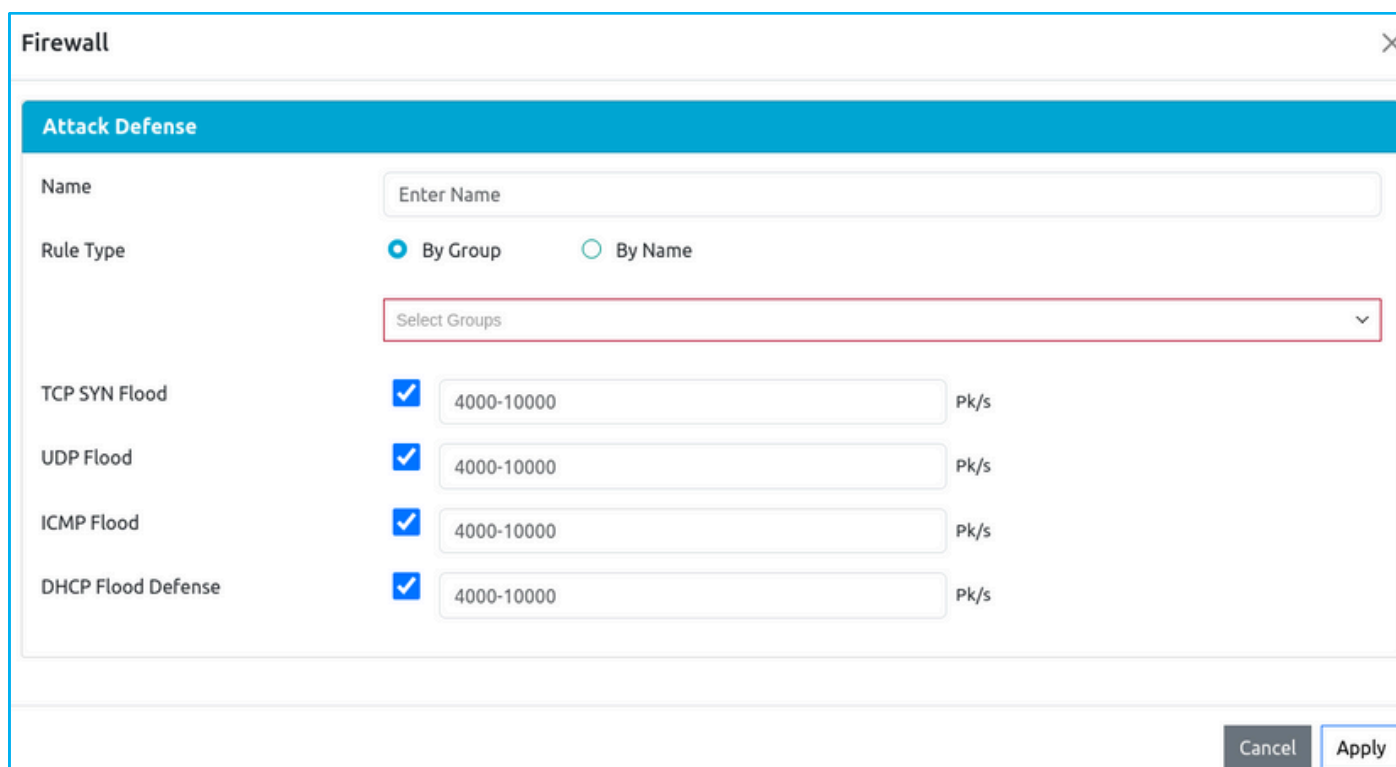
Configuration → Firewall → Attack Defense



The screenshot shows the 'Attack Defense' configuration page. At the top right, there is a breadcrumb trail: 'Configuration / Firewall / Attack Defense'. Below the header, there is a search bar and an 'Add' button. A table displays the configuration entries. The table has three columns: 'Name', 'Rule Type', and 'Action'. There is one entry with the name 'anjali' and a rule type of 'By Group'. The 'Action' column contains three icons: a green eye, a pencil, and a red trash can. At the bottom left, it says 'Showing 1 to 1 of 1 entries'. At the bottom right, there are navigation buttons: 'Previous', '1', and 'Next'.

Name	Rule Type	Action
anjali	By Group	  

Attack defense refers to strategies, measures, or mechanisms put in place to protect computer systems, networks, and data from various forms of cyber-attacks. It involves safeguarding against unauthorized access, malicious software, data breaches, and other security threats that could compromise the confidentiality, integrity, or availability of digital assets.



The screenshot shows the 'Firewall' configuration dialog box. The 'Attack Defense' section is highlighted in blue. It contains the following fields and options:

- Name:** A text input field with the placeholder 'Enter Name'.
- Rule Type:** Two radio buttons: 'By Group' (selected) and 'By Name'.
- Select Groups:** A dropdown menu with the placeholder 'Select Groups'.
- TCP SYN Flood:** A checkbox (checked) followed by a text input field containing '4000-10000' and the unit 'Pk/s'.
- UDP Flood:** A checkbox (checked) followed by a text input field containing '4000-10000' and the unit 'Pk/s'.
- ICMP Flood:** A checkbox (checked) followed by a text input field containing '4000-10000' and the unit 'Pk/s'.
- DHCP Flood Defense:** A checkbox (checked) followed by a text input field containing '4000-10000' and the unit 'Pk/s'.

At the bottom right of the dialog box, there are 'Cancel' and 'Apply' buttons.

**TCP SYN flood:** A TCP SYN flood is a type of DDoS (Distributed Denial of Service) attack that exploits the TCP protocol's three-way handshake process. Enable the check box and enter the number between 1 to 10000. For example, if you set the number like 500 the device will generate an alert when more than 500 tcppackets per second are coming to device.

**UDP flood:** A UDP flood attack is a type of DoS(Denial of Service) attack where an attacker floods a target system with a large number of UDP (User Datagram Protocol) packets in a short amount of time. Enable the check box and enter the number between 1 to 12000. For example, if you set the number like 500 the device will generate an alert when more than 500 udp packets per second are coming to device.

**ICMP flood:** An ICMP (Internet Control Message Protocol) flood attack is a type of DDoS (Distributed Denial of Service) attack where an attacker overwhelms a target system with a high volume of ICMP packets. . Enable the check box and enter the number between 1 to 1500. For example, if you set the number like 500 the device will generate an alert when more than 500 icmppackets per second are coming to device.

**DHCP flood defense:** A DHCP (Dynamic Host Configuration Protocol) flood attack involves overwhelming a DHCP server with a high volume of DHCP requests, exhausting its resources and preventing it from serving legitimate client requests. Enable the check box and enter the number between 1 to 4000. For example, if you set the number like 500 the device will generate an alert when more than 500 dhcppackets per second are coming to device.

<b>LOGS.....</b>	<b>4</b>
User Logs.....	4.1
Alarms.....	4.2

# Logs

Logs → User Log → Monitor Captive Log

Monitor Captive Log( 0) Dashboard / Monitor Captive Log

Show  entries Search:  [Export](#)

Login Time	Client Ip	Client Mac Address	Network Name	Username	Ap Mac Address	Message
No data available in table						

Showing 0 to 0 of 0 entries [Previous](#) [Next](#)

In Monitor Captive Log you able to see the Data of all the connected clients. Click [Export](#) to export the Data Sheet.



# Logs

Logs → Alarms → Manage Alarms

Manage Alarms Dashboard / Manage Alarms

Show  entries [✕ Clear All](#)

Search:

AP Name	Location Name	MAC Address	Alarms Type	Detection Time	Description	Action
Vipul-AP	Office-Location	68:33:2c:00:52:73	offline	2023-10-20T11:28:31.896Z	device offline	
Vipul-AP	Office-Location	68:33:2c:00:52:73	offline	2023-10-20T11:25:37.287Z	device offline	

Showing 91 to 92 of 92 entries Previous 1 ... 6 7 8 9 10 Next

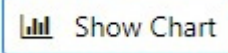
Alarms in logs are essential for maintaining the health and security of systems. It helps to identify and address problems proactively, reducing downtime, minimizing security risks, and ensuring that critical events do not go unnoticed. If you enable Alarms then it will display the system Vulnerabilities, Device Status(online/ offline) and all the other device logs.

<b>Stats.....</b>	<b>5</b>
Networks.....	5.1
Clients.....	5.2
Spectrum.....	5.3

# Stats

Stats → Networks

To check the statistics of a particular network click on



Statistics - Networks Dashboard / Statistics / Networks

Show  entries Search:

Network Name	Operating Mode	Action
ambuj	wep	Show Chart
common	open	Show Chart
demo@kenstel.com	wep	Show Chart

Showing 1 to 3 of 3 entries Previous **1** Next

**ambuj**

[Refresh](#)

Showing Current Month data

Traffic

**ambuj**

Showing Current Week data

Traffic

Client Count

**ambuj**

Showing 1 Day data

Traffic

Client Count

Select Selected Date

**ambuj**

Showing 1 Hour data - Fri Oct 27 2023 (Today)

Traffic

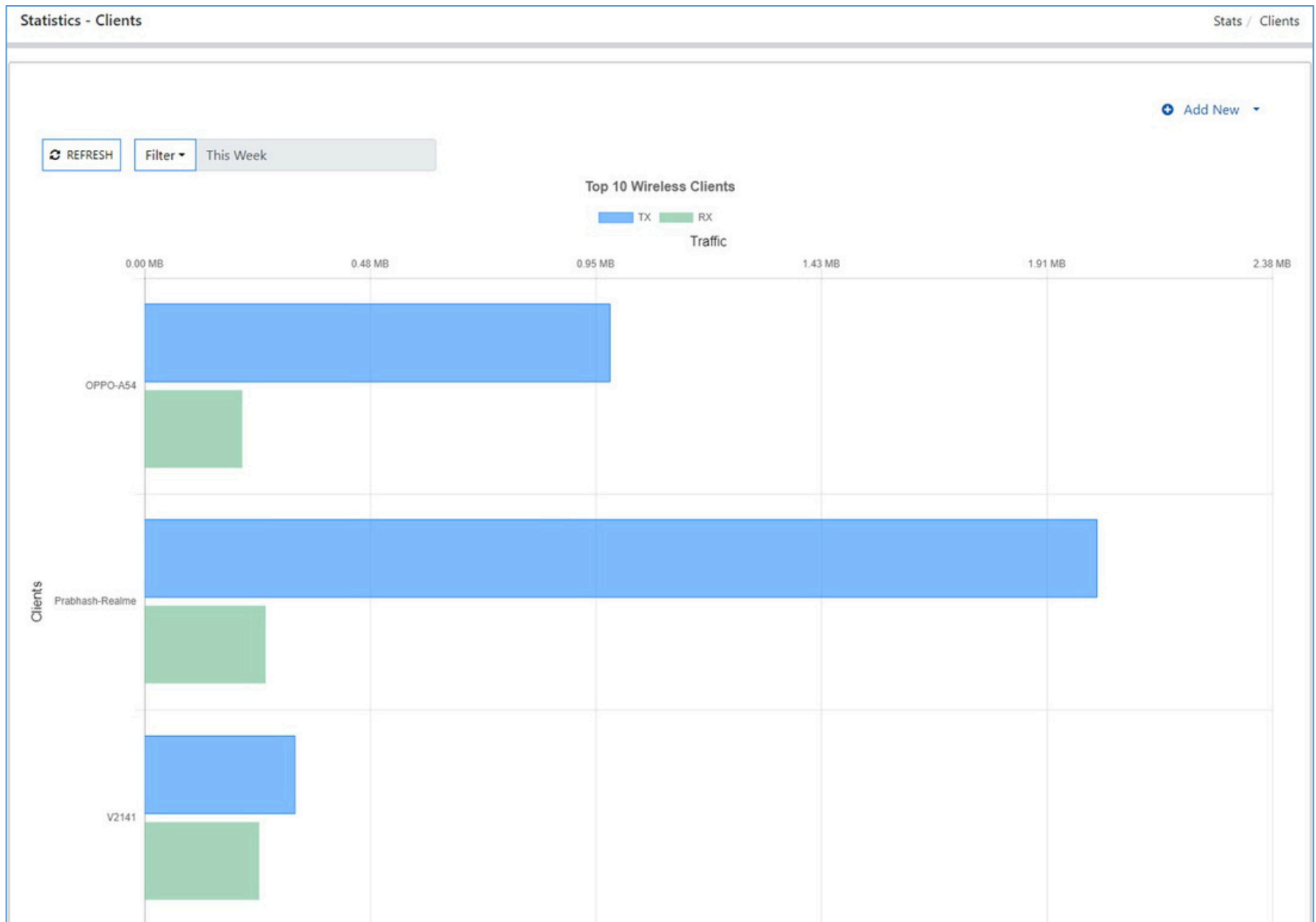
Client Count

Select Selected Hour

Here, you can check your network's statistics, such as how much data it consumes in an hour, a day, a week, or a month.

# Stats

Stats → Clients

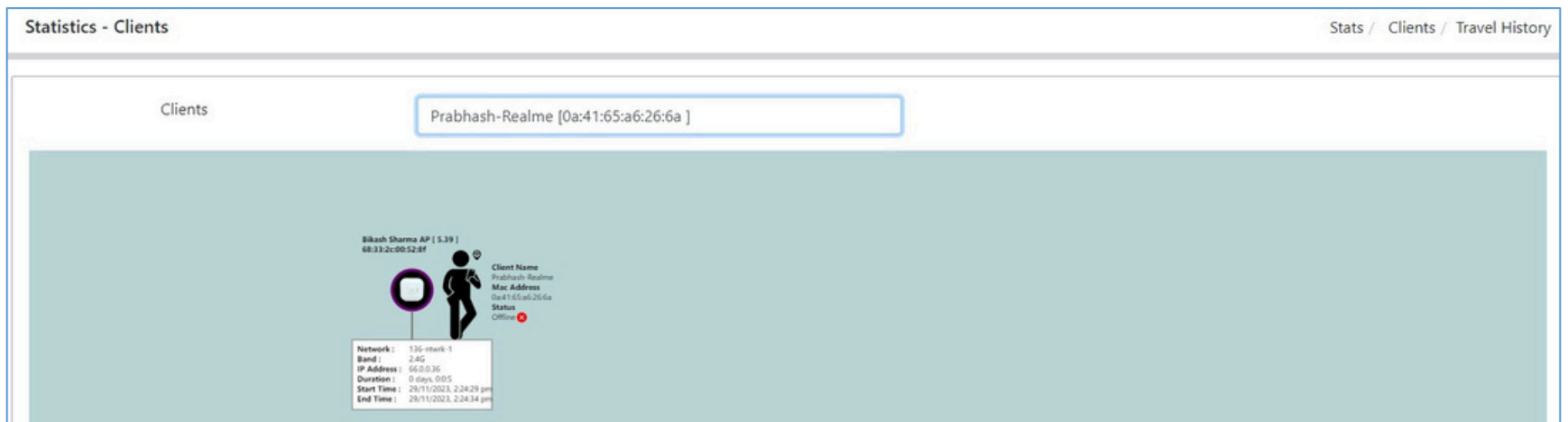
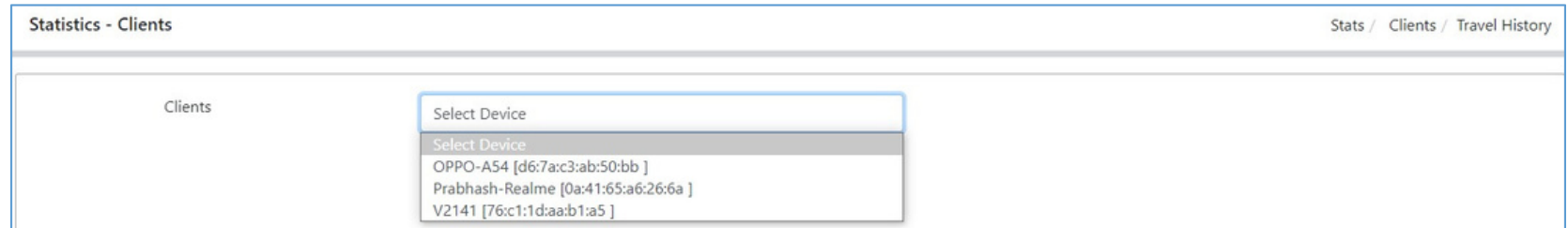


Clients are the devices connected to a specific network. Here, you can check the clients' statistics, including download and upload data consumption.

# Stats

To check the client's history click on

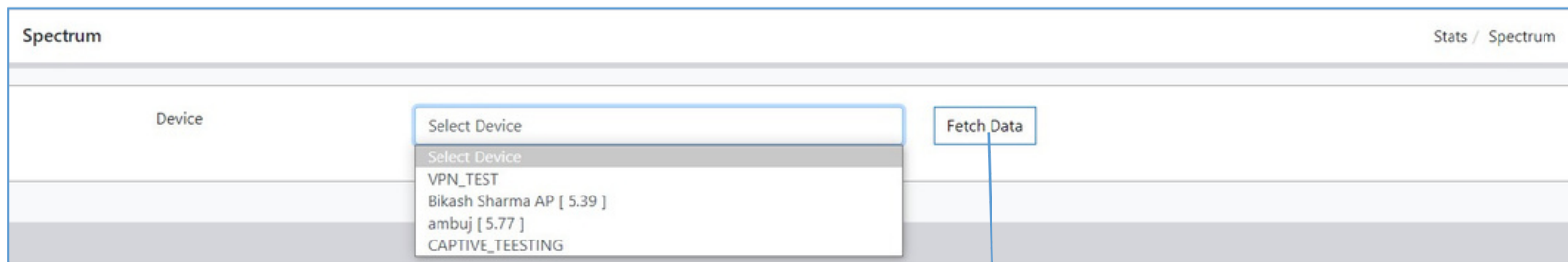
Stats → Clients → Add New → Client Travel History



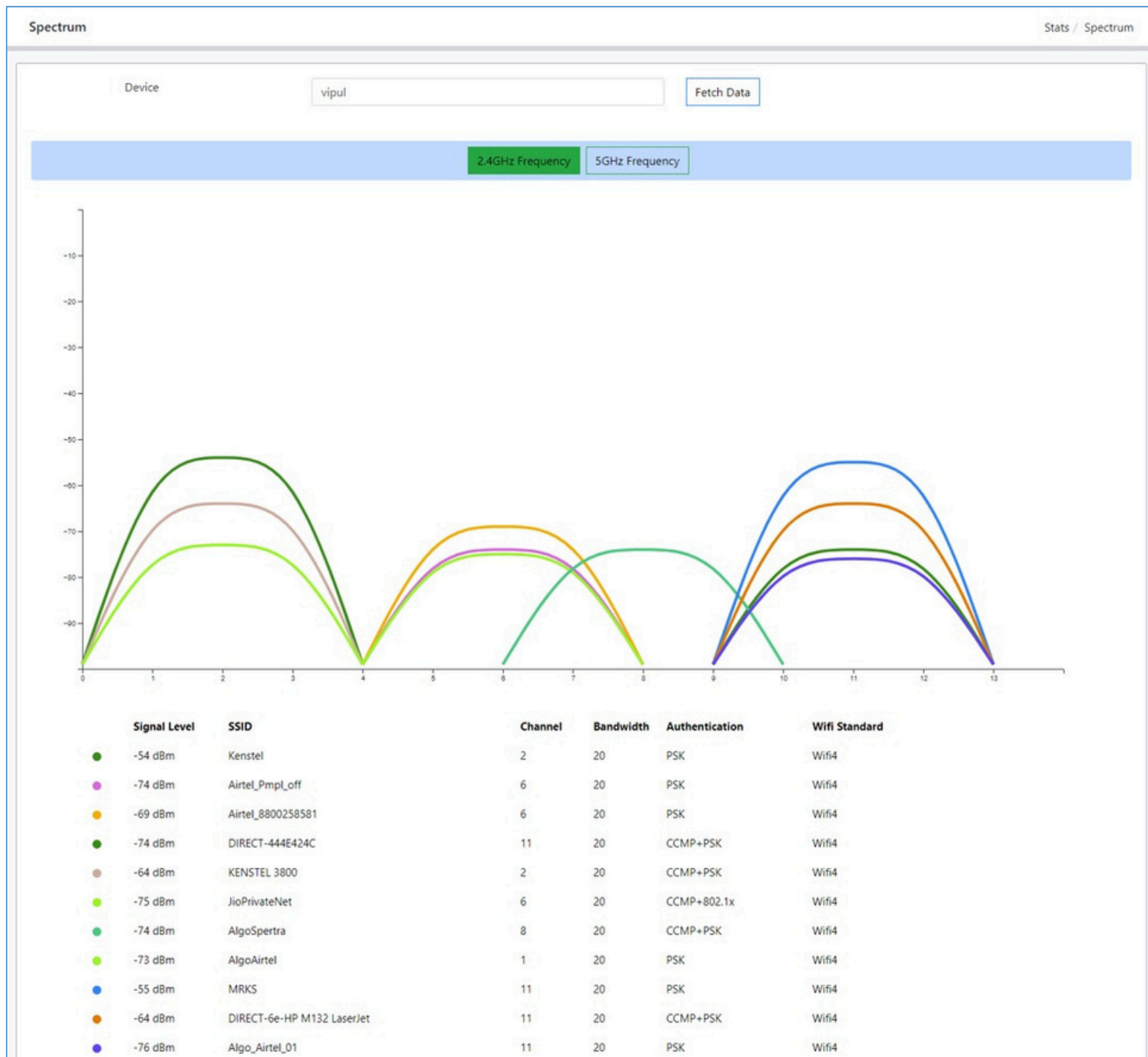
Here you can check the data history of a client.

# Stats

Stats → Spectrum

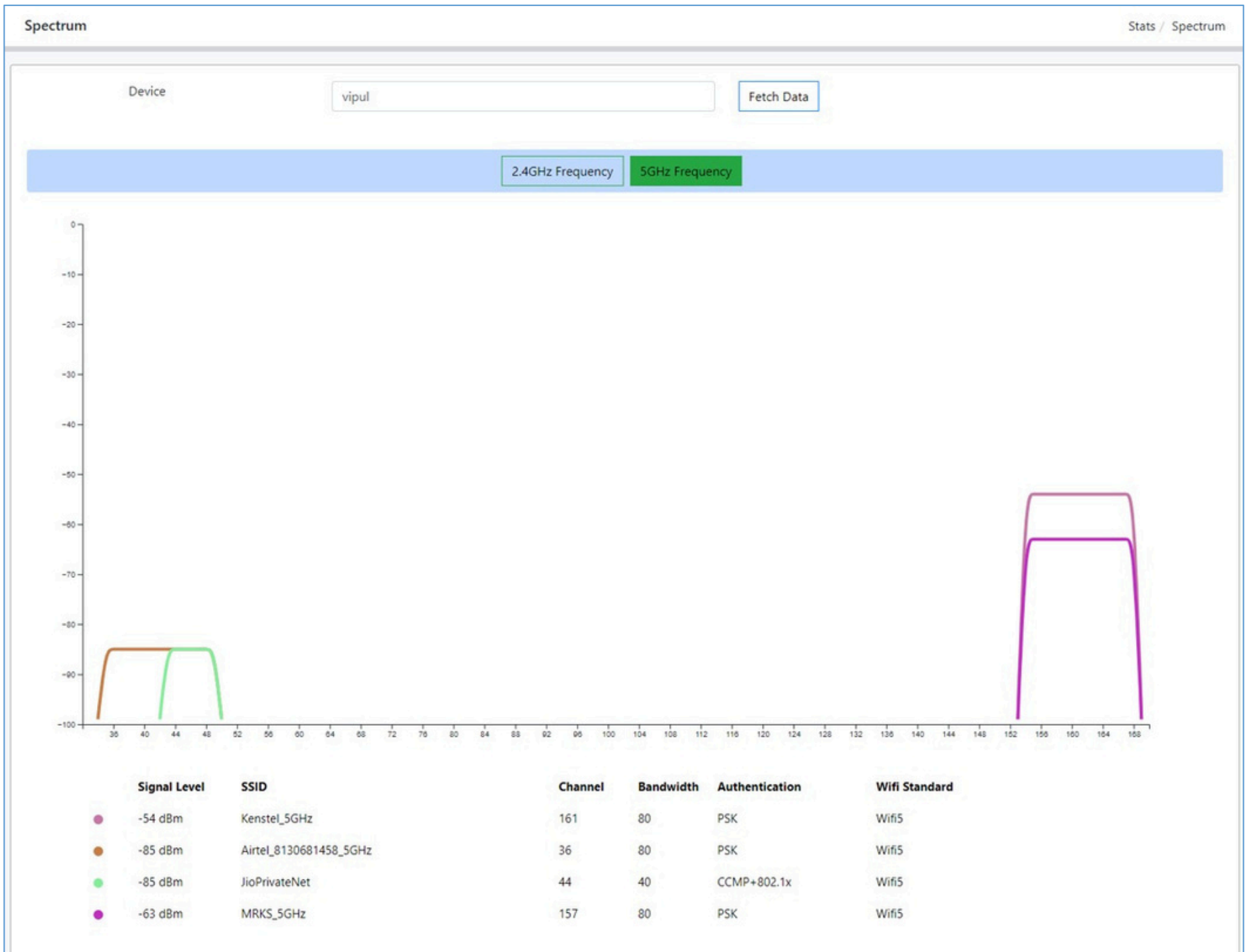


Select device and click on Fetch data



Here you able to see the statistics of the nearby devices. You can check the stats in 2.4 GHz as well as in 5 GHz. These are the stats of 2.4 GHz

# Stats



These are the stats of 5 GHz

**Update.....6**

# Update

To Update firmware, firstly go to administration page then select Firmware Model, Firmware Version and Firmware Image (you can choose your image file from your gallery) then click on

 Release Update Button.

Administration - Update your Account Information Administration / Administration

---

**YOUR RECENT LOGINS**

Show  entries Search:

IP Address	ISP	Country	City	Region	Zip Code	Timezone	Date/Time
42.108.27.201	Vodafone Idea Ltd.	India	Gurugram	Haryana	122001	Asia/Kolkata	Wed May 08 2024 09:04:15 GMT+0000 (Coordinated Universal Time)

Showing 401 to 401 of 401 entries Previous 1 ... 37 38 39 40 **41** Next

This computer is using IP address 122.162.151.225.


[Sign out all sessions](#)

**UPGRADE FIRMWARE**

Firmware Model \*

Firmware Version \*

Firmware Image \*

 Release Update

**YOUR EMAIL ADDRESS**  
When you change your email address, an email will be sent to your new address for verification.

---

**ADD PRODUCTS**  
Enter a kenstel product name

---


**YOUR ACCOUNT**  
[Show/Hide](#) account settings.

---

**CHANGE YOUR PASSWORD**  
Changing your password will clear all your active sessions.

# Update

After Release Update, go to **Updates** → then Select your device and Click [Add to Upgrade](#) to update and then OK.

 12 AVAILABLE

---

Show  entries [Add to Upgrade](#)

Search:

<input type="checkbox"/>	Model	Name	MAC	IP Address	Current Sw. Version	Upgrade Sw. Version
<input type="checkbox"/>	KRO-110-5G	KRO_2	68:33:2c:00:57:e1	N.A		1.0.8
<input checked="" type="checkbox"/>	KRO-110-D4G	KRO_3	68:33:2c:00:57:e3	N.A		1.0.0

Showing 11 to 12 of 12 entries Previous 1 **2** Next

**Administration.....7**

Administration.....7.1

Add Management.....7.2

Configuration.....7.3

# Administration

Administration - Update your Account Information Administration

**YOUR RECENT LOGINS**

Show  entries Search:

IP Address	ISP	Country	City	Region	Zip Code	Timezone	Date/Time
No data available in table							

Showing 0 to 0 of 0 entries

This computer is using IP address 192.168.5.81.

On this Administration page, you are able to see the details of all the clients connected to the cloud.

Click on  for Sign out all the clients

**YOUR EMAIL ADDRESS**

When you change your email address, an email will be sent to your new address for verification.

Here you can update your Login Id.

**YOUR ACCOUNT**

[Show/Hide](#) account settings.

Name

Address

City


Country/Region


Zip or postal code


Phone

Here you can update your Account.

**CHANGE YOUR PASSWORD**  
Changing your password will clear all your active sessions.

Current Password  

New Password  

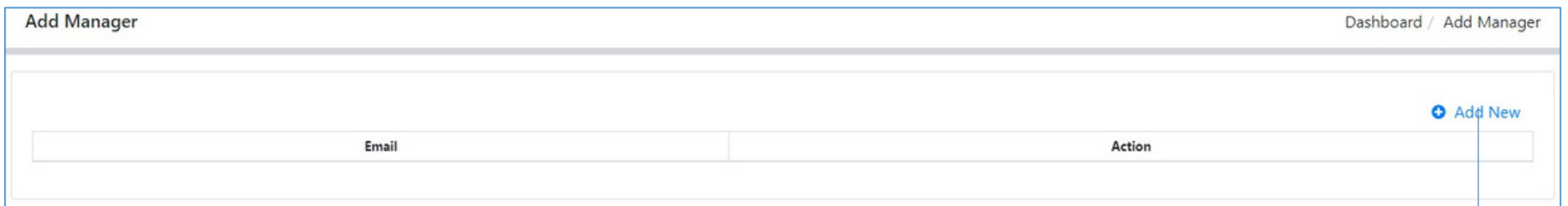
Confirm Password  

Here you can update your Password.

**Note:** Please read the instructions carefully while updating .

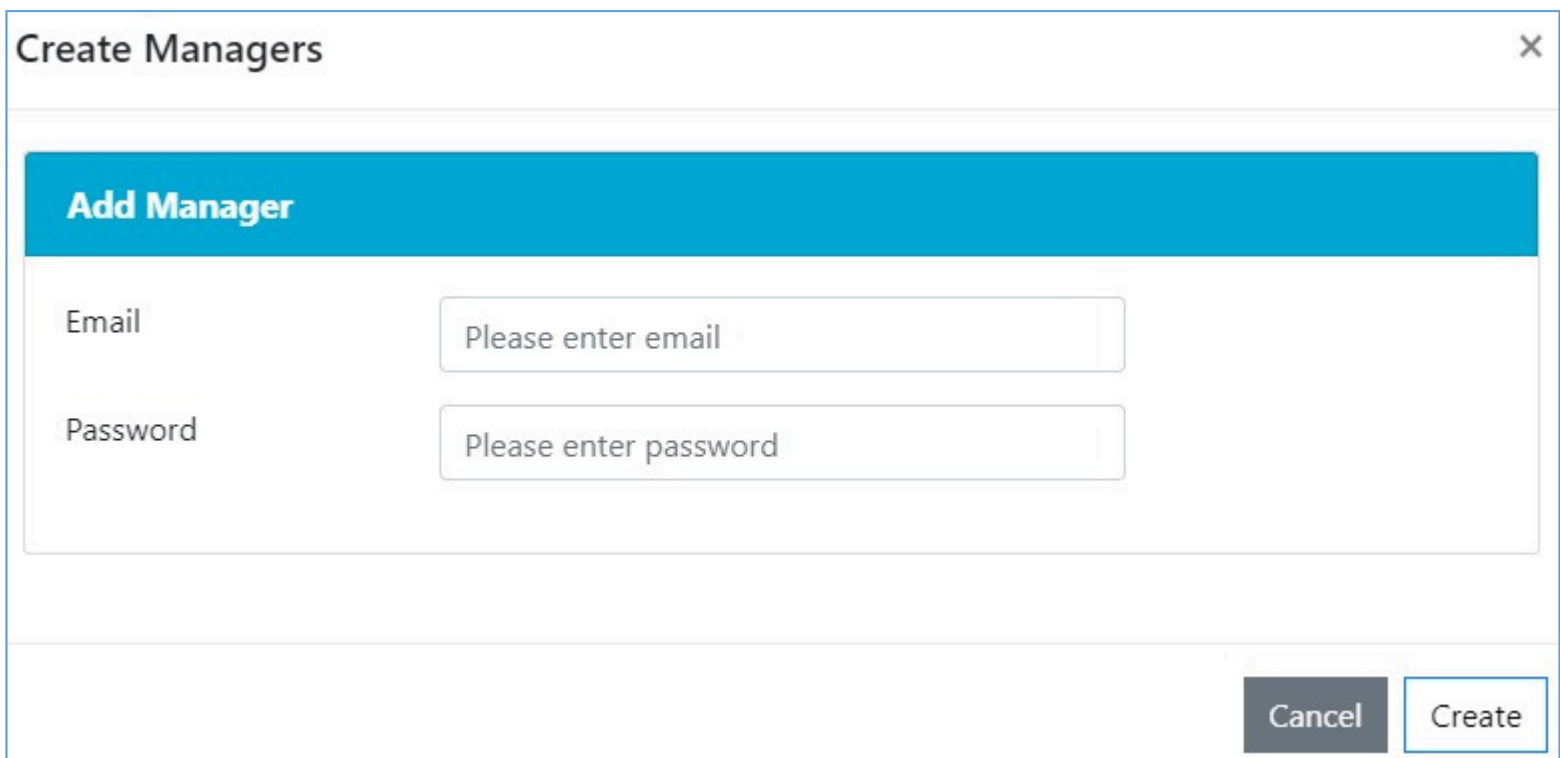
# Administration

Administration → Add Manager



The screenshot shows a web interface titled "Add Manager". In the top right corner, there is a breadcrumb trail "Dashboard / Add Manager". Below the header, there is a table with two columns: "Email" and "Action". The "Action" column contains a blue link with a plus icon and the text "Add New".

Here you get an overview of Manager.



The screenshot shows a modal dialog titled "Create Managers" with a close button (X) in the top right corner. Inside the modal, there is a blue header bar with the text "Add Manager". Below the header, there are two input fields: "Email" with the placeholder text "Please enter email" and "Password" with the placeholder text "Please enter password". At the bottom right of the modal, there are two buttons: "Cancel" and "Create".

Input the credentials and click on create. With this email and password you can login to the cloud.

# Administration

Administration → Configuration Management

## CREATE BACKUP SETTINGS

Create Backup

Click on Create Backup for a backup file of the configuration

## UPLOAD BACKUP SETTINGS

Upload backup \*

Select your file

Upload

Select the downloaded backup file and click on UploadButton to Upload.

## FACTORY RESET

Factory Reset

Click on Factory Reset to reboot the cloud .