Unibox User Guide

An intelligent Network Access Controller

Wifisoft Solutions Private Limited

Publication Date
Aug 31st , 2018

Applicable Products

The administration guide applies to the following products –

- UniBox U50 & U100
- UniBox U200 & U500
- UniBox U1000, U2500, U5000

Disclaimer

WIFI-SOFT SOLUTIONS PRIVATE LIMITED MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Wifi-soft shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for Wifi-soft products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Wifi-soft shall not be liable for technical or editorial errors or omissions contained herein.

Wifi-soft assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Wifi-soft.

Unibox Overview

UniBox is a network access controller and a hotspot gateway that helps network administrators secure and control access to wired or wireless networks. It is used as hotspot controller, network controller and Internet gateway in variety of businesses, hospitality venues, shopping malls, hospitals, schools and colleges, transport venues, enterprises and any place where networks need to be managed. UniBox provides various functions like access control, user management, AAA server, billing system, multi-WAN router, firewall, URL logging, VPN server, AP controller, bandwidth control, reporting/analytics and advertisement.

UniBox can be used for managing public wireless (or wired) networks at Wi-Fi hotspots/ hotzones, campus and public-access networks. It can be used by private enterprises for controlling access to their private networks, isolating and authenticating guest traffic via a splash page, enforce time and usage policies and to allow secure and limited access to BYODs by employing self-registering / requesting for IT approval of their BYOD devices and.

UniBox is an all-in-one gateway controller i.e. it functions both as a firewall and an access controller as well as an authentication and billing server. It implements a captive portal that restricts unauthenticated users from getting access to the network resources e.g. Internet. In addition, it also provides an on-board authentication and billing server to verify the user's credentials and charge the user for using the network.

UniBox can be also deployed with a central authentication and billing (OSS/BSS) server. In this case, UniBox will function in controller-only mode and will use the services offered by the central server. If the hotspot / hospitality operator wants to manage multiple hotspots centrally then UniBox is deployed in the controller mode. It works seamlessly with Wifi-soft's cloud-based management platform – WiFiLAN.

UniBox comes in different models based on number of concurrent users it can handle. The models range from 50 concurrent users to 5000 concurrent users.

UniBox comes with built-in access point controller and NMS system. The AP controller is responsible for controlling and configuring UniMax access points. It also provides a comprehensive NMS system that provides the real-time status and health of each access point.

In addition, UniBox can be deployed to work with wide range of industry standard wireless access points like Cisco, Ruckus, Aruba, DLink, Ubiquiti to name a few and can easily be overlaid in any existing wired or wireless network in a small to large sized networks. The software stack is installed on standard x86 hardware running Linux variant. This makes UniBox very versatile and is capable of scaling to support thousands of users on the network.

Primary functions

UniBox is primarily deployed as a network access controller and hotspot gateway to manage enterprise networks, guest access networks and public Wi-Fi hotspots. It also incorporates various security functions that are useful for managing enterprise networks –

1. **Network Configuration**
   Unibox provides you the ability to interface and monitor your network by providing various network configuration and monitoring options. UniBox is deployed as a gateway so it sits between the private LAN and public WAN / Internet network. UniBox comes with multiple Ethernet ports. Each port can be configured as WAN or LAN port thus giving flexibility to the administrator to create multiple LAN segments or configure multiple WAN connections.
   The WAN port supports various configuration options like Dynamic and Static IP. Multiple LAN profiles can be created and each LAN segment can be configured with a separate DHCP server. In addition, the port can be configured to tag the traffic with VLAN tags.

   Other than port configuration, UniBox provides features like DHCP server and DNS that allows administrator to configure IP addressing and to choose specific domain name servers. Built-in monitoring module, allows to you to monitor all the network elements like wireless access points, IP cameras, POS terminals, etc in the network. The NAT feature provides network address translation and port forwarding thus enabling access to the internet by the guests and BYODs as well as secure access to internal devices from the Internet. Unibox also provides SNMP agents and SNMP traps to interface with third-party NMS systems. Finally the DDNS feature allows administrators to use DDNS services like anyDNS, no-ip etc that allows access to UniBox deployed on a dynamic IP.

2. **Captive Portals**
   Captive Portals are displayed to the hotspot and BYOD users when unauthenticated users try to connect to a Wi-Fi hotspot. The Captive Portal is displayed as a result of redirection of the client on the network. It provides an interface for the user to provide login information and pass this information to the Authentication Server for validation. Unibox provides predefined templates for designing captive portals using the click-and-customize method. Alternatively, administrator can also design the captive portal separately and host it on an external web server. UniBox provides customization of logo, branding, images, text and layout of the captive portals to suit specific branding requirements.

   Captive Portals also provide an option for user provisioning (online registration) by requesting the users to create their accounts using a payment option like credit card or PayPal. UniBox manages the complete end-to-end workflow of the user provisioning process.

3. **MAC Login / BYOD**
   Many businesses, especially for non-manufacturing workforce, are witnessing an explosive demand by the employees to use their own personal devices, like smart phones, tablets and

ultrabooks / laptops to check their emails, access to intranet portals like sharepoint and to have access to a limited number of web applications servers, while 95% use of these personal devices is for Internet access. It is an IT nightmare and most of the time, under pressure from supervisors and higher levels, IT departments are simply allowing these users / personal devices to access the Internet thru company network by having them use the company private wireless networks, though most of these users are not at all malicious, nonetheless, the security posture of the devices and the websites / content some of them accessing thru the company network, has potential for security breaches / work / virus infection to company business servers and other business computers. Unibox allows self-registration of such devices wherein the user of such personal device will request for access from IT department by filling up a short browser based form splashed thru the Unibox, as user tries to go to Internet, and then submits the same over to the IT department, which then approves or otherwise the access and then notify the user via their company email to be of granted access to the limited BYOD network. This process not only allows approved devices on the network, it also allows to take away the access if a device is lost / stolen or if an employee leaves the company and at the same time allows companies to enforce policies, bandwidth caps, content filtering etc.

4. **User Authentication and Tracking**
   Once the user, say an education/residence environment, is provisioned in UniBox, s/he can use the captive portal to gain access to the network. This involves AAA (Authentication, Authorization and Accounting) services from the RADIUS server. This service is responsible for validating user's credentials and providing access to the Internet and any limited internal web / application servers if so allowed. It also performs accounting function by collecting the CDR/session records for each user. UniBox running in local authentication mode run an internal AAA server that is responsible for all the AAA services on the network.

5. **Billing**
   UniBox comes with a comprehensive billing module that allows administrators to configure different billing plans, create access codes, perform credit card clearing, interface with PayPal and generate revenue reports. Most US credit card payment gateways are supported, and other country payment gateways can be helped with, if there is sufficient demand.

6. **Bandwidth control**
   UniBox comes with many bandwidth control tools that allow administrators to effectively manage bandwidth among the users. It provides options to enforce group-level or per-user level bandwidth control rules to ensure optimal use of the network bandwidth.

7. **Policy Management**
   UniBox provides wide range of policies to restrict usage, enforce fair usage and identify misuse of the network. These policies can be applied to group of users and tracked by the administrator on a regular basis.

8. **Traffic Management & QoS**
   UniBox offers various tools to effectively manage and control the data usage on the network in addition to maintaining QoS. Traffic management can be done at different levels like group of users, per user, per application or port or a subnet of IP addresses. UniBox provides different policies to enforce fair usage on the network or penalize users who are misusing the network traffic.

9. **Reporting and Analytics**
   Extensive reporting capabilities allow administrators to keep watch on all the activity on the network. UniBox also analyzes the data collected from the users and display analytics like usage trends, OS/Devices used, top users, etc.

Important Concepts

1. **RADIUS (AAA)**
   RADIUS stands for Remote Authentication Dial-In User Service. The protocol is defined by IETF (Internet Engineering Task Force) and is described in detail in RFC 2865 and RFC 2866.

2. **Captive Portal**
   Captive Portal (AKA – login or landing page) is the page that enforces authentication on the network managed by UniBox. The Captive Portal can be either hosted inside the UniBox or can be hosted on an external web server.

3. **Bandwidth Control**
   Bandwidth control mechanisms are required to control the bandwidth for each user on the network. UniBox offers various bandwidth control functions to help the administrators regulate the bandwidth usage and punish the users who hog the bandwidth.

4. **User Provisioning and Management**
   UniBox provides completely automated mechanism for provisioning users on the public networks like Wi-Fi hotspots. Unauthenticated users are presented a registration page to create an account online. The registration page may offer billing plans for paid hotspots or UniBox also allows administrators to add user's account directly in the system.

   User accounts created are generally associated to a particular groups, policies or plans. Users Internet usage can be restricted based on the plan or groups they belong. Unibox allows you to configure various restrictions for each user like Session timeout, Concurrency Limit, Idle Timeout, Upload/Download Rate, Daily Upload/Download Quota, Sessions per day and Usage Quota.

   Unibox does comprehensive accounting of each user which provides you with details like Start time and End time of Sessions, Duration, MAC Addresses, Upload/Download Data Size per session and the session termination reason. It also maintains Agent and Authentication history which provides you information about user's browser, OS, IP/MAC addresses, login timing, bandwidth usage and more. Administrator also has a privilege to expire, suspend or activate users or even disconnect the user from the network. Finally the user's activity and authentication history can be exported to a PDF or Excel file to analyze it further.

5. **Billing**
   For a paid network like Wi-Fi hotspot, it is necessary to provide online payment option to the end-users. The billing system allows administrators to charge credit cards, interface with PayPal, define billing plans, view transactions and configure the payment gateway details. Before enabling billing, administrator needs add the payment gateway settings in UniBox.

When the user registers for a new account, UniBox passes the credit card details to the payment gateway for processing. If the card is charged successfully, the user's account is created in subscriber table and user is given access based on the billing plans he selects.

Similarly, administrator can create different types of prepaid (access) codes or PINs which can be exported or printed in a business card sized format for distribution. The end user can enter the prepaid code on the portal page and gain access to the network (Internet) for the allotted time or bandwidth.

6. **SMS Based Login**

SMS based login employs two-factor authentication process (also known as OTP – one time password) to validate the user with his/her mobile number. With the rise in cyber crimes, many countries require that hotspots operators validate the user's mobile number at a public WiFi hotspot. SMS based login helps these operators to comply with this requirement. Additionally, this process also allows the operator to collect mobile/cell phone numbers for marketing and promotional activities.

How does it work?

When the customer visit your WiFi Hotspot, s/he will see a login page (Captive Portal) requesting them to enter her/his mobile (cell) number. Customer enters the mobile number along with the other optional details like personal information, email, preferences, etc. On receiving the information, UniBox sends a SMS with a login code (randomly generated) to the registered Mobile Number. Customer needs to enter the code on the login page to gain access to the Internet. UniBox provides different variants to this process to allow operators to implement different business models on the network.

7. **Social Media Integration**

Social media is a network of all people who get together as a society over the Internet and connect with each other for sharing information, knowledge, news, events etc. We have number of popular social networking websites like Facebook, Twitter, Google and LinkedIn.

There is a rising trend to capture social media information for the users who access Wi-Fi at public hotspots. Most of the social media websites provide rich API to retrieve user's profile that is extremely valuable to companies for profiling users, understanding user trends and building marketing strategies. For end-user's perspective, the users don't need to remember username and password for each hotspot. Instead they can just use their Facebook ID to gain access to the hotspot.

UniBox provides different options to validate user's credentials using their social media profile. It also seamless collects the user's public information to generate analytics and trends.

8. **Activity Logging (URL Tracking)**

Activity logging means tracking the user browsing activity and logging the URLs the user visits while using UniBox managed network. This is an optional feature and can be activated on need basis. When activated, UniBox starts keeping track of the Internet activity for the user and logs the activity in a database. Administrators can generate various reports or use the search tool to find URLs visited by a user on the network. Additionally administrator can log and archive the information centrally by streaming the information to a remote server. This may be required for regulatory compliance.

9. **Network Monitoring and Alerts**

   Monitoring allows administrators to check the health of all the network elements like access points, switches, cameras, printers, etc inside the network. It monitors each element periodically to ensure that the connectivity is intact. If an outage is detected, an alert is generated and sent to the right person so a repair work can be carried out before the end users get affected.

UniBox Models

UniBox is sold in three standard variants –

SMB Models

Models Available : U50 and U100

These models are ideal for small to medium networks that support up to 100 concurrent devices. They are generally deployed for small hotspots in cafes, retail shops, small offices, motels, etc. The models are available in a small, compact enclosure and is powered by a separate 12V DC adapter. It supports 3 gigabit Ethernet ports.

Enterprise Series

Available Models: U200 and U500

This model is ideal for medium sized networks and is capable for support up to 200 to 500 concurrent devices. This UniBox is ideal for medium venues like hotels, motels, shopping plaza, training institutes, medium sized businesses, etc.

Campus Series

Available Models: U-1000 and U2500

These models are designed for high-traffic, large networks and is capable of handling up to 1000 concurrent users. The model comes in 1-U form factor and comes with 6 gigabit ports. It is ideal for larger venues like large hotels, schools/colleges, enterprises, etc

Large Campus Series

Models: U5000

These models support large number of concurrent users and provides high throughput. It comes with 6 gigabit Ethernet ports and 2 SFP+ ports. It is ideal for very large venues like convention centers, universities, airports and large enterprises.

In addition, you can also order custom model for networks that have more than 5000 concurrent users or where there is a need for a redundant power supply and redundant LAN side connections for hook up to a stack of enterprise switches or two core enterprise switches, for better resiliency. For large scale and critical operations, it is recommended to deploy a pair of controllers in active / passive mode. The configuration from the active can be backed up along with the user database to the passive unit (not suitable for hospitality operations, because of dynamic nature of guest accounts, but a spare unit with configuration restored and user accounts recreated or in case of external radius server hosting such accounts will work. Table on the next page shows the complete list of Features, Hardware Specifications and Software Specification for each model.

Feature Description	Unibox 150	Unibox 250	Unibox 550	Feature Description	Unibox 150	Unibox 250	Unibox 550
Network Interfaces				**Billing Options**			
Ethernet ports	2	4	4	Credit card billing	✗	✓	✓
USB ports	2	4	4	PayPal Integration	✓	✓	✓
Wi-Fi	✓	✗	✗	plans	✓	✓	✓
Authentication				Prepaid Coupons	✓	✓	✓
Built-in AAA server	✓	✓	✓	Custom payment gateways	✗	✓	✓
RADIUS client	✓	✓	✓	**Subscriber Management**			
IP/MAC binding	✓	✓	✓	Subscriber provisioning on captive portal	✓	✓	✓
authentication	✓	✓	✓	MAC Binding	✓	✓	✓
Captive Portal	✓	✓	✓	Administrator approval	✗	✓	✓
links/Whitelisting	✓	✓	✓	Temporary suspension	✓	✓	✓
WISPr compliant	✓	✓	✓	Time & Bandwidth quota	✓	✓	✓
Networking				**Activity Logging**			
Static & Dynamic Routing	✓	✓	✓	Logging each user session	✓	✓	✓
Multiple WAN options	✓	✓	✓	Tracking visited URLs for each user	✗	✓	✓
Layer-2 isolation	✓	✓	✓	Monitoring user port activity	✓	✓	✓
NAT/Port forwarding	✓	✓	✓	logs	✓	✓	✓
DHCP server	✓	✓	✓	**Caching**			
SNMP Traps	✗	✓	✓	Caching web pages for faster retrieval & bandwidth optimization	✓	✓	✓
3G/4G support	✓(addon)	✓	✓	URL Filtering	✓	✓	✓
Concurrent Users	50	200	1000	URLs	✓	✓	✓
Bandwidth Management				**Captive Portals**			
Policy Based Access	✓	✓	✓	Branded captive portals with multiple login options	✓	✓	✓
User and Group policies	✓	✓	✓	portal	✓	✓	✓
Time based access policies	✓	✓	✓	Advertisements on captive portals	✗	✓	✓
Fair Usage Policy	✓	✓	✓	SSL certificates	✓	✓	✓
Per User bandwidth mgmt	✓	✓	✓	**Traffic Analysis**			
Monitoring				Detect users with torrent & P2P traffic	✗	✓	✓
24x7 monitoring of each internal network element	✓	✓	✓	Apply policies to offending users	✗	✓	✓
Up/Down Alerts	✓	✓	✓	ports	✗	✓	✓
Google map integration	✓	✓	✓	Generate real-time & historical reports	✓	✓	✓
Reporting				**Administration**			
Online user statistics	✓	✓	✓	Web based management	✓	✓	✓
Historical usage reports	✓	✓	✓	Role based access to management port	✓	✓	✓
graph	✓	✓	✓	Remote Syslogs	✓	✓	✓
Graphical analysis of upstream (ISP) bandwidth	✓	✓	✓	Multi-language support	✓	✓	✓
Revenue Reports	✓	✓	✓	Configuration backup	✓	✓	✓
Hardware				**Physical Dimensions**			
Processor	AMD Geode LX800	Intel Atom	Intel Core2-Duo	Form Factor	Standalone (fanless)	1-U rackmount	1-U rackmount
Memory	256 MB	1 GB	2 GB	Dimensions	176 - 174 - 30 mm	17" - 1.7" - 9.8"	17" - 1.7" - 9.8"
Storage	4/8 GB CF	250 GB SATA HDD	250 GB SATA HDD	Net Weight	0.5 kg	4.5 kg	5 kg
Input Voltage	12V DC	100 - 240 V	100 - 240 V				
Power Consumption	5 W	200 W	250 W				

Installation

This section explains how to install UniBox in your network. UniBox needs to be deployed as a network gateway so it is installed between the LAN and WAN network. UniBox is always shipped with two or more Ethernet ports. The photos below display the various components of two UniBox variants – standalone unit and 1U server unit.

Standalone Unit

UniBox U50/U100

UniBox U-100 standalone unit comes with three Ethernet ports, serial port, two USB ports and a power jack. The photo shows the various connectors available to the user. The LAN port needs to be connected to your private network that UniBox will manage. The WAN port needs to be plugged into your Internet (WAN) connection.

<<Image here>>

UniBox U-200

UniBox U-200 standalone unit comes in 1U form factor with 4 Ethernet ports, 2 USB ports, serial port and power jack. The photo shows the various ports available on UniBox U200. Any port can be configured as WAN or LAN port. The admin can create multiple WAN profile and then assign these profiles to multiple Ethernet ports. If multiple WAN ports are assigned, then UniBox will be automatically configured for load balancing and failover.

Similarly any port can be configured as LAN port and multiple LAN profiles can be setup and assigned to physical LAN ports.

UniBox U-500 /U-1000

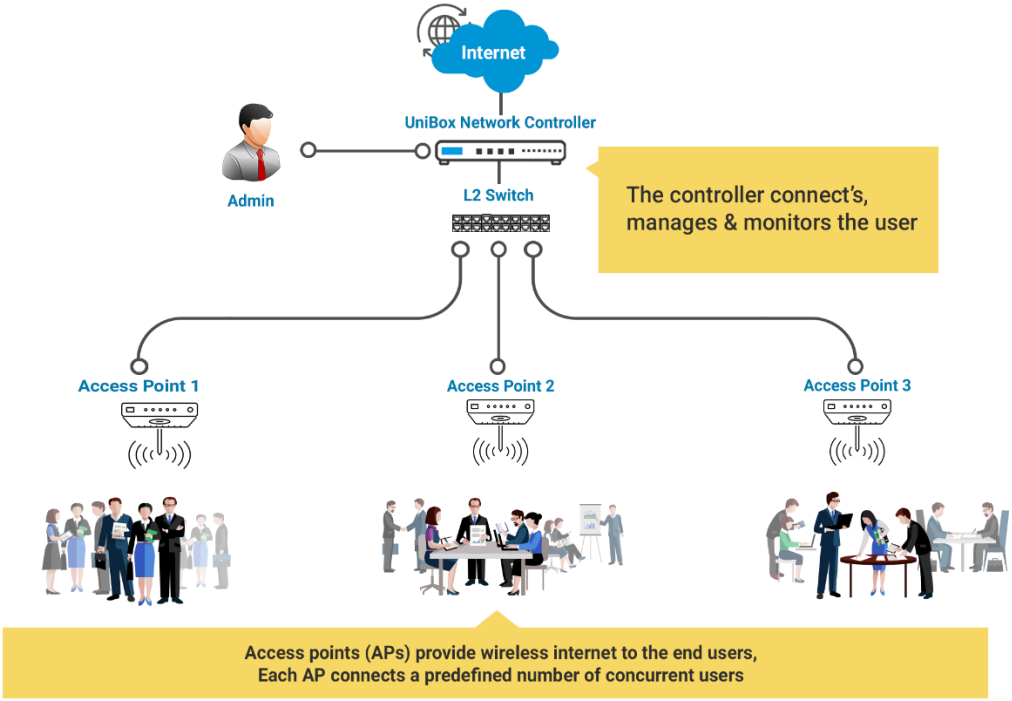
UniBox U-500 / U-1000 models comes with a 1U form factor and is generally installed in a server rack. The unit comes with 6 Gigabit Ethernet ports. The admin is free to chose any port as LAN or WAN port. Depending on client requirements, the U500 or U1000 might also come with 2 SFP+ ports. These ports can be assigned LAN or WAN profile depending on the client requirements.

Network Deployment

The diagram below shows a simple deployment scenario for UniBox. It is generally deployed as a hotspot gateway/controller within a wired or wireless network. In case of a wireless network, several access points are deployed across the venue to provide adequate signal coverage to the users. These access points are connected centrally into a POE switch using CAT-5e cables or via Power injectors. The LAN port of UniBox is plugged into the switch. The access points are usually configured in bridge mode thus allowing the clients to directly communicate with the UniBox. UniBox is responsible for assigning IP addresses on the network. It also functions as gateway for all the clients on the network. The WAN port of UniBox is connected to the WAN circuit. Administrators can place a firewall in between UniBox and the Internet if desired. Otherwise the WAN port directly connects to the modem. The WAN settings are programmed in UniBox.
When authentication is enabled, each user needs to provide the correct login credentials in order to access the Internet. UniBox also performs many other functions like bandwidth control, activity tracking, caching, content filtering, policy management, etc. In short, UniBox provides administrator with complete control on the network.
We will go through various scenarios in which Unibox can be deployed. Lets start with Simple Unibox Deployment Scenarios (UDS1).

UDS1: Unibox Deployment Scenarios 1 – Simple Deployment

Description: An Internet connection to Unibox (WAN Port) via Firewall and then spreads out internally through different Access Points (AP's) connected to Switch which is further connected to Unibox (LAN Port). End User connects to the various Access Points and goes through the Unibox before they browse the Internet. Diagram below shows detailed deployment of Unibox.



Feature Summary

Networking

This section allows administrators to configure the network settings of UniBox. These settings are needed to configure the WAN and LAN ports of UniBox and other network related parameter. Following items can be configured –

1. Port settings – Configure IP settings for WAN and LAN ports.
2. DNS server – configure the primary and secondary DNS servers
3. DHCP server – UniBox runs a DHCP server that issues IP addresses to the clients connected on LAN ports.
4. IP Routes – configure the default and additional IP routes for the Internet traffic
5. NAT – configure network address translation rules to allow port forwarding functions
6. Device Monitoring – configure network devices like access points, switches, router, etc for monitoring and view the monitoring results
7. SNMP – configure the SNMP agent and traps
8. Dynamic DNS – Configure Dynamic DNS in case Unibox WAN port IP Address is dynamic and changes frequently. Dynamic DNS helps you to resolve Unibox Hostname even if your WAN IP address is changing frequently.

Authentication

UniBox provides a redirect function whereby the network user is redirected to a captive portal before getting access to network resource like Internet. UniBox also provides a local authentication mechanism to authenticate the users via the RADIUS server. In addition, the administrator can also configure UniBox to authenticate users via an external RADIUS server.

Bandwidth Management

Bandwidth management is increasingly an important function for public access networks – wired or wireless. With the explosive growth of online video and rich-media applications, there is increasing demand for bandwidth and allocating fair bandwidth among users has become extremely important.

UniBox provides several bandwidth control mechanism and policies to regulate the bandwidth for each user. This allows administrators to implement fair usage policy among the users and not allow anyone to hog the bandwidth.

Policies

UniBox implements various policies to control access and bandwidth of the online users. Administrators can categorize users into various groups and apply the policies on a group basis. The policies help the administrator implement fair usage, penalize users or limit bandwidth for each user.

Captive Portal

Captive portal is the first page the users see when she connects to the network. The captive portal is used to identify the user before the user gets access to the network resource like Internet. The captive portal can be either hosted on UniBox or it can be loaded from an external web server. UniBox provides a simple, template-based captive portal design that the administrators can easily customize with the company branding.

The external captive portal provides administrators much more flexibility and control on the design and layout of the web page.

Billing

Billing is an important function for Wi-Fi hotspots. UniBox provides a billing engine that gets seamlessly integrated with the captive portals. Billing can be done either using access (prepaid) codes or using credit card or PayPal. Administrators can define various billing plans in the system and offer the billing plans to the guest on the captive portal. Alternatively she can also generate batch of access codes and distribute them to the end users. Billing section also generates various reports to track the monthly revenues from the hotspot.

Reporting

Reporting is an important function of UniBox since administrator can retrieve various reports on usage, revenue and health of the network. The usage reports are used to check the bandwidth usage, online time and other details of the users. The billing reports provide information about the revenue generated from the users. The reports can be downloaded in Excel or PDF format for archiving or further processing.

Subscriber Management

If administrator configures UniBox to use on-board RADIUS server for user authentication then the user database is stored locally in UniBox database. UniBox provides comprehensive interface to manage the user information.

Monitoring

UniBox can be used to monitor the health of the wired or wireless network. It provide a monitoring service that can be used to check whether the network devices like switches, access points, routers, firewalls, etc are online and the connectivity is intact. UniBox can send alerts to the administrators in case there is an outage to avoid lengthy downtime for the network users.

Administration

UniBox provides multiple administration account and each one can be configured with custom access control rules. This ensures that the administrator can provide adequate access to UniBox data based on the user privileges

Interfaces

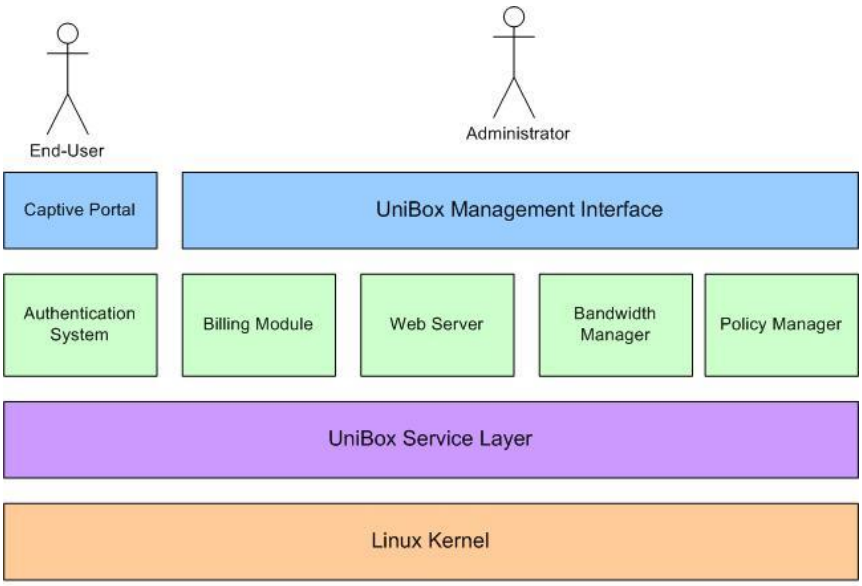
Depending on the model, UniBox provides multiple Ethernet ports. Each UniBox has at least two Ethernet interfaces – LAN and WAN.

Technical Overview

Architecture

UniBox is built on robust and scalable software architecture to ensure a reliable, round-the-clock performance. UniBox firmware runs on the latest Linux kernel and is compatible with any x86 hardware platform. This provides UniBox a lot of options for deployment. Technically, it is possible deploy UniBox firmware on a custom designed x86 server to support more than 5000 users.

The software architecture for UniBox is as shown –



UniBox System Architecture

Menu Summary

UniBox offers the following menu options to the administrators. Some models may not have the menu options. Please refer to your admin console to check the menu options available for your model.

Network

- WAN
- LAN
- VLAN
- Interfaces
- DNS
- VPN
- Monitoring
- DDNS
- IP Routes
- Routing

Wireless

- Heatmaps
- Manage APs
- Clients

Authentication

- Controllers
- Groups
- User Management
- Passthrough
- Portals
- SMS
- MAC Blacklist
- External Services

Control

- Policies
- Content Filter

Advertisement

- Category
- Ads
- Campaign

Billing

- Plans
- Payment Gateway
- Billing Configuration
- Transactions

- Email Templates
- Email Relay
- Vouchers
- PMS

Tools

- Diagnostics Tools
- Remote Syslogs
- User Activity Logs
- Event Logs
- Conntrack Logs

Reports

- Online Users
- User Agents
- SMS
- Social Media
- System
- Usage
- Billing
- Advertisement
- Monitoring
- Automated Reports

Admin

- Accounts
- Profile
- License
- Configuration
- Approvals
- Time
- Reset
- Reboot
- Power Off
- Logs

Getting Started

Before you deploy UniBox, you need to setup your wireless or wired network and need to provision your Internet connection from the local Internet service provider. UniBox functions as a gateway on your network so it is deployed between the WAN and LAN portion of your network. You may also deploy UniBox in the DMZ along with the firewall.

In case of a wireless network, the LAN portion connects to a switch or an access point. The switch aggregates the traffic from various wireless access points and feeds it into UniBox. UniBox runs a DHCP server to lease IP addresses to all the clients on the LAN.

The WAN port is usually connected to the modem or router provided by the ISP. In case the network has a hardware firewall, UniBox is generally deployed after the firewall.

The diagram below shows the rear view of UniBox.

<<UniBox Image>>

The administrator can designate any port for WAN port. Generally the first port (ETH0) is considered as the default LAN port. All the other ports are not configured. Administrator can configure other ports as LAN or WAN port depending on their requirements.

The LAN port is accessible at 192.168.100.1 and subnet mask is 255.255.255.0. It runs a DHCP service so when you connect your laptop the LAN port, it should issue you an IP address in the 192.168.100.x range.

If you are unable to access the LAN port, please reset the UniBox and retry. Alternatively you can also configure static IP address on your laptop to connect it to the LAN port.

1. Configure NIC of your Laptop or desktop to have following network configuration (Unibox LAN port by default has 192.168.100.1 IP address):
    a. IP Address: 192.168.110.2
    b. Subnet Mask: 255.255.255.0
    c. Gateway: 192.168.100.1
2. Connect your Laptop with the network interface you just configured by using standard Ethernet CAT 5 cable (Patch Cord) to the LAN port of Unibox (Refer to screenshot above to know Unibox LAN port)
3. Open your browser (I.E., chrome etc.) and browse the URL http://192.168.100.1
4. Once you load the Unibox User Interface, login with Admin credentials i.e. Username: admin and Password: admin. Enter the correct captcha value you see on the page.
5. Connect cable coming from your ISP connection to the other port of Unibox.
6. If it is a Static connection you need to have WAN Port configuration details like IP addresses, Subnet mask and Gateway from your ISP which can be used to configure your Unibox WAN port after it is set to Static. For Dynamic connection your WAN port gets the network configuration parameters automatically from your ISP once it is connected. You need to set you WAN to Dynamic mode in that case. In case of PPPoE connections also, you need to get the WAN port configuration parameters values from your ISP and then you can set your WAN port to either PPPoE mode before you enter the configuration parameters.

7. You should now be able to browse internet. Disconnect your laptop and connect Ethernet switch (Number of Ports on your switch will depend on the number of access points you have and the number of clients you want to connect to your Hotspot).
8. You can now connect either your access points or the client systems to the switch. In case you connect access point, end will connect to Unibox via access points.
9. You can connect you System/Laptop to the switch you just connected, access the Unibox user interface by browsing URL http://192.168.100.1 and continue configuring and customizing Unibox based on your Hotspot Requirements.

1. DASHBOARD

The dashboard gives an overall view of the status of the UniBox. It displays the status of all the important features present in the UniBox, which might be helpful in discovering any failure in the working of the UniBox and hence be able to repair and rectify the problems that rise up.

The dashboard represents the information in two ways,

1.1 Tabular Dashboard

The tabular dashboard gives a view of:

- **Services** – The statuses of all the services provided by the UniBox are displayed. This allows an admin to know if there are any services that do not function as they are supposed to.
  - If the status of the services show a 'Thumbs-up' icon ( ), then it indicates that the services are functioning without a hitch.
  - If the status of the services show 'Thumbs-down' icon ( ), it indicates that there may be some problem with the functioning of the services.

- **Status** – The statuses of all the configured features are displayed. If the status against a feature shows as a 'thumbs-up' icon , then it indicates the proper functioning of the respective feature. Similarly, if the status of a feature shows the 'thumbs-down' icon, then it indicates certain discrepancies faced by the feature and needs to be looked into.

  Also, the features that are not configured, cannot have a status. So, an icon ( ) representing the 'not configured' state of the feature is displayed against the respective feature.

- **Other Information** – This displays all the information related to the UniBox device. The dashboard shows the information related to the device, that includes the number of online users or devices, the current time, the uptime of the system, the controller model and the serial number. To get a detailed information about the device, click on the **details icon** provided there. See.

- **Event Information** – This information lets an admin know the number of issues that have been logged into the system. The events or issues are segregated based on the different types of severity, namely, critical, warnings, errors, alerts, and logs. To know more about the events, click on the **details icon** that has been provided.

- **Interfaces** – All the interfaces configured in the UniBox displayed here, along with their data rates. The rate at which the packets are received and transferred is displayed along with the total rate. To see the details of all the profiles, click on the **details icon** provided.

- **Controller** – This displays all the controllers that have been configured in the UniBox with their active status. If the status of a controller shows the 'thumbs-up' icon, then it indicates the controller is working perfectly. Similarly, if a controller has issues or problems, then the status is indicated by the 'thumbs-down' icon. Clicking on the **details icon** will display the detailed description of the controllers.

- **WAN** – The WAN profiles defined in the UniBox are displayed, giving their current status. The status of a WAN profile is indicated by a 'thumbs-up' icon, if the WAN interface is functioning properly. At the same time, if the status of a WAN interface is indicated by a 'thumbs-down' icon, then there is a problem or the WAN interface is currently down.

- **AP Status** – This gives an overview on the status of all the APs configured in the UniBox. The AP status displays the number of access points that are UP or DOWN, the number of unknown APs and also the number of wireless clients. Unknown APs are the APs that are discovered in the network but not yet configured. To get a detailed information on the APs, click on the **Details icon** provided, which will redirect the admin to the AP management section, allowing him/her to view, configure, edit, and delete the APs.

- **RAM** – The information on the RAM size of the system is displayed. This shows the total RAM size, the amount of RAM used, the size of RAM that remains free, and also the amount of RAM that has been assigned as swap space. To get more information, click on the **details icon**.

- **CPU** – The status of the processor is displayed. It shows the amount of the processor being consumed by the users and the system, in percentage. Also the percent of the processor kept idle and some other information.

- **Storage** – The total storage of the system is displayed along with the amount of space used and also the remaining free space available.

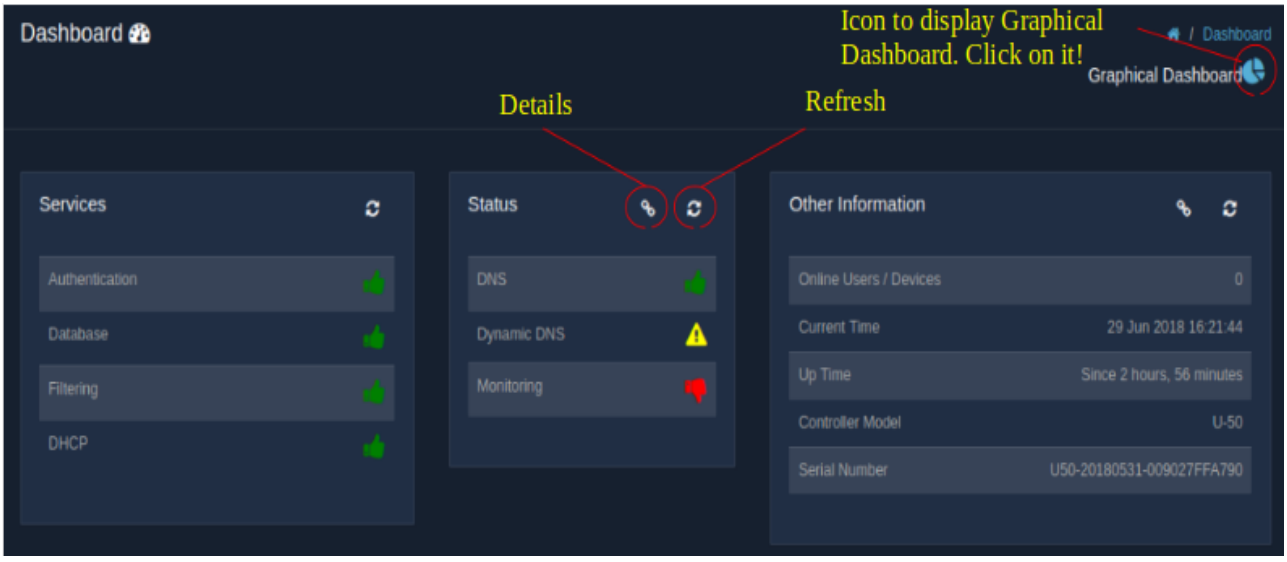


Fig. 1.1(a)

Fig. 1.1(b)

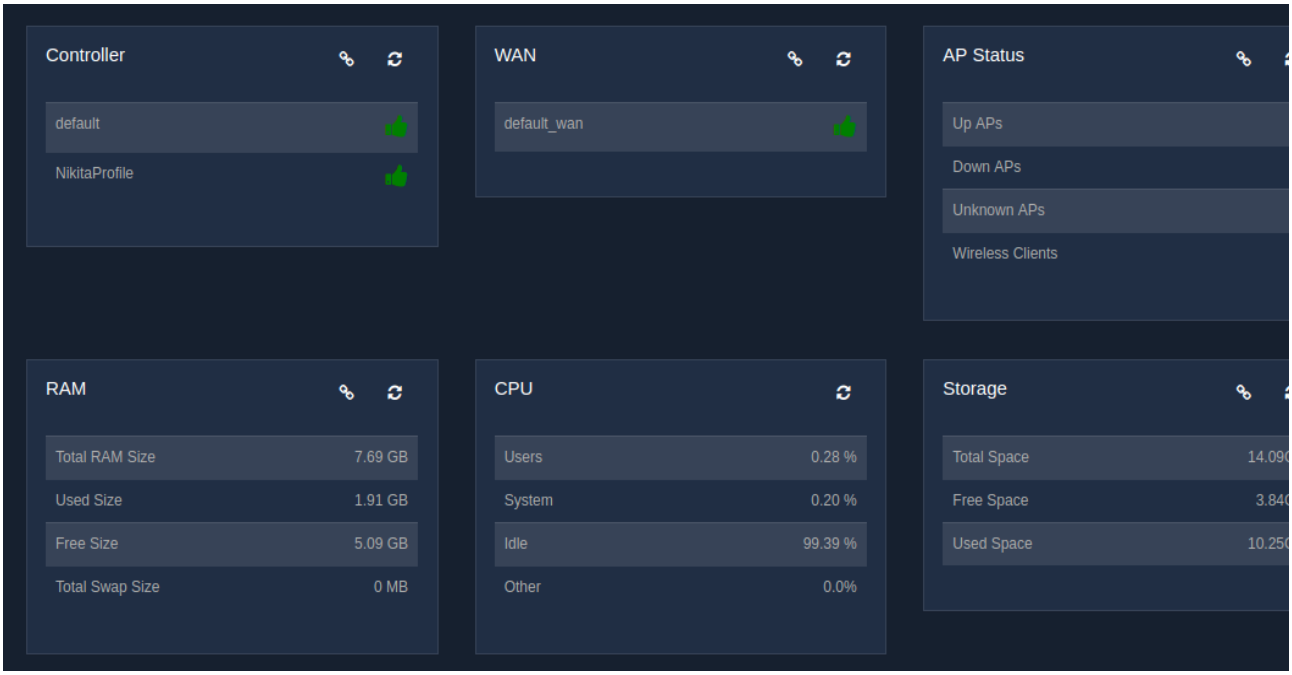


Fig. 1.1(c)

1.2 Graphical Dashboard

The graphical dashboard gives a statistical view of:

- **Users** – This displays a user versus time graph of connected and online users. The graph displays the daily statistics of the users on a timely basis.

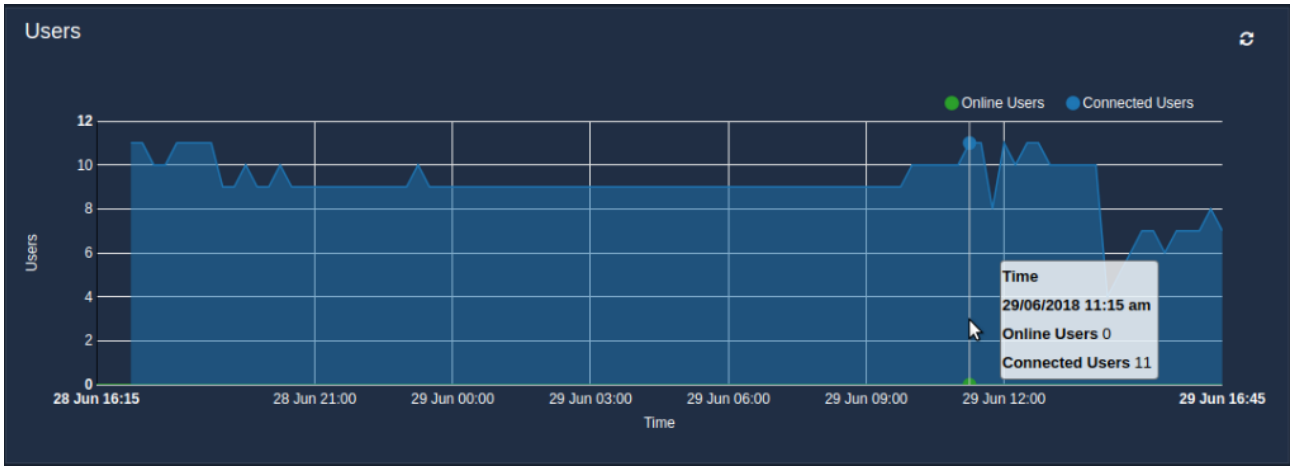


Fig. 1.2.1

- **<u>Bandwidth Usage</u>**:

  - <u>LAN</u> – This graph shows the daily bandwidth (download and upload rates) consumed by the LAN ports over the given time period.

  - <u>WAN</u> – The bandwidth (upload and download rates) passing through the WAN ports is represented in a graphical form on a daily basis.

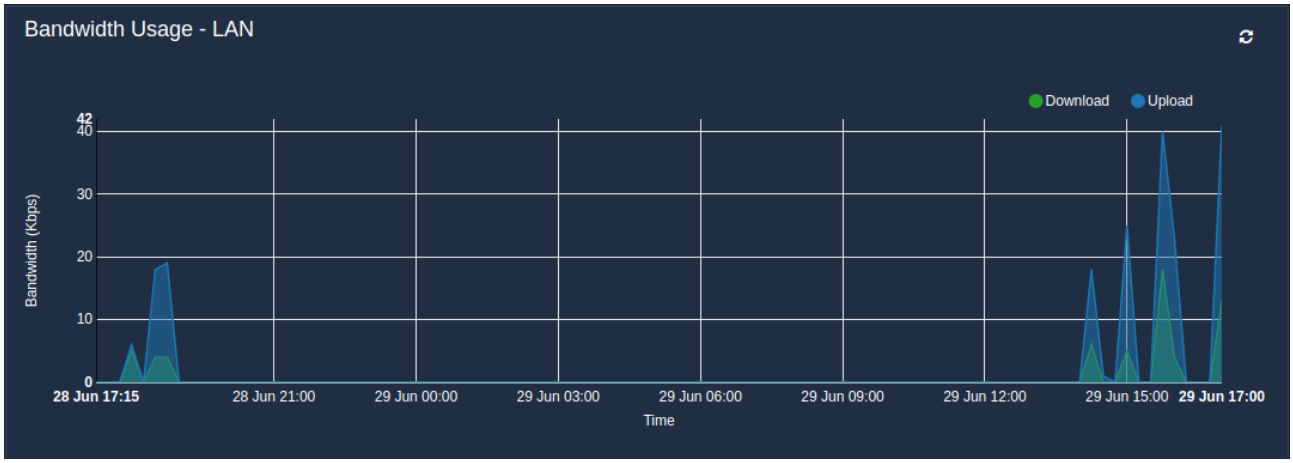


Fig. 1.2.2(a)

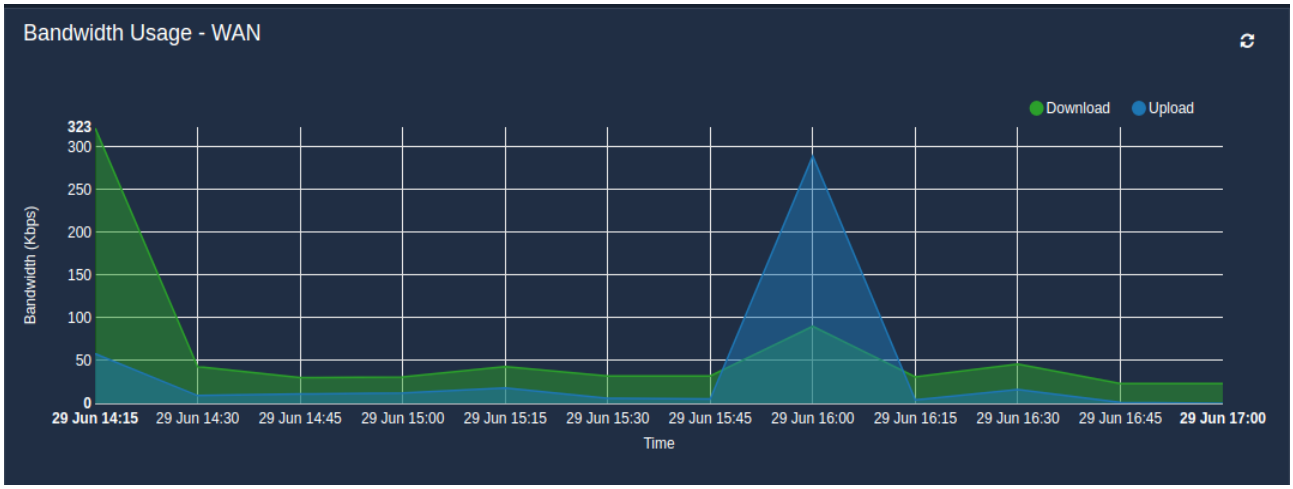


Fig. 1.2.2(b)

- **<u>Internet Bandwidth</u>** – The graph displays the upload and download speed of the Internet connection from the ISP, that has been noted down every three hours over 24 hour period.

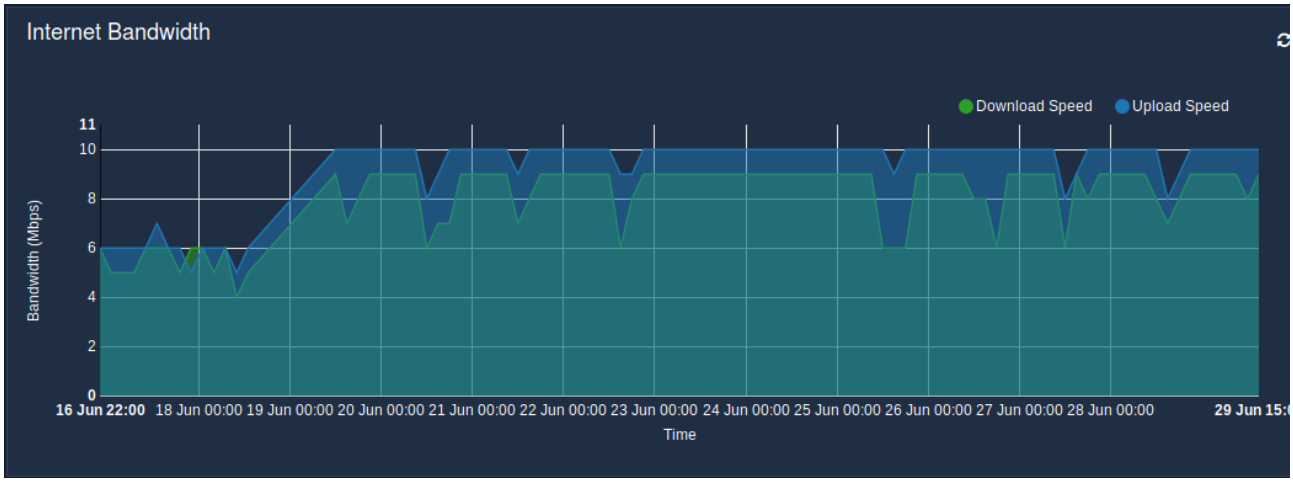


Fig. 1.2.3

- **<u>Port Connections</u>** – The number of opened ports over 24 hours is represented in the graphical form. The opened ports are either destination ports or source ports.

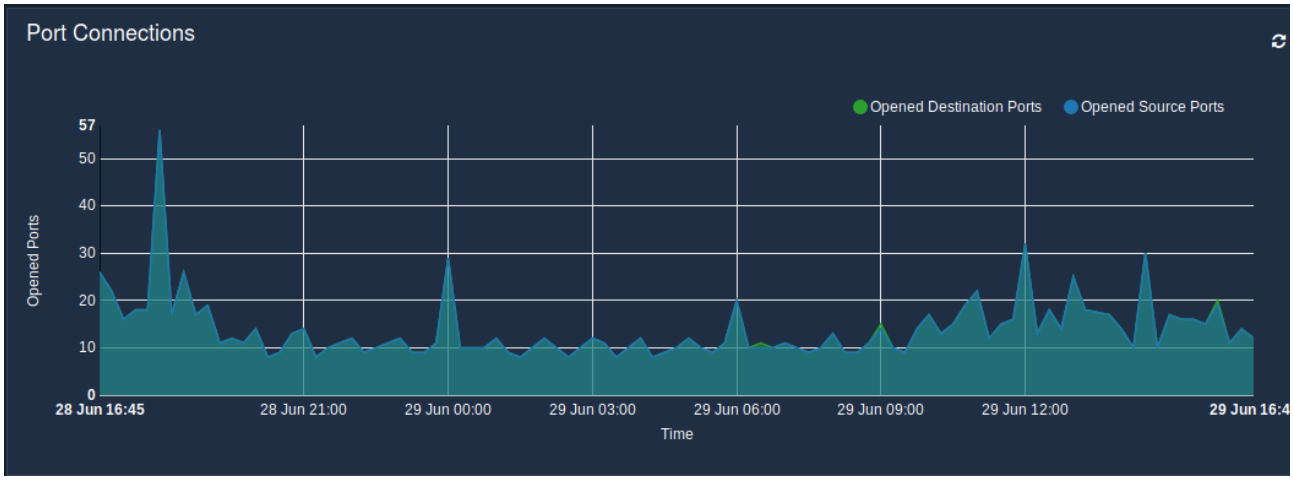


Fig. 1.2.4

- **<u>Section</u>**:
  - <u>Memory Section</u> – The pie chart displays the amount of memory used and also the amount of memory that is free and available.
  - <u>Disk Section</u> – The amount of disk space used and the disk space available is represented in the pie chart.
  - <u>CPU Section</u> – The pie chart represents the percent of the processor that is active and also the percent of the processor that is idle.

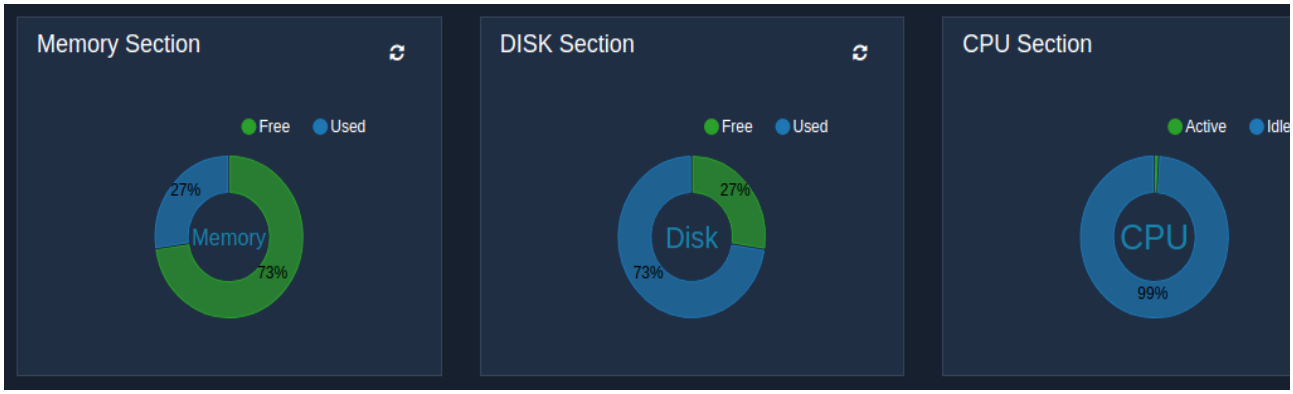


Fig. 1.2.5

<u>Note</u>: To refresh the status of the different entities, click on the refresh icon provided for each entity.

2. NETWORK

2.1 WAN

2.1.1 Create / New WAN Profile

Administrators are allowed to add a new WAN profile. The WAN profile can be either static or dynamic. For static settings, enter the IP address, subnet mask and gateway IP for connection. The changes will take effect after the configurations are applied.

To create a WAN profile, go to the 'WAN' section under the 'Network' module present in the sidebar and click on the '**+**' icon. A modal form is displayed that is required to be filled in to create a WAN profile.

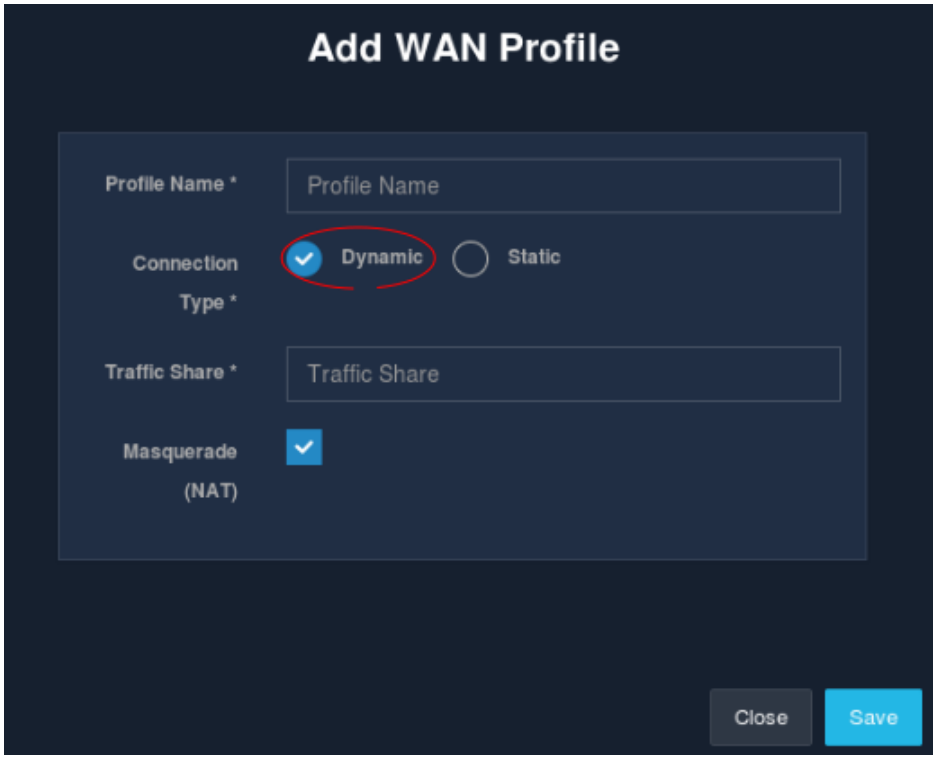


Fig. 2.1.1(a)

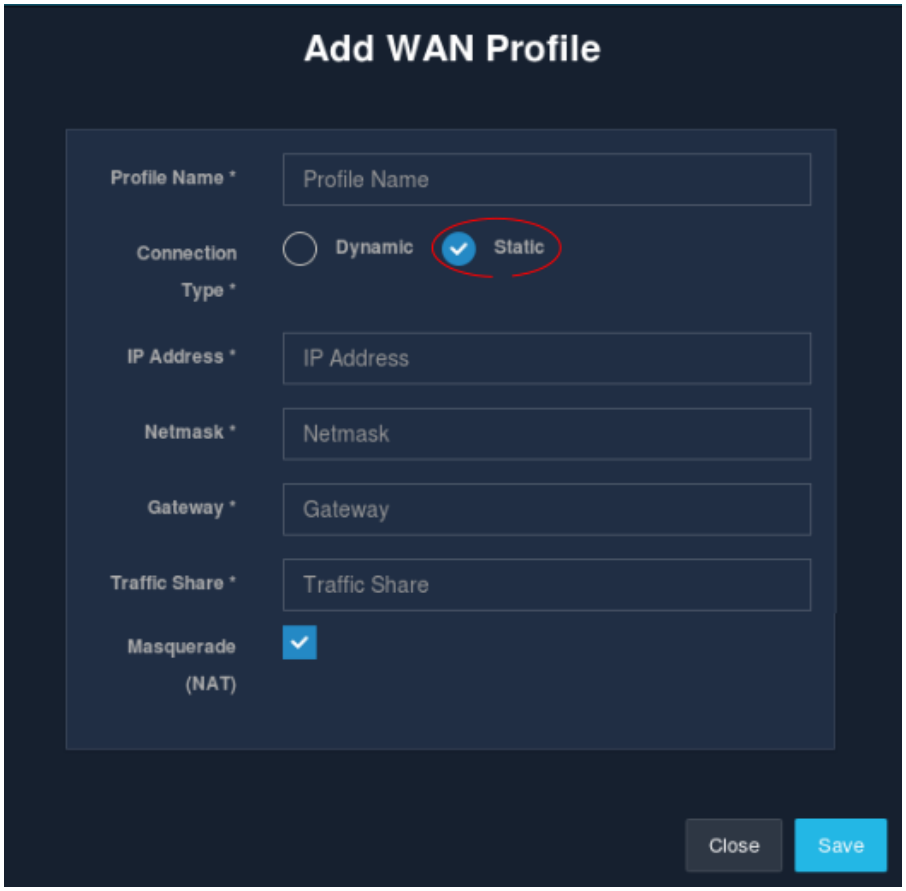


Fig. 2.1.1(b)

Fields	***Description***
Profile Name	Name of the WAN profile.
Connection Type	Select the type of connection, either static or dynamic.
IP Address	Enter the WAN side IP address.
Netmask	Enter the subnet mask.
Gateway	Enter the gateway IP.
Traffic Share	Enter the share of traffic the WAN connection should get. The traffic share will decide the amount of LAN traffic going through the WAN port. If there is only one WAN profile, then 100% traffic will go through the WAN port. For multiple WAN profiles, the value should be less than 100. **Default is 100 percentage.**
Masquerade	Tick the check-box if the WAN connection should masquerade the traffic.

Table 2.1.1

Once the details are filled in, click on the 'Save' button. And there! A new WAN profile is created.

2.1.2 List WAN Profile

WAN profiles define the internet port settings. The list of all the WAN profiles is displayed in a table. The list displays the type of connection, assigned IP address, Netmask, gateway IP for the WAN connection, traffic share along with the profile name. The listing table also contains an 'Operations' column wherein there are options to edit or delete WAN profiles.

To view the list of WAN profiles, go to the 'WAN' section under the 'Network' module in the sidebar.

Fig. 2.1.2

2.1.3 Edit WAN Profile

An admin can make changes to an existing WAN profile settings. To edit a WAN profile, click on the edit icon present in the 'Operations' column in the 'WAN' section of the 'Network' module. A modal form, similar to the one displayed during creation, is displayed to make changes to the already existing settings. Note that if the settings are incorrect, then the WAN side will become inaccessible. Refer.

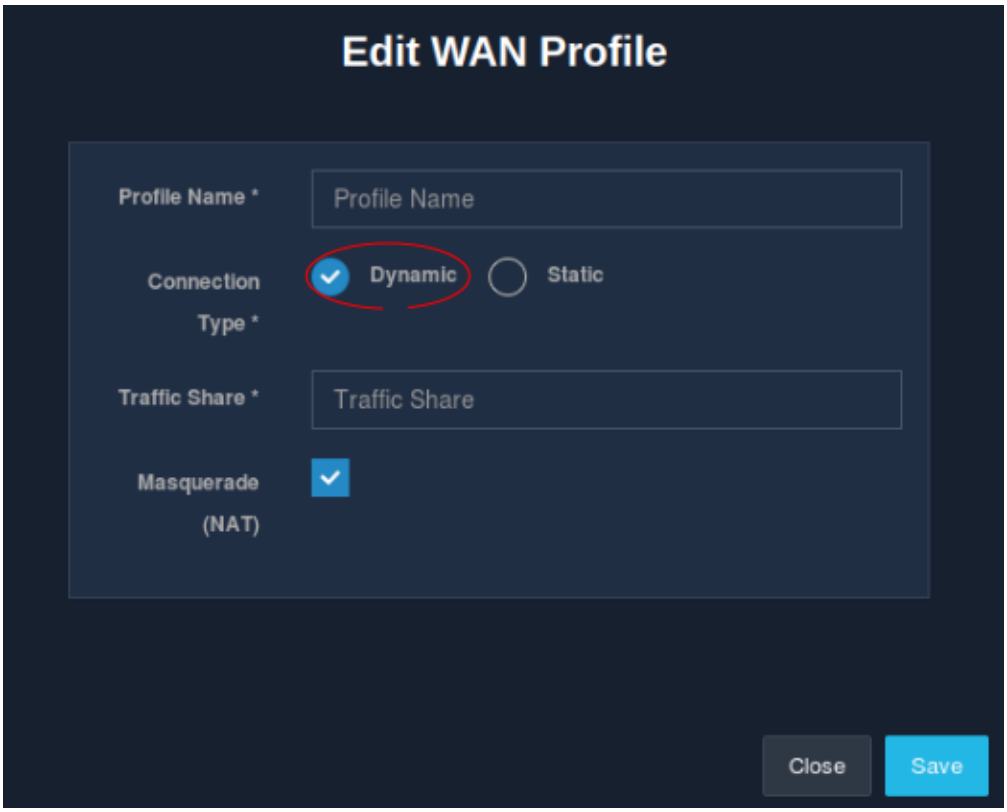


Fig. 2.1.3 (a)

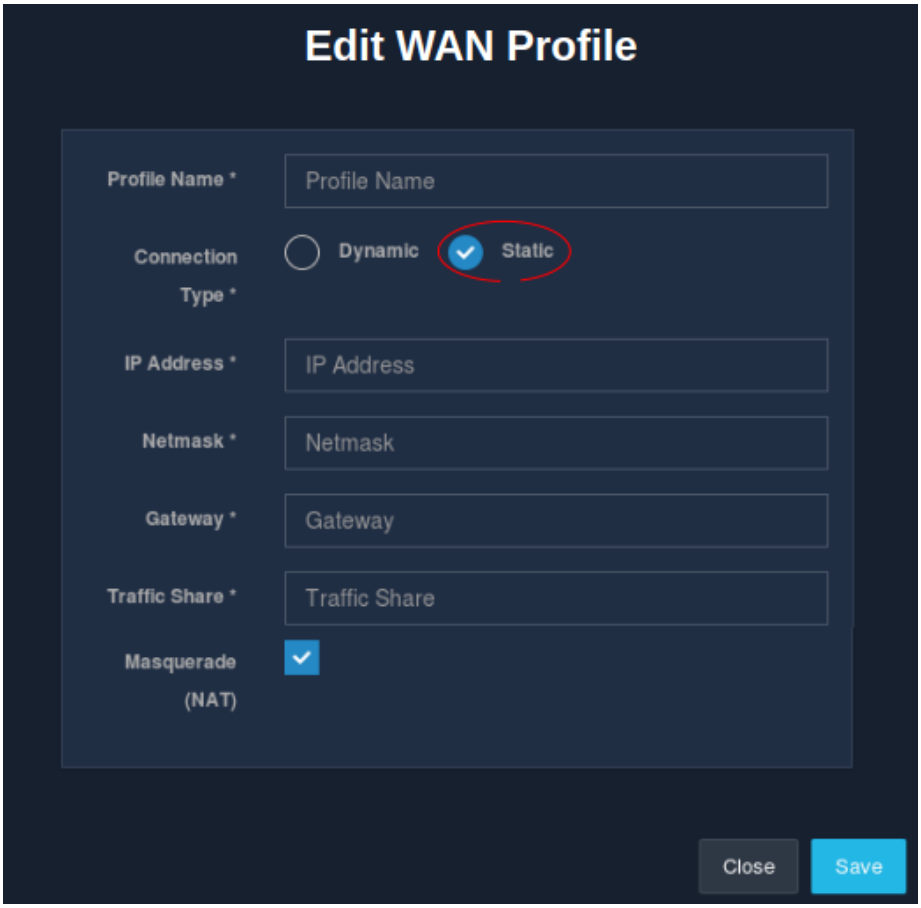


Fig. 2.1.3 (b)

Click on the 'Save' button to apply the changed configurations.

2.1.4 Delete WAN Profile

An admin is given the option to delete an existing WAN profile. To delete a WAN profile, click on the delete icon in the 'Operations' column present in the 'WAN' section under the 'Network' module.

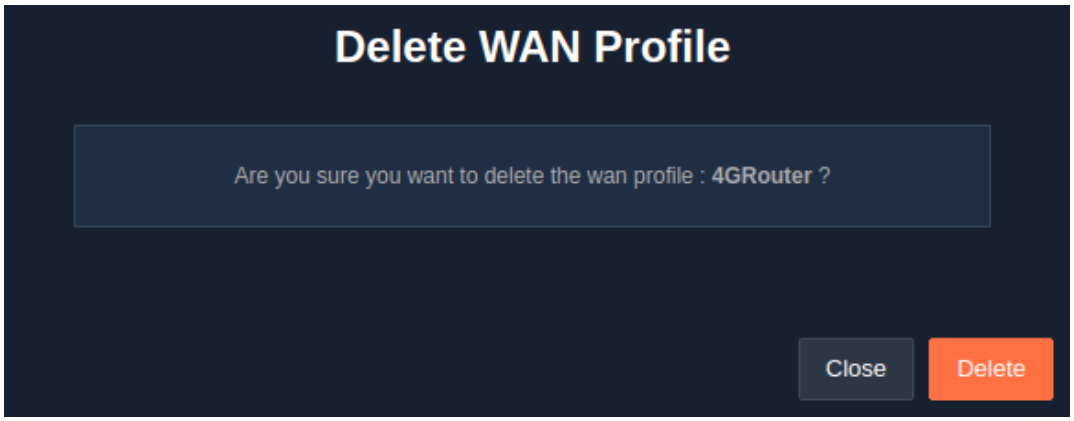


Fig. 2.1.4

Click on the 'Delete' button to delete a profile.

2.2 LAN

2.2.1 Create / Add New LAN Profile

An admin is provided the facility to add a new LAN profile for the UniBox. The LAN profile will be applied to one of the available ports to create a LAN port on UniBox. The LAN profile will have an option to enable DHCP service on the LAN port. Configure the LAN IP address of the port along with the subnet mask. Set the number between 1 and 254 for the start and end of the DHCP pool. Note that the start should be smaller than the end number.

To create a LAN profile, go to the 'Network' module and select the 'LAN' section. Then click on the '**+**' icon. A window displays a form to be filled in with the information required to add a new LAN profile.

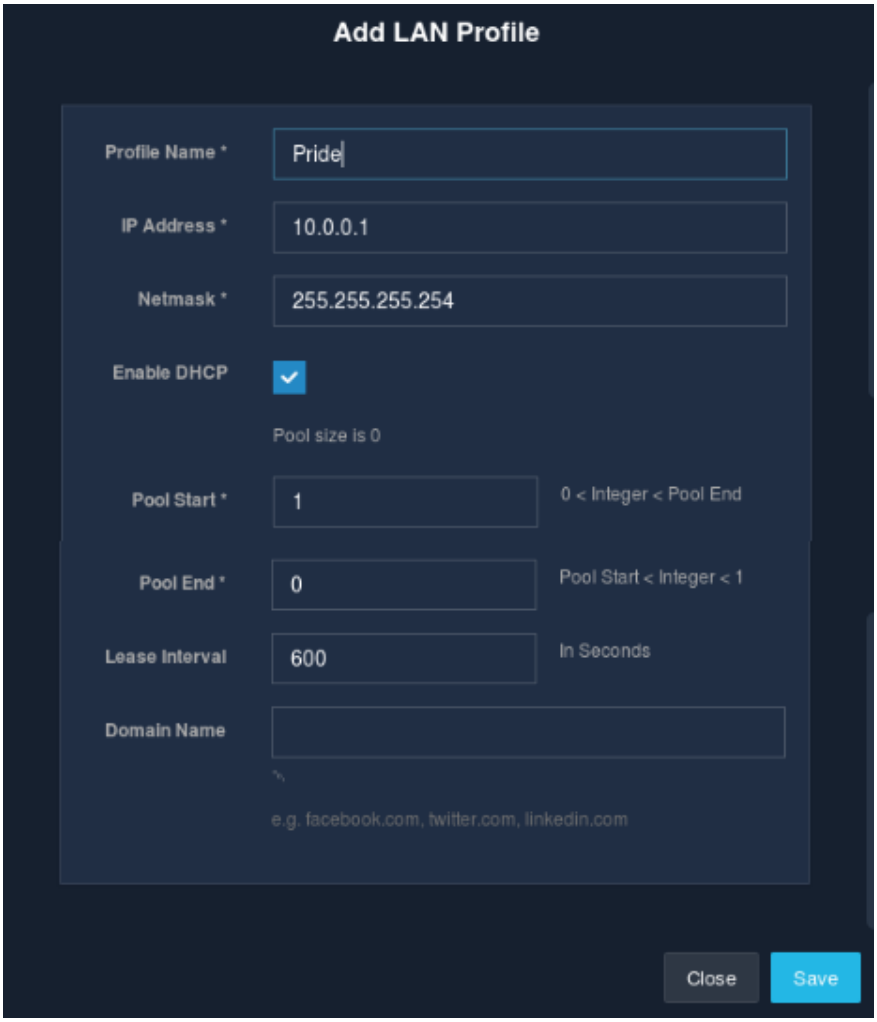


Fig. 2.2.1

Fields	*Description*
Profile Name	Name of the LAN profile.
IP Address	Enter the IP address of the LAN port.
Net Mask	Enter the subnet mask.
Enable DHCP	Enable DHCP service on the LAN port.
Pool Start	Enter the starting IP of the DHCP pool.
Pool End	Enter the ending IP of the DHCP pool.
Lease Interval	Enter the DHCP lease interval in seconds.

Domain Name	Enter the domain name for the DHCP service.

Table 2.2.1

Click on the ‘Save’ button to apply the information and create a LAN profile.

2.2.2 List LAN Profile

All the LAN profiles configured on the UniBox are listed down in a tabular form. The list displays the profile name, IP address of the LAN port, subnet mask, and whether the LAN port has enabled DHCP services or not. The listing table also contains an ‘Operations’ column where the options to edit or delete profiles are available.

To view the list of LAN profiles, go to the ‘LAN’ section in the ‘Network’ module.

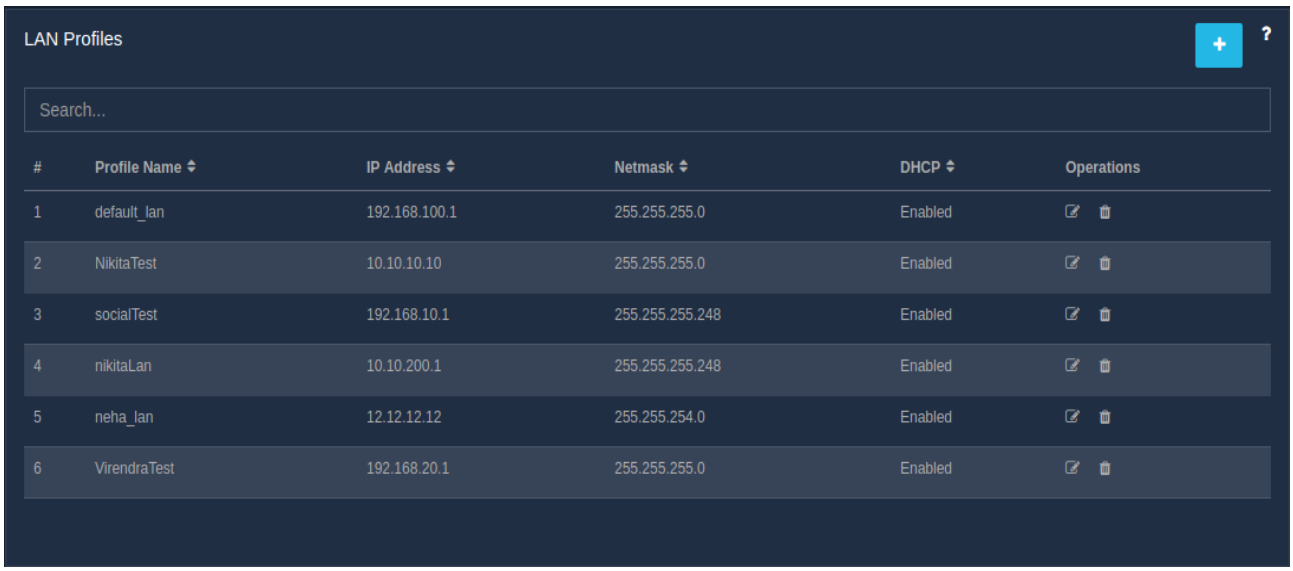


Fig. 2.2.2

2.2.3 Edit LAN Profile

The edit option allows an admin to edit or make changes to an already existing LAN profile. While changing the configurations of the profiles, make sure to change the DHCP pool accordingly.

To edit a LAN profile, click on the edit icon in the ‘Operations’ column present in the ‘LAN’ module. All the clients connecting to the LAN port will be issued new IP addresses.

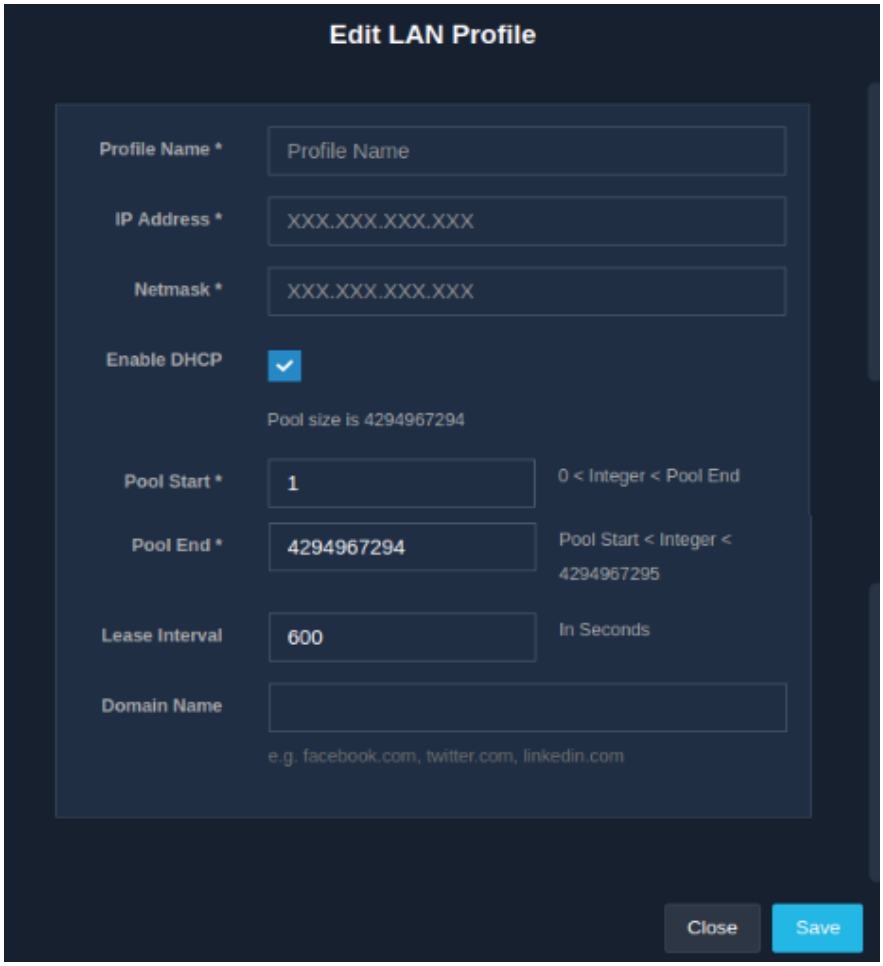


Fig. 2.2.3

Click on the 'Save' button to update and apply the new settings. When the settings are changed, all the online users will have to relogin.

2.2.4 Delete LAN Profile

An admin can delete a configured LAN profile. LAN profiles can only be deleted once they are dissociated from the LAN interface. To dissociate or remove the LAN profile from the LAN interface, refer to the Interface section.

To delete LAN profiles, click on the delete icon in the 'Operations' column present in the 'LAN' section of the 'Network' module. A message window appears to confirm the delete action about to be performed.

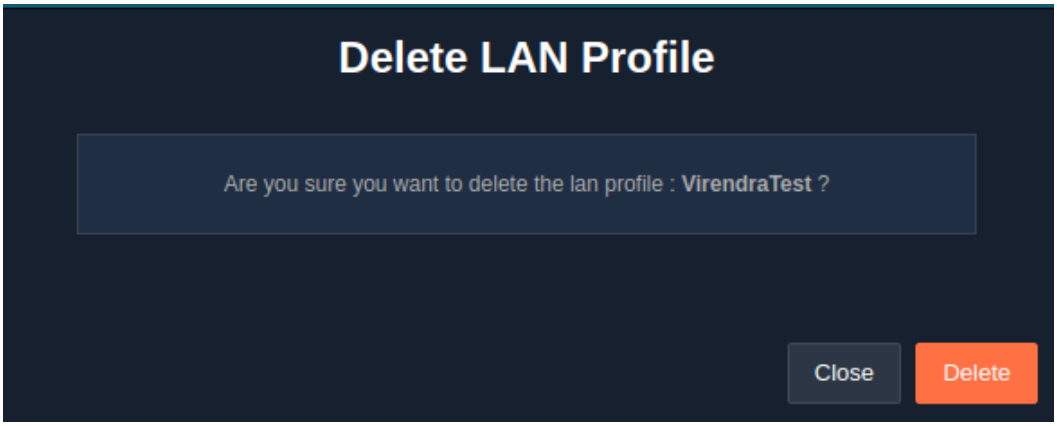


Fig. 2.2.4

Click on the 'Delete' button to surely delete the LAN profile.

2.3 VLAN

2.3.1 Create / Add New VLAN Profile

VLAN are virtual subnet created for dividing network into logical subnets and isolating the traffic on the physical network.

Use this feature to define a VLAN profile in UniBox. The profile can be applied to a physical or virtual port and all the traffic following from the port will be tagged with the VLAN tag(s). Administrators can define a fixed single VLAN tag or a range of VLAN tags. In case of a range of VLANs, the start ID and end ID must be specified.

To create a VLAN profile, go to the 'Network' module and in the 'VLAN' section, click on the '+' icon. A modal form is displayed where the information required to create a VLAN profile are to be filled in. The fields in the form change with the change in the types of VLAN:

- **Fixed**: It refers to a single VLAN tag.
- **Range**: It refers to the wide range of VLAN tags that can be defined.

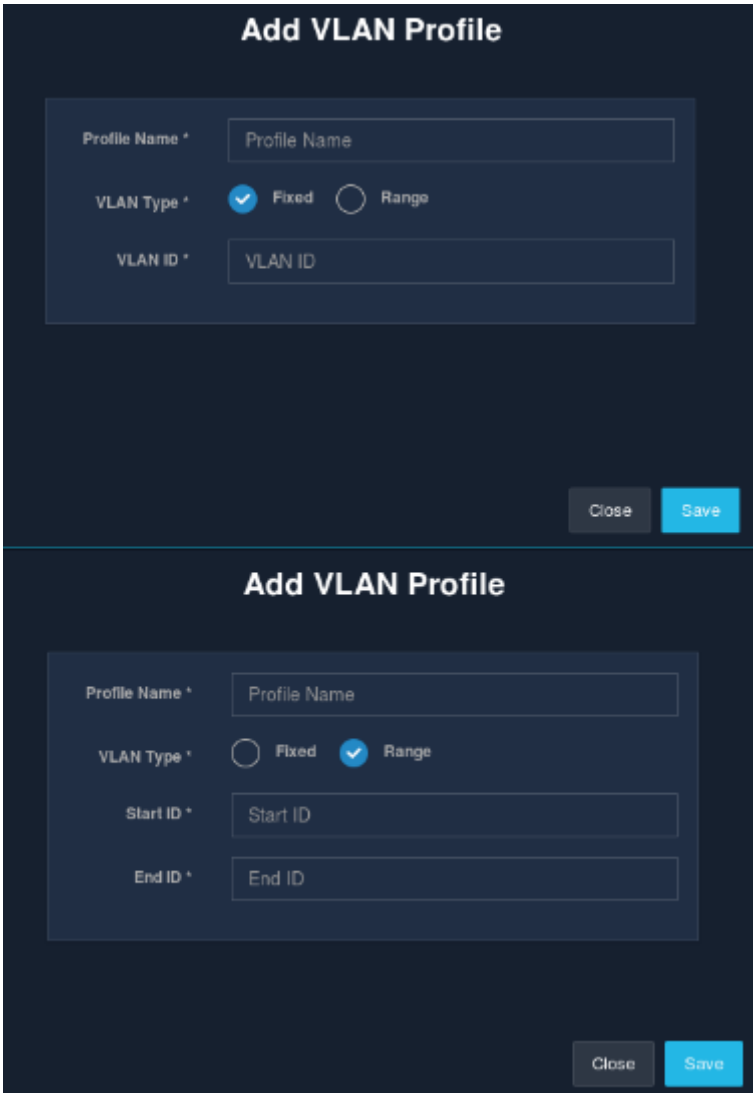


Fig. 2.3.1

Fields	***Description***
Profile Name	Name of the VLAN profile.
VLAN Type	Select one of the VLAN type, either Fixed or Range.
VLAN ID	Enter the VLAN ID for single or fixed VLAN.
Start ID	Enter the start of VLAN ID for VLAN of the range type.
End ID	Enter the end of VLAN ID for VLAN of the range type.

Table 2.3.1

Finally, click on the 'Save' button to save the configurations and create a VLAN profile.

2.3.2 List VLAN Profile

All the VLAN profiles configured in UniBox are displayed in a list. The list displays the profile name, VLAN type, VLAN ID, end Id and start Id. The listing table also contains an 'Operations' column, which provides the options to edit or delete profiles.

An admin can view the list of VLAN profiles by going to the ‘Network’ module and selecting the ‘VLAN’ section.

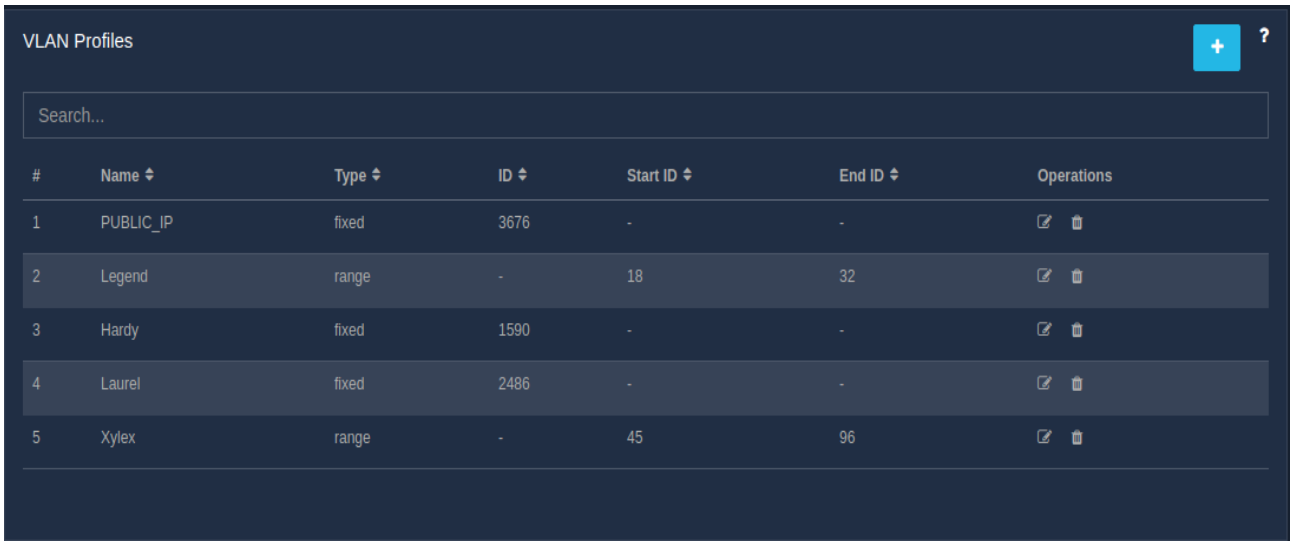


Fig. 2.3.2

2.3.3 Edit VLAN Profile

The edit option allows an admin to make changes to the configurations of an already existing VLAN profile.

To edit a VLAN profile, click on the edit icon in the ‘Operations’ column present in the ‘VLAN’ section under the ‘Network’ module. A modal form is displayed to make the required changes to the configuration.

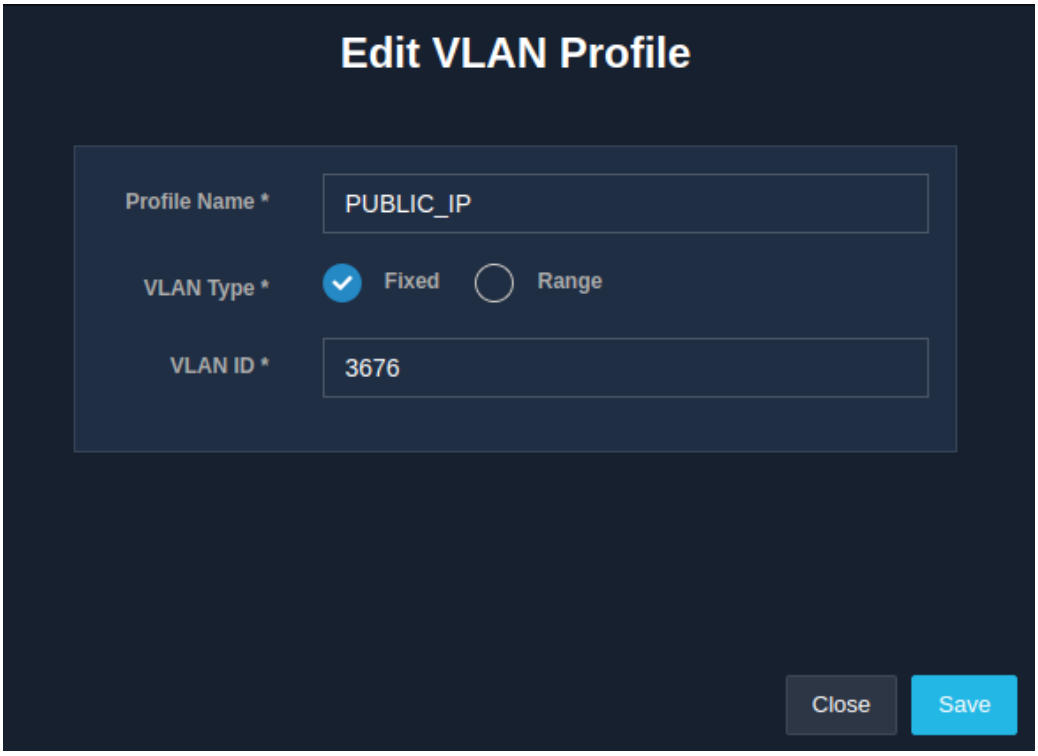


Fig. 2.3.3

2.3.4 Delete VLAN Profile

The delete option allows an admin to delete an existing VLAN profile. It is important to disassociate the VLAN profile from the port before deleting the VLAN profile.

To delete a VLAN profile, go to the 'Network' module and then select the 'VLAN' section. Click on the delete icon present in the 'Operations' column against the profile that needs to be deleted.

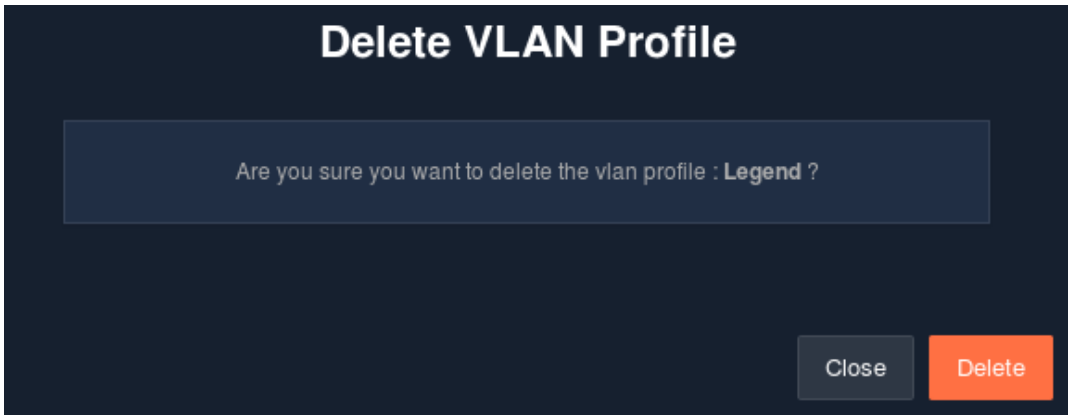


Fig 2.3.4

2.4 Interfaces

2.4.1 List Interface

All the available physical network interfaces on the UniBox hardware are listed down in a table. An admin can assign any LAN or WAN profile to the interfaces. In the list, each interface is labelled as 'eth#' where # is the number of the interface like eth0, eth1, etc. The list displays the port number, type of profile (LAN or WAN), name of the assigned profile, VLAN status (enabled or disabled) and the status of the port. If the connection is active, the port will appear UP else DOWN.

To view the list of interfaces, go to the 'Network' module followed by the 'Interfaces' section. The listing table also contains a column, named 'Operations', which provides the options to configure or reset interfaces.

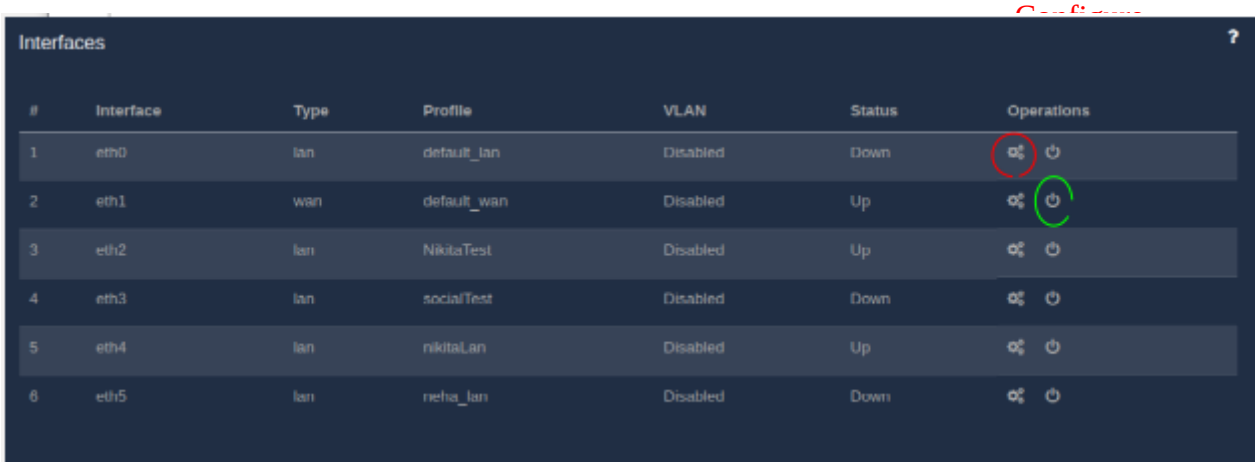


Fig 2.4.1

2.4.2 Configure Interface

An admin is facilitated with the feature to configure the network interface. The admin can assign the interface to either LAN or WAN profile. If the the interface is assigned to a LAN profile, the interface will function as LAN port. If the interface is assigned to a WAN profile, the interface will function as WAN port. The admin can also enable VLAN tagging by enabling the VLAN profile and select VLAN profile from the list in the drop-down menu.

To configure an interface, go to the 'Network' module and then the 'Interface' section. The listing table contains an 'Operations' column, which has one of the options as configure. Click on the configure icon. A window drops-down, displaying a form to fill in the configuration details.

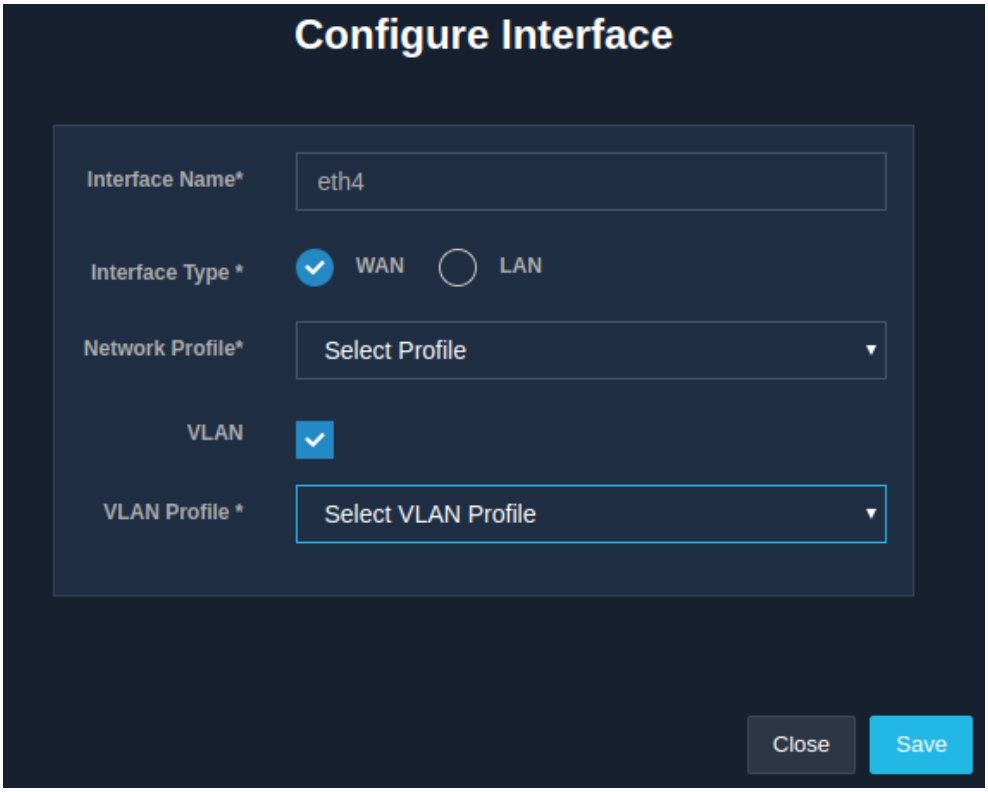


Fig 2.4.2

Fields	***Description***
Interface Name	Name of the network interface. This field is non-editable.
Interface Type	Select whether the interface type is WAN or LAN.
Network Profile	Select the LAN or WAN profile to associate with the interface.
Enable VLAN	If enabled, the interface will tag the traffic with the assigned VLAN tag.
VLAN Profile	Select the VLAN profile from the list.

Table 2.4.2

Click on the 'Save' button after all the details are entered in, to apply the configurations.

Note: For multi-WAN setup, admin will have to configure at least two WAN profile on two separate interfaces.

2.4.3 Reset Interface

The reset feature allows an admin to remove all the profiles associated with the network interfaces. The interface will be available for another configuration once the profile is removed. All the devices connected to the interface will lose their connectivity to the UniBox once the profile is removed.

To reset an interface, click on the reset icon in the 'Operations' column present in the 'Interfaces' section. A message window slides down to confirm the reset action.

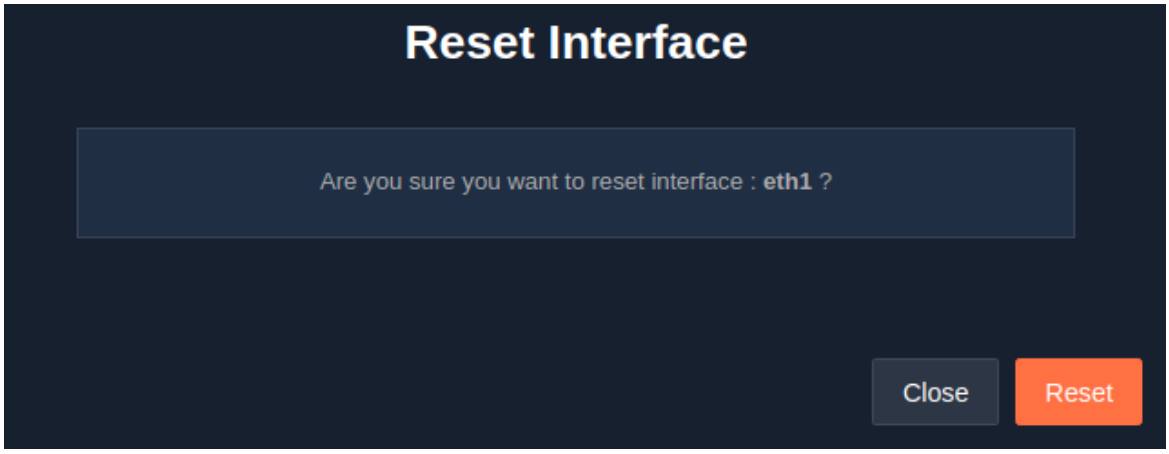


Fig 2.4.3

2.5 DNS

2.5.1 Create DNS

An admin is allowed to add a new DNS server. All devices connected to the UniBox will use the DNS servers configured in this section.

To create a DNS server, select the 'DNS' section under the 'Network' module. Then click on the '+' icon, a window pops-up to get the DNS server's IP address.

Fig 2.5.1

Field	Description
DNS Server IP	Enter the IP address of the DNS server.

Table 2.5.1

Once the DNS server IP is entered, click on the ‘Save’ button.

2.5.2 List DNS

All the DNS servers configured in the UniBox are listed down in a table. The DNS servers will be used in the order they were added.

To view the list of the DNS server, go to the ‘Network’ module followed by the ‘DNS’ section. A listing table displays the configured DNS servers and also consists of an ‘Operations’ column, which provides the options to edit or delete DNS servers.

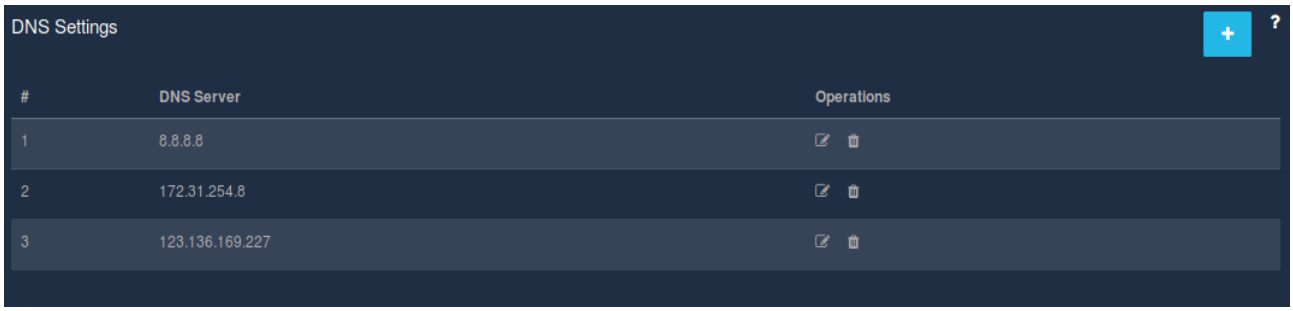


Fig 2.5.2

2.5.3 Edit DNS Server

The edit feature serves an admin with an option to make changes to an existing DNS server settings.

To edit a DNS server, click on the edit icon made available in the ‘Operations’ column in the ‘DNS’ section present in the ‘Network’ module. A window slides down to make change to the DNS server’s IP. Refer.

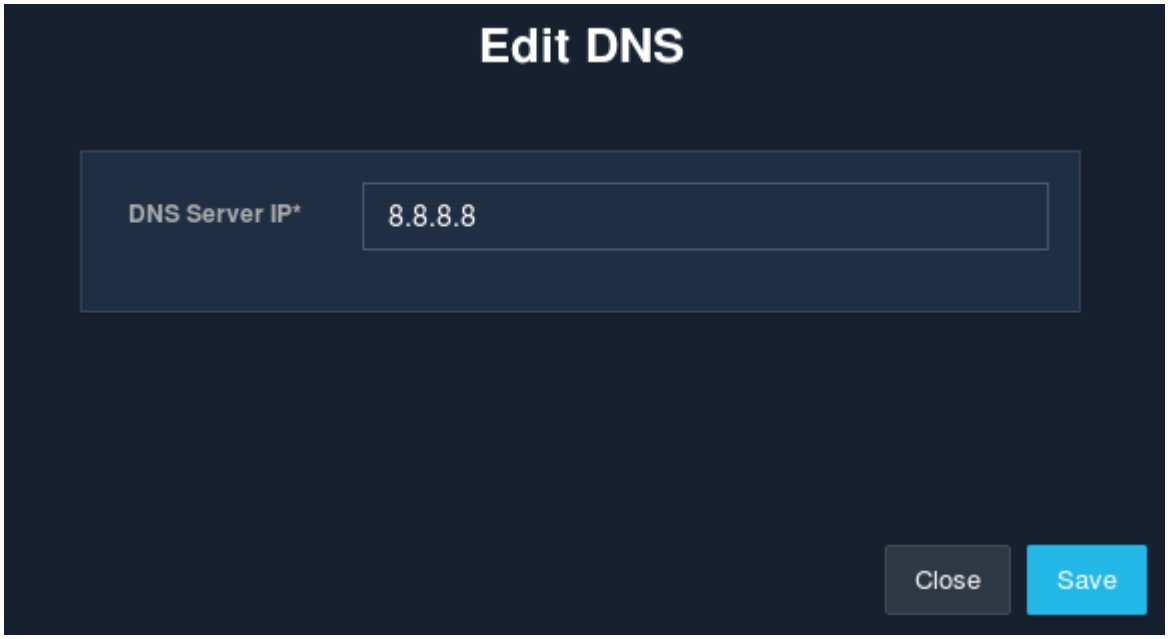


Fig 2.5.3

Once the required changes are made to the server IP address, click on the 'Save' button to save the configuration for the changes to take effect.

2.5.4 Delete DNS Server

To delete a DNS server, all an admin has to do is, click on the delete icon in the 'Operations' column present in the 'DNS' section of the 'Network' module. A message window appears asking to confirm the delete action.

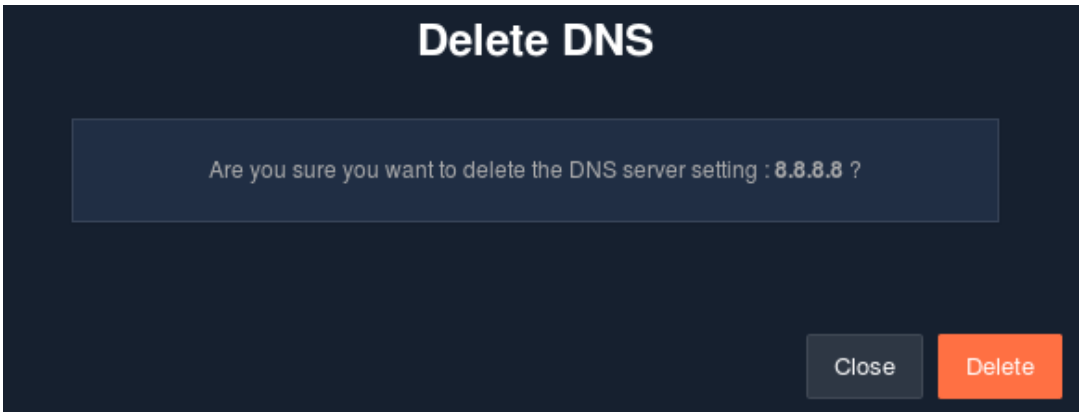


Fig.2.5.4

Click on the 'Delete' button to surely delete the DNS server.

2.6 VPN

An admin is facilitated with the feature which allows him/her to run a VPN server inside UniBox. This feature is beneficial if the admin wants to offer VPN access into the enterprise network. The VPN can run in two modes:

- Bridges (TAP):-
  - It behaves like a real network adapter, except that it is a virtual adapter.
  - Can transport any network protocols (IPv4, IPv6, Netalk, IPX, etc.).
  - Works at layer 2, which means that the Ethernet frames are passed over the VPN tunnel.

- Can be used in bridges.

- Router (TUN):-
  - It has a lower traffic overhead, transports only traffic which is destined for the VPN client.
  - Transports only layer 3 IP packets.
    - Drawbacks of TUN -
      - Broadcast traffic is not normally transported.
      - Can only transport IPv4 (OpenVPN 2.3 adds IPv6)
      - Cannot be used in bridges.

The VPN server will require a signed SSL certificate for authenticating the client. By default, UniBox comes with a signed SSL certificate, but the client can upload their own SSL certificate in UniBox.

To configure an on-board VPN server, go to the 'Network' module followed by the 'VPN' section. A page displays a form to gather all the details required to configure a VPN server.

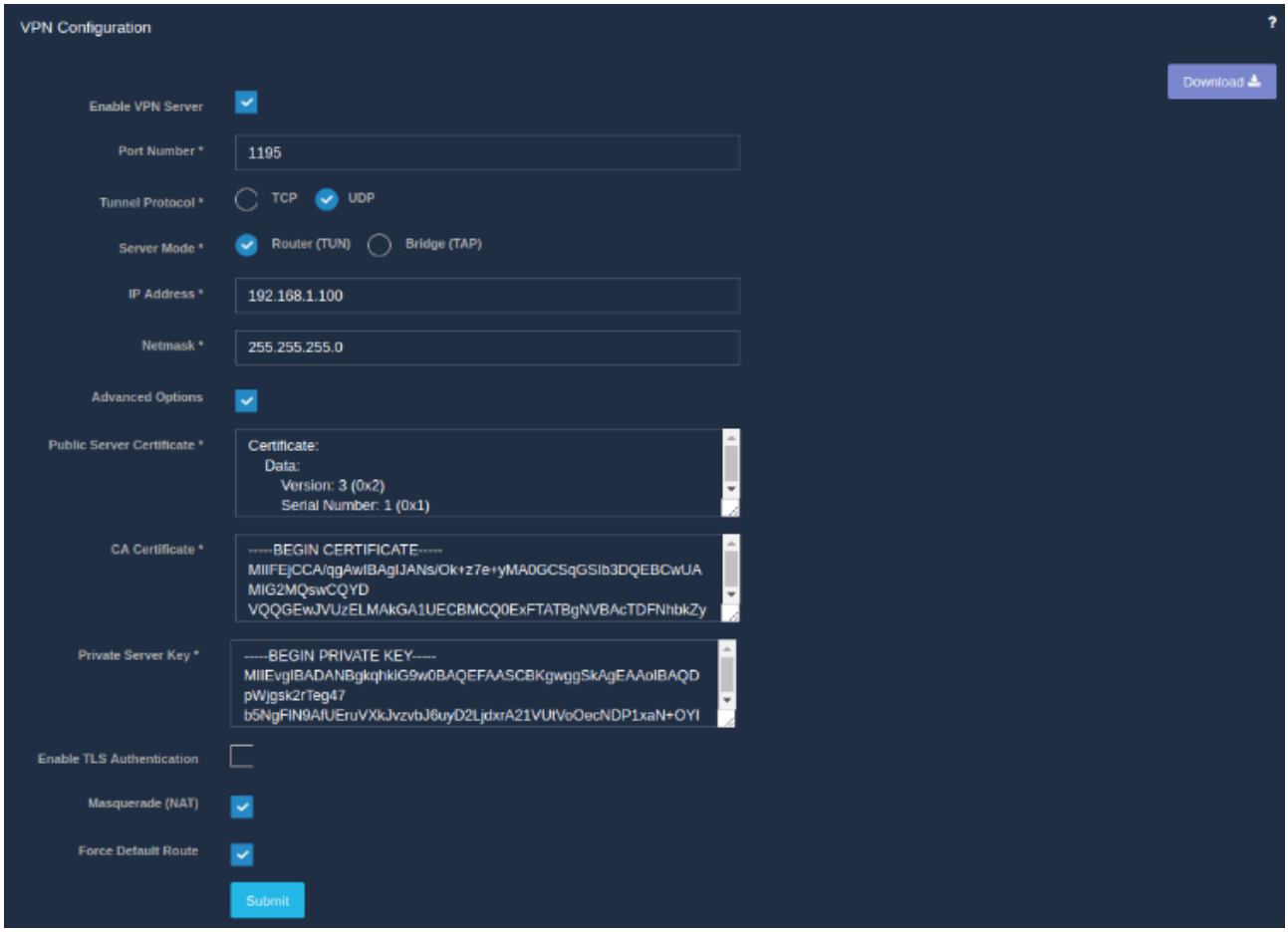


Fig.2.6

Fields	Description
Enable VPN server	If enabled, the VPN server will run the UniBox and will accept remote clients.
Port Number	Enter the port number for VPN server.
Tunnel Protocol	Select the tunnel protocol, either TCP or UDP.
Server Mode	Select the VPN server mode, either TAP or TUN.

IP Address	Enter the IP address of the VPN server. Clients will connect to this IP from remote sites.
Netmask	Enter the subnet mask.
LAN Profile	Select the LAN profile on which the VPN server will run.
Advanced Options	Tick-off the checkbox to enable advanced options.
Public Server Certificate	Enter the public server certificate.
CA Certificate	Enter the CA certificate.
Private Server Key	Enter private server key.
Enable TLS Authentication	If enabled, TLS authentication is enabled.
TLS Auth Key	Enter the authentication key for TLS authentication.
Masquerade (NAT)	Tick the check-box for the server to enable masquerading of the packets.
Force Default Route	Tick the check-box if the server should force the traffic on default IP route.

Table 2.6

When all the details are carefully filled in, click on the 'Submit' button.

2.7 Monitoring

The UniBox monitors each configured device periodically, then alerts the admin if there is an outage. UniBox uses the MAC address of the device for monitoring as the IP address of the device may change if the device is on a dynamic IP. Also, MAC address monitoring is more reliable. The admin is required to enter the MAC address of the interface that will be connected to the UniBox for monitoring.

2.7.1 Create / New Monitoring Device

An admin is facilitated with the services that allows him/her to configure a new device for monitoring. If the UniBox is used within a wireless network, then admin can configure the devices in UniBox for monitoring. UniBox will check the status of all devices periodically and will send email alerts if any of them are down. The UniBox can monitor devices, both on LAN and WAN side. LAN side devices are monitored using their MAC address while the WAN side requires the IP addresses.

UniBox runs a monitoring process that will periodically check the status of all access points. Admin can configure one or more email addresses for notification.

To add a new monitoring device, go to the 'Network' module followed by the 'Monitoring' section. Then, click on the '**+**' icon, a modal form appears to gather information required to add a new device for monitoring.

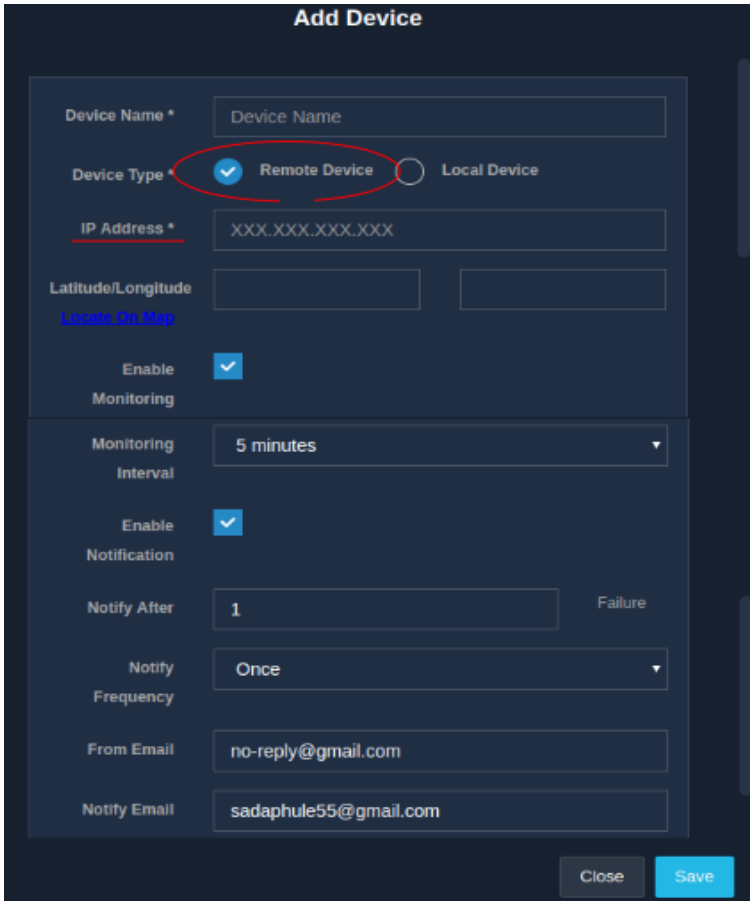

Add Device
Device Name *
Device Name
Device Type *
Remote Device
Local Device
IP Address *
XXX.XXX.XXX.XXX
Latitude/Longitude
Locate On Map
Enable Monitoring
Monitoring Interval
5 minutes
Enable Notification
Notify After
1
Failure
Notify Frequency
Once
From Email
no-reply@gmail.com
Notify Email
sadaphule55@gmail.com
Close
Save

Fig 2.7.1(a)

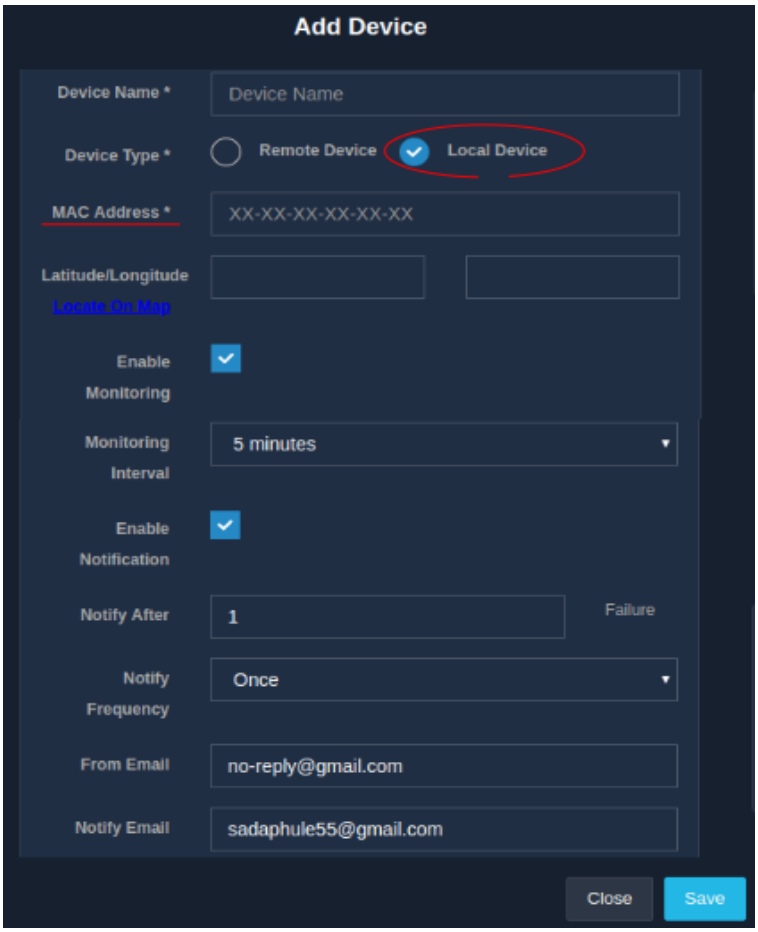


Fig 2.7.1 (b)

Fields	***Description***
Device Name	The name of the device to be monitored. Enter a name that will make identifying the device easier.
Device Type	Select the device type, either remote or local. For devices that are: • **Remote** – Enter the public IP address. • **Local** – MAC address is compulsory.
IP Address	Enter the Public IP address of the remote device to be monitored.
MAC Address	The MAC address of the local device to be monitored.
Latitude/Longitude	The latitude and longitude coordinates of the device to be monitored, (if available), for plotting the AP on the map.
Enable Monitoring	Ticking off the check-box enables the device to be monitored.
Monitoring Interval	Select the interval for monitoring the device from the options available in the drop-down menu. UniBox will monitor the device after the configured interval.

Enable Notification	If ticked-off, the UniBox will email the UP or DOWN status of the device to the configured email addresses.
Notify After	Enter a number which indicates the number of failures after which the notification will be sent.
Notify Frequency	Indicates whether the notification is sent once or multiple times. Default: Once.
From Email	Email address (only one) from which the notification will be sent.
Notify Email	Email addresses to which the notifications will be sent to. Multiple email addresses should be separated by comma.

Table 2.7.1

Click on the 'Save' button to apply all configurations entered and monitor a device.

2.7.2 List Monitoring Device

The table provides an admin with a list of all the devices configured for monitoring.
The list provides the status of the devices configured, whether they are UP or DOWN, along with the name of the device, IP address, MAC address, device vendor, monitoring status (enabled or disabled) and the last monitored time. Also the listing table contains the 'Operations' column, which provides the services of edit and delete.

To view the list of all the added monitoring devices, go to the 'Network' module followed by the 'Monitoring' section. The list will be visible along with the option to search devices based on the status, the fields (device name, IP address or MAC address) and the value of the selected criterion.

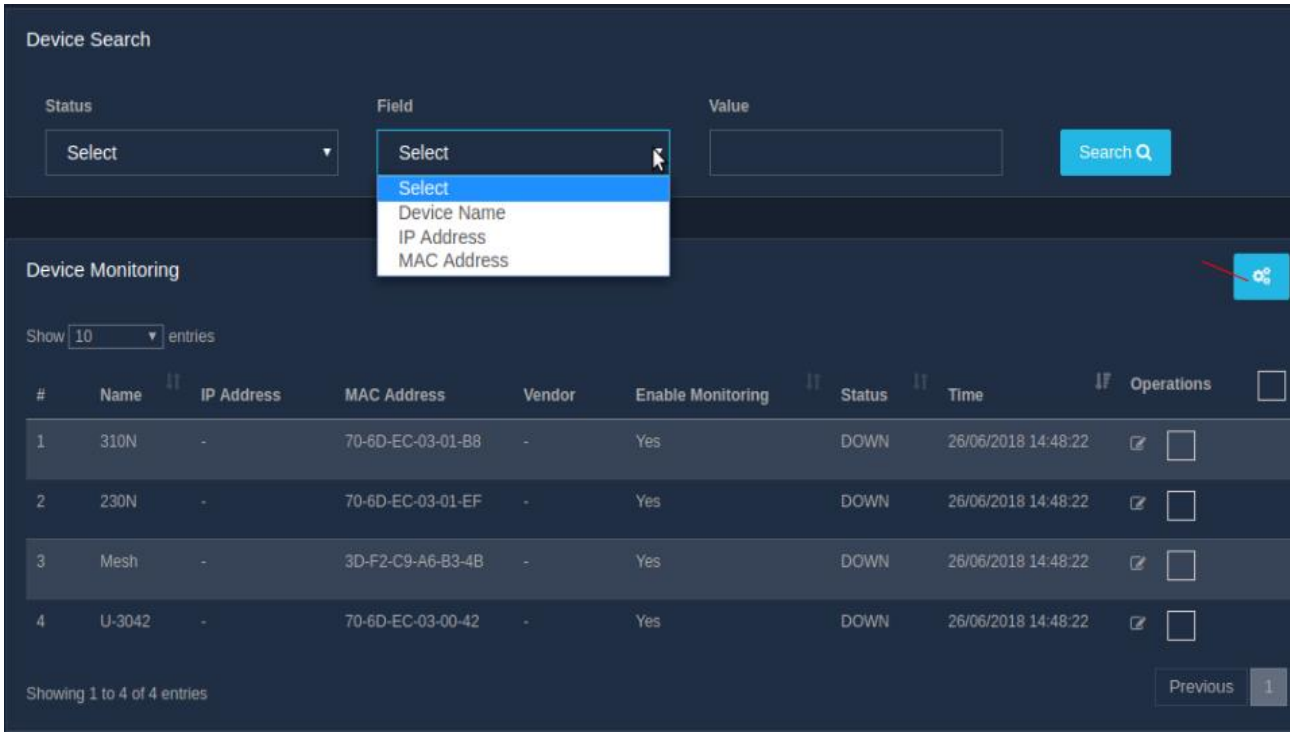


Fig 2.7.2

2.7.3 Edit Monitoring Device

An admin is allowed to make changes to the information about an already existing monitoring device.

To edit the device information, click on the edit icon in the ‘Operations’ column present in the ‘Monitoring’ section of the ‘Network’ module. A modal form with the previously entered information is displayed for all the necessary changes to be made. Refer

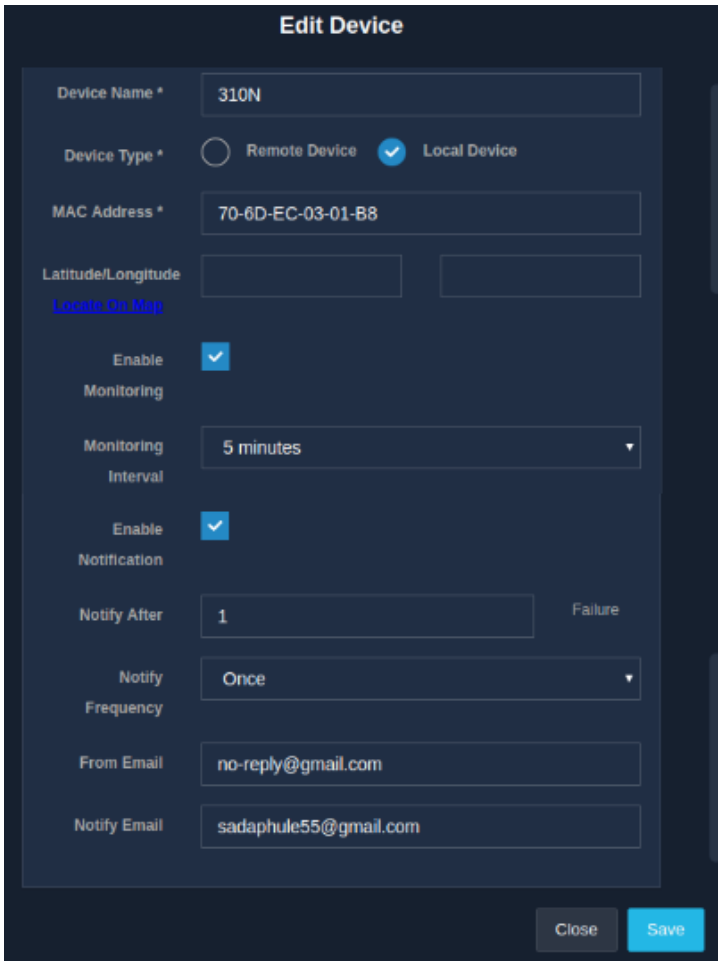


Fig 2.7.3

Once the necessary changes are made, click on the ‘Save’ button to apply the changes.

2.7.4 Configure Monitoring Device

An admin is provided with the facility to specify the default configuration of the monitoring devices. If multiple monitoring devices are added, it is advisable to set the default monitoring settings before adding the devices. This will ease the chore of configuring the notification settings of each device.

To set the default notification settings, select the ‘Monitoring’ section in the ‘Network’ module. Then click on the configuration icon, which displays a form to configure the devices.

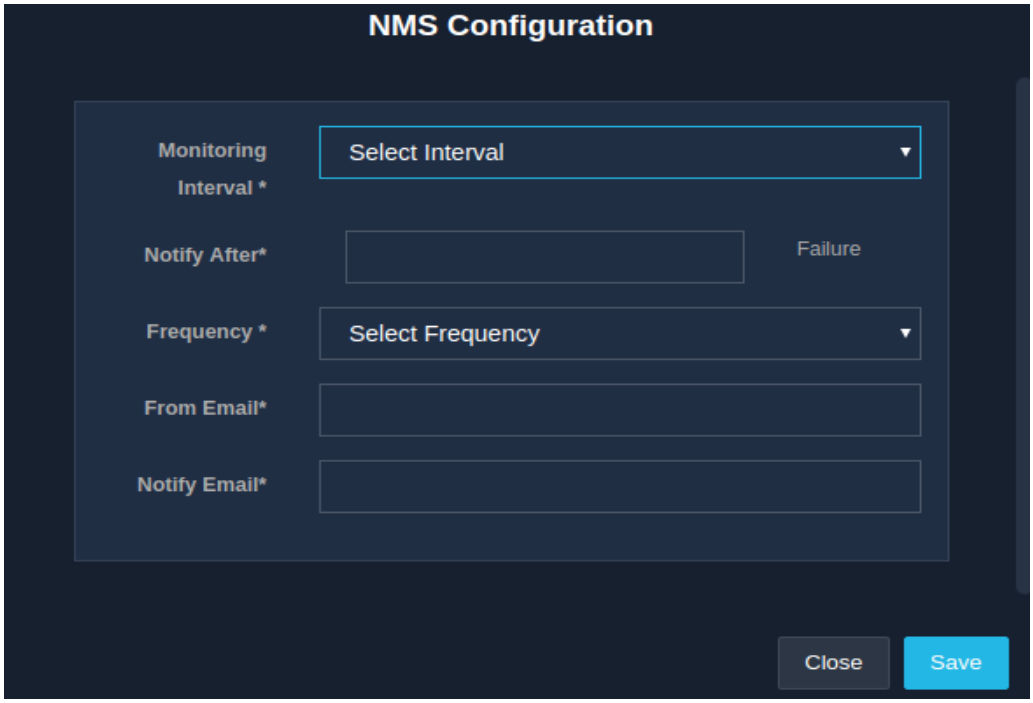


Fig 2.7.4

Fields	***Description***
Monitoring Interval	The default time interval for monitoring the device.
Notify After Failure	This setting will send notifications after the configured successive failures.
Frequency	Indicates whether the email notification is to be sent once or multiple times.
From Email	The email address from which the email notification will be sent.
Notify Email	The email address to which the email notification will be sent to. Multiple email addresses should be separated by commas.

Table 2.7.4

Once the configurations are entered in, click on the 'Save' button to apply and set the said configurations.

2.7.5 Delete Monitoring Device

To delete a device from the monitoring list, tick-off the checkbox in the 'Operations' column present in the 'Monitoring' section of the 'Network' module. When a check-box is ticked-off, the delete icon appears above the listing table. Clicking on the delete icon displays a message window asking to confirm the delete action.

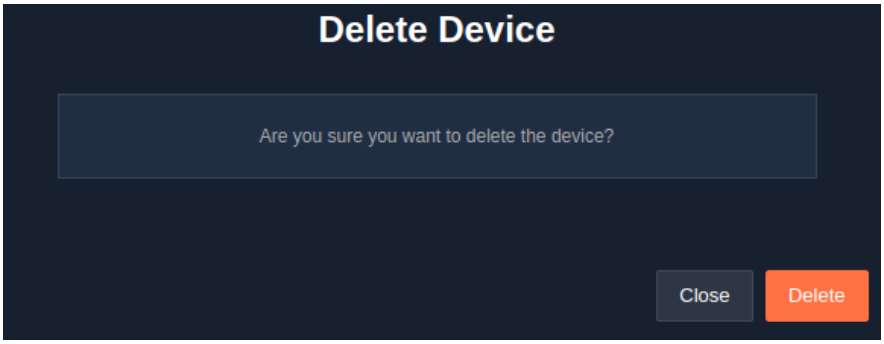


Fig 2.7.5

Click on the 'Delete' button to delete the device from the monitoring list.

Note: Multiple devices can be deleted at a time by ticking-off the checkboxes of those devices that are to be deleted.

2.8 DDNS

An admin is allowed to configure the Dynamic DNS client in the UniBox. Configuring Dynamic DNS client will help an admin to access the UniBox from public network, even when the UniBox WAN IP is set on dynamic mode and the IP changes frequently. DDNS client on UniBox will periodically update the host name record stored at the dynamic DNS server with WAN port settings. Admin can access the UniBox from a public network using the specified DDNS hostname.

To configure a Dynamic DNS client, go to the 'DDNS' section in the 'Network' module. A page displays a form meant to collect the details required to configure the DDNS client.

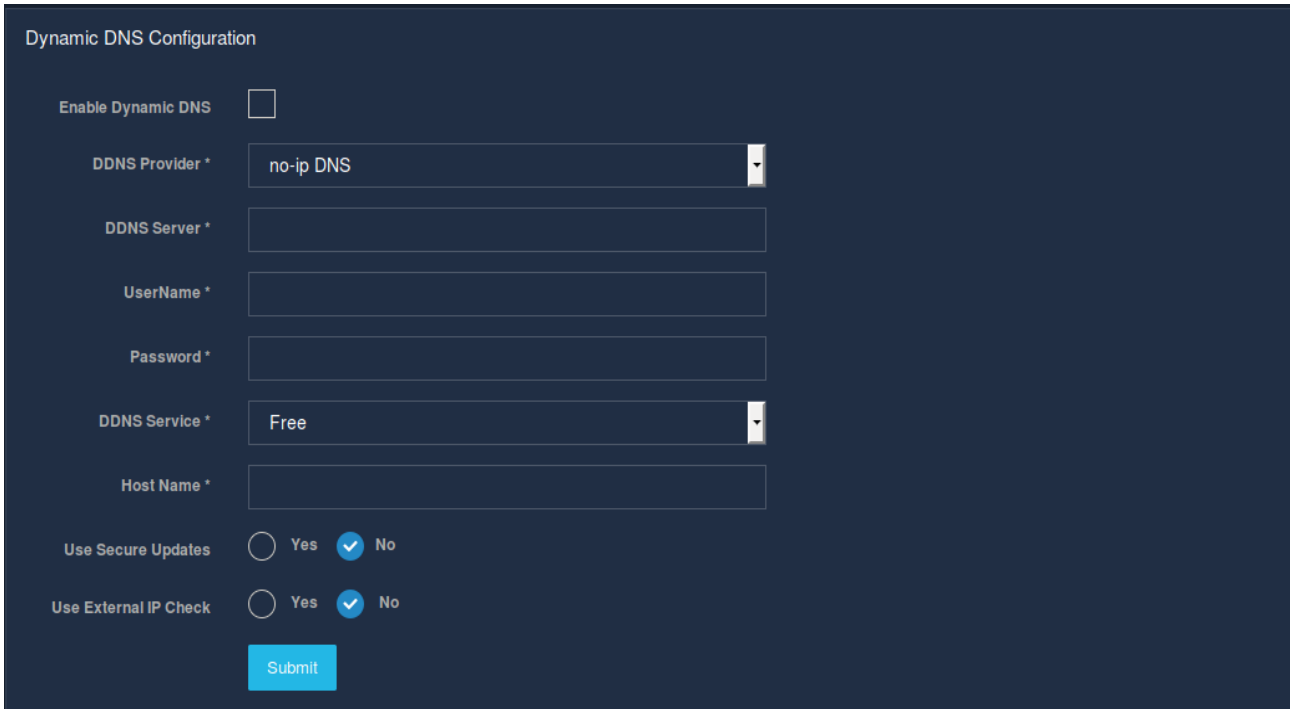


Fig 2.8

Fields	***Description***
Enable Dynamic DNS	Ticking-off the check-box will enable the Dynamic DNS client in UniBox. This client is responsible for updating the UniBox WAN IP to the DDNS server.
DDNS Provider	Select the Dynamic DNS service provider from the drop-down list. At present, two Dynamic DNS providers are supported: • Dyn DNS • no-ip DNS **An admin has configure his/her own account from these providers.**
DDNS Server	Enter the server name of the Dynamic DNS provider.
Username	Enter the username of the already created account on Dynamic DNS server.
Password	Enter the password of the already created account on the Dynamic DNS server.
DDNS Service	Select the Dynamic DNS from the drop-down menu, either free or customer (paid).
Host Name	Enter the fully qualified hostname to be updated against the IP address in the Dynamic DNS server records. The settings should be obtained from the DDNS provider.
Use Secure Updates	If 'Yes', DNS record updates are sent to the DDNS server over secure (HTTPS) channel.

Use External IP Check	If 'Yes', the gateway public (WAN) IP is obtained and used for DNS updates. It is used in private network settings.

Table 2.8

Once all the details are filled in, click on the 'Submit' button to save all the configurations of the DDNS.

2.9 IP Routes

2.9.1 New IP Routes

An admin is allowed to create a new IP route on the UniBox for both inbound as well as outbound traffic. The IP route will decide how the packets are routed from the UniBox to other hosts or networks. The IP routes can be defined for a specified host or network. If defined for a specific host, then UniBox will use the specific rule to route the IP packets to that host.

To create or add a new IP route to UniBox, go to the 'IP Routes' section in the 'Network' module. Then click on the '**+**' icon, where a modal form is displayed to collect the information required to add a new IP route.

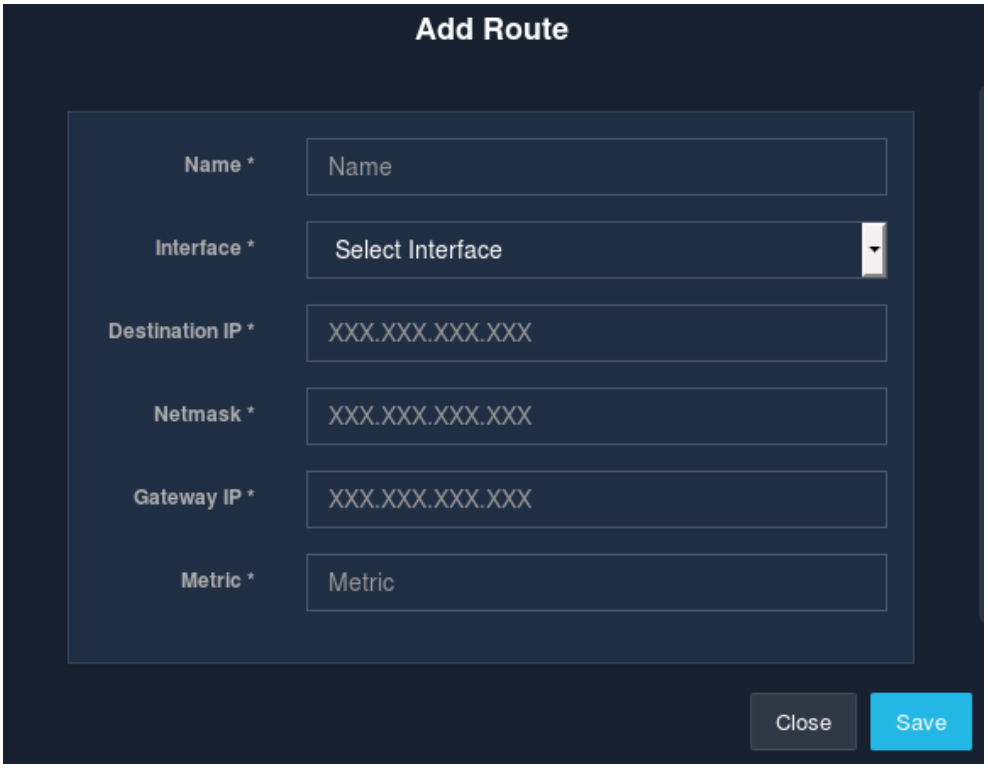


Fig 2.9.1

Fields	*Description*
Name	Name of the IP route.
Interface	WAN or LAN interface on which the rule will be applied.
Destination IP	Enter the final destination. If the type is host, then destination is the specific IP of host or else the

	netmask and destination will determine the destination network.
Netmask	Enter the subnet mask for the destination IP.
Gateway IP	The IP address of the gateway that is the middleware between the source and destination.
Metric	Cost of the path to the destination. The cost is based on various factors like bandwidth, number of hops, etc.

Table 2.9.1

Click on the ‘Save’ button to apply the configurations and add a new IP route.

2.9.2 List IP Route

All the IP routes configured in the UniBox are displayed in the listing table. The default IP route will display the route available to all UniBox clients. This cannot be edited since it is auto-generated when the WAN port settings are set. An admin can add additional IP routes depending on the network requirements.

To view the list of all the IP routes, go to the ‘Network’ module followed by the ‘IP Routes’ section. The listing table contains the name of the route, the interface on which the route is configured, the destination IP, netmask, the gateway IP, metric and also the ‘Operations’ column, which contains the options to edit and delete.

Fig 2.9.2

2.9.3 Edit IP Route

The edit feature allows an admin to make changes to an already existing IP route. The interface defines the network on which the route applies.

To edit an IP route, go to the ‘Network’ module followed by the ‘IP Routes’ section. Then click on the edit icon that is present in the ‘Operations’ column. When clicked, a modal form is displayed to edit the information that was previously given while adding the IP route.

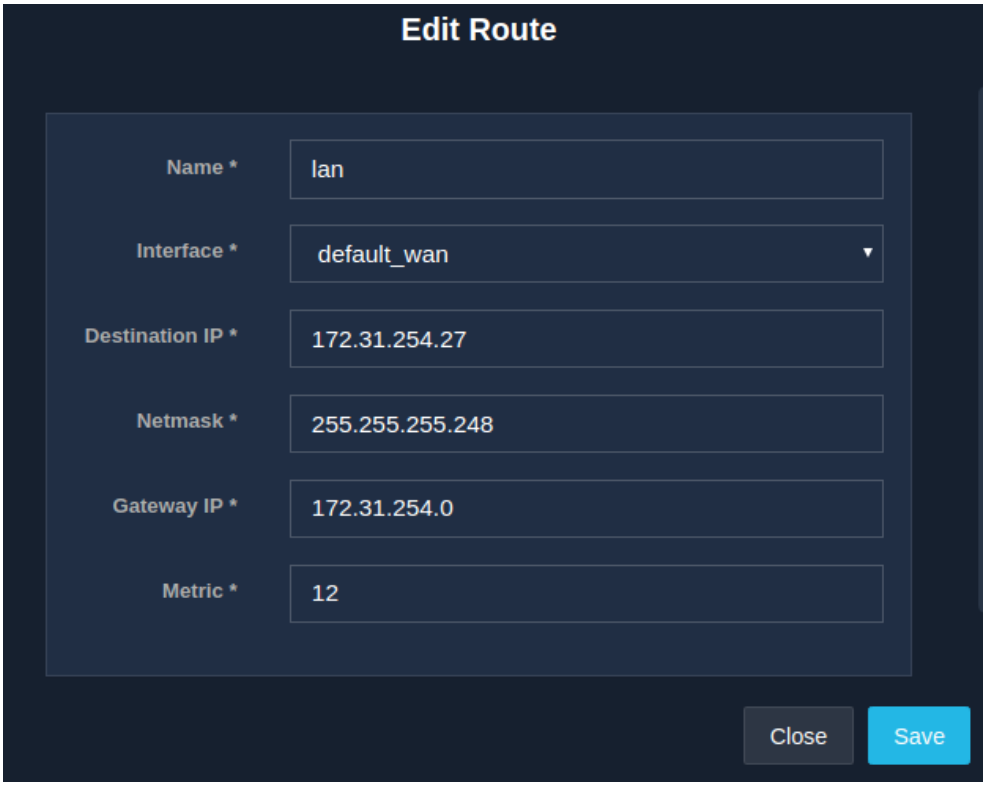


Fig 2.9.3

Click on the 'Save' button to set and apply the changes made.

2.9.4 Delete IP Route

To delete the IP route, click on the delete icon present in the 'Operations' column in the 'IP Routes' section of the 'Network' module. A message window pops to confirm the delete action.

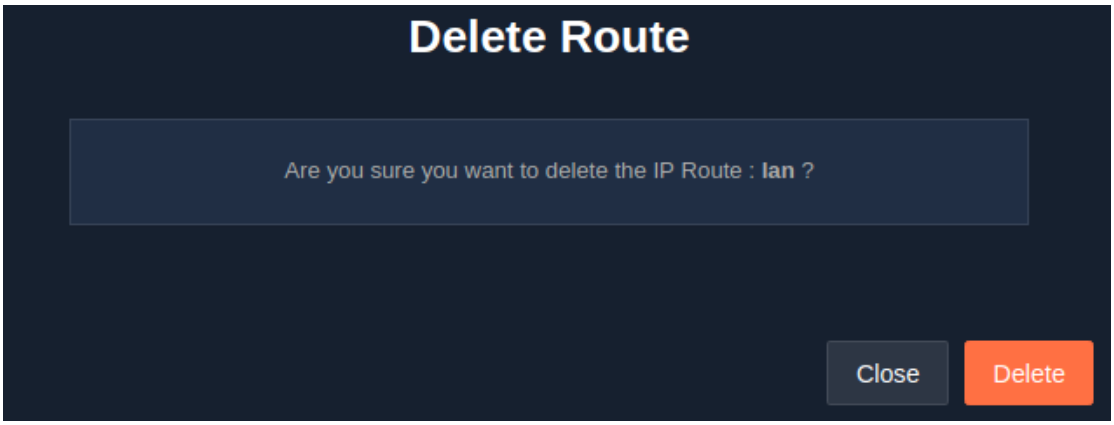


Fig 2.9.4

Click on the 'Delete' button to remove the IP route.

2.10 Routing

2.10.1 Post Forwarding

The NAT rules are used by the UniBox to forward either incoming or outgoing packets to specific hosts within the LAN network. The NAT rules can be configured for different ports. For example, to access a client inside the UniBox network, there is a need to configure a port forwarding NAT rule. The NAT rules can be configured for both TCP and UDP packets.

2.10.1.1 New Port Forwarding

An admin is allowed to add a new Network Address Translation (NAT) rule to UniBox. By default, UniBox will block all the traffic from the WAN port to the LAN port. A NAT rule will allow an admin to selectively allow specific port traffic to pass from the WAN port to LAN port based on the way the rule is defined.

To add a new NAT rule, go to the 'Network' module followed by the 'Routing' section. Then go to the 'Post Forwarding' sub-section and click on the '**+**' icon. A modal window is displayed to collect the information required to add a new rule.

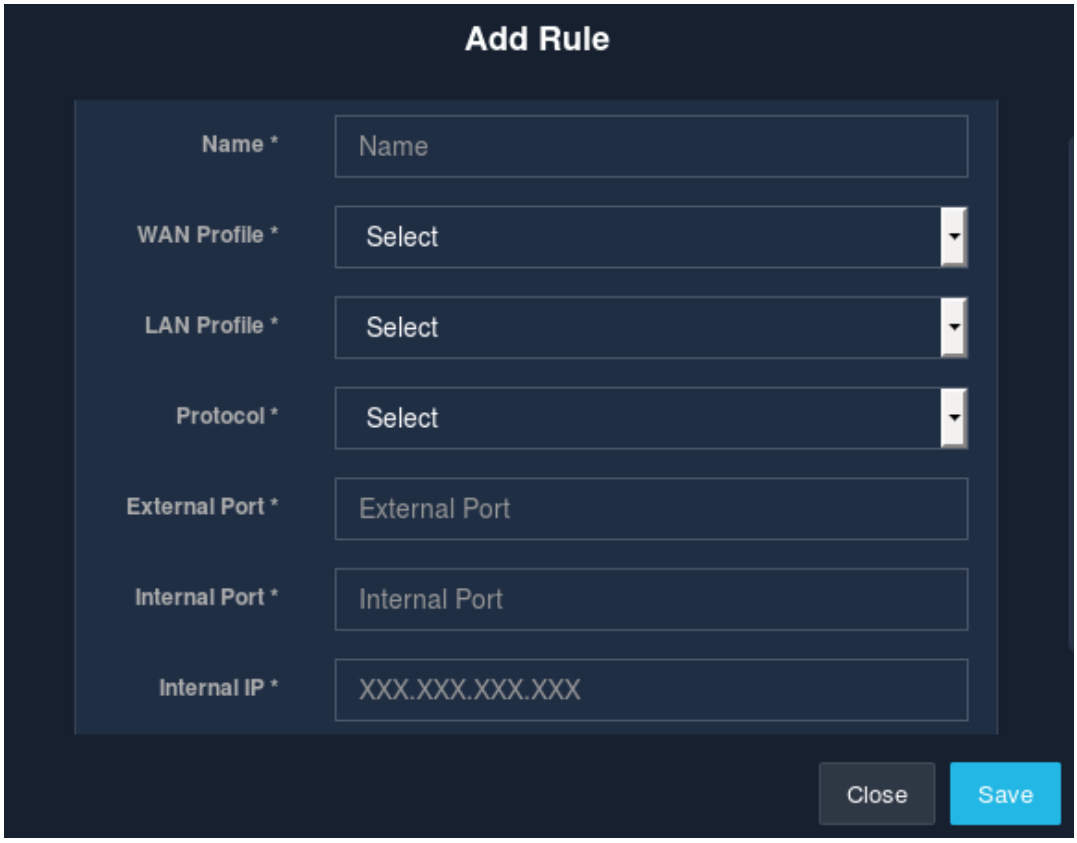


Fig 2.10.1.1

Fields	*Description*
Name	Enter the name of the NAT rule.
WAN Profile	Select the WAN profile.
LAN Profile	Select the LAN profile.
Protocol	Select whether the rule applied to TCP or UDP or both the traffic.
External Port	Enter the port number (1-65535) that will be forwarded to an internal port.
Internal Port	Enter the port number (1-65535) to which the traffic will be forwarded.

Internal IP	Enter the IP address of the client inside the LAN network.

Table 2.10.1.1

Click on the ‘Save’ button to save and apply the newly defined rule.

2.10.1.2 List Port Forwarding

A table lists down all the NAT port forwarding rules defined in the UniBox. The listing table displays the name, WAN profile, LAN profile, protocol, external and internal port, along with the private IP address of the client. The table also contains the ‘Operations’ column providing the edit and delete options.

To view the list of all the NAT rules, select the ‘Post Forwarding’ sub-section from the ‘Routing’ section in the ‘Network’ module.

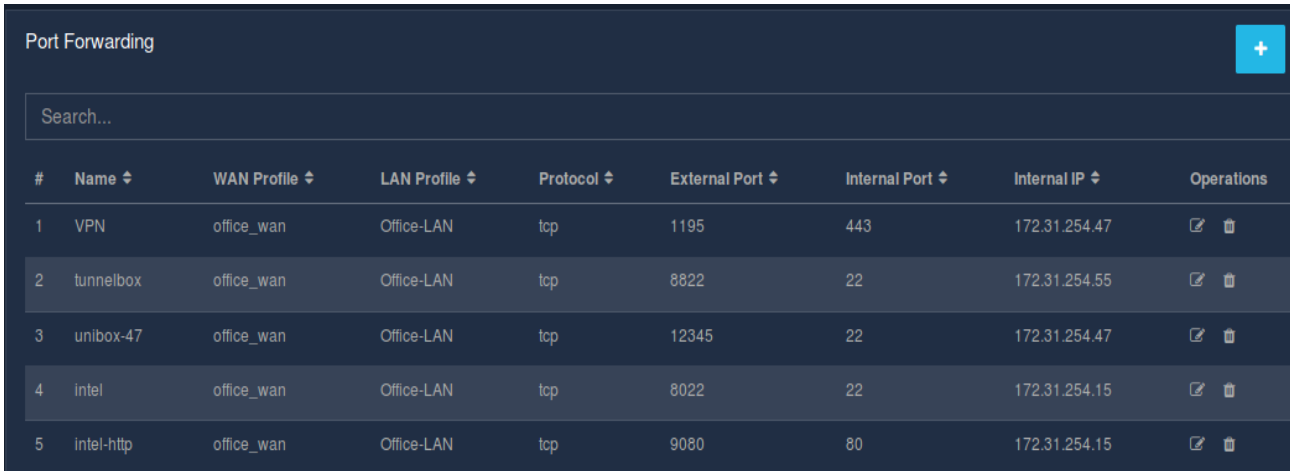


Fig 2.10.1.2

2.10.1.3 Edit Port Forwarding

To modify or make changes to an already existing NAT rule, click on the edit option present in the ‘Operations’ column in the ‘Post Forwarding’ sub-section of the ‘Routing’ section, found in the ‘Network’ module. A modal form displays all the previously acquired information to make the necessary changes.

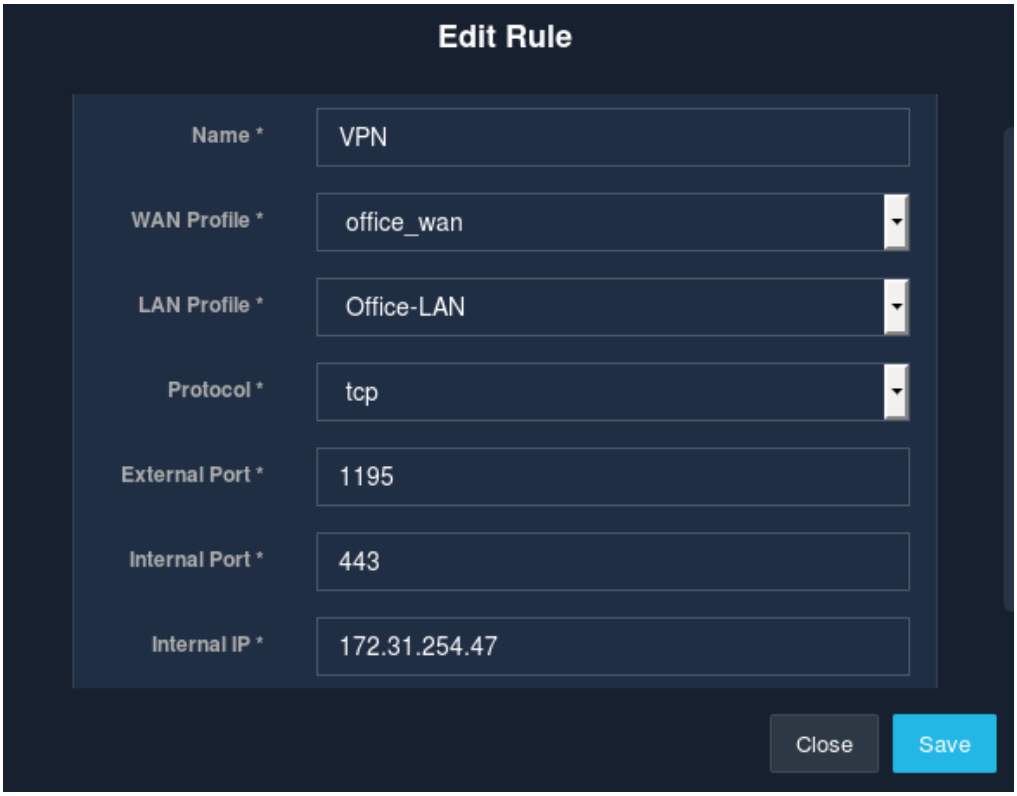


Fig 2.10.1.3

Click on the 'Save' button to set and apply all the changes made.

2.10.1.4 Delete Port Forwarding

Deleting a NAT rule is quite simple. Click on the delete icon present in the 'Operations' column in the 'Post Forwarding' sub-section of the 'Routing' section. A window displays a message to confirm the delete action.

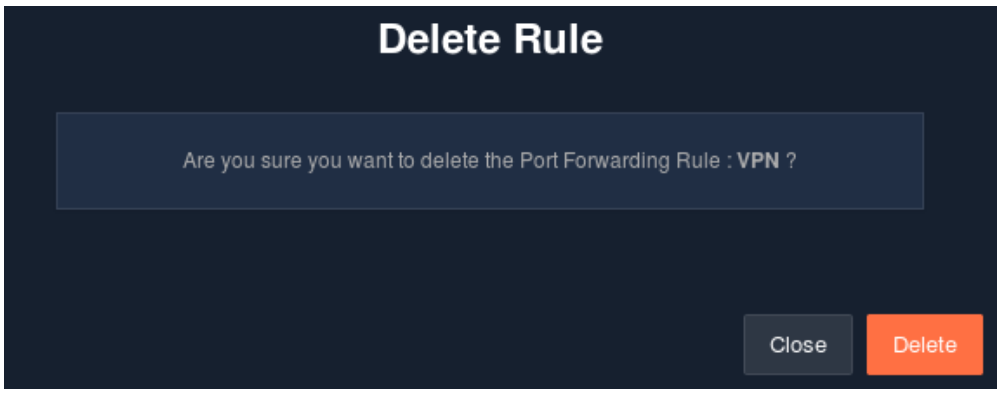


Fig 2.10.1.4

Click on the 'Delete' button to delete a NAT rule.

2.10.2 Group Routing

2.10.2.1 New Group Routing Rules

An admin is facilitated with the feature to configure a group routing rule in UniBox. The rule allows a specific group of authenticated users to access the LAN segment. Usually the rule is used to route the traffic to the server pool or the restricted subnets for a group of users.

To add a new group routing rule, go to the 'Network' module and select the 'Routing' section, followed by the 'Group Routing' sub-section. Then, click on the '**+**' icon which displays a modal form to collect information required to add a new group routing rule.

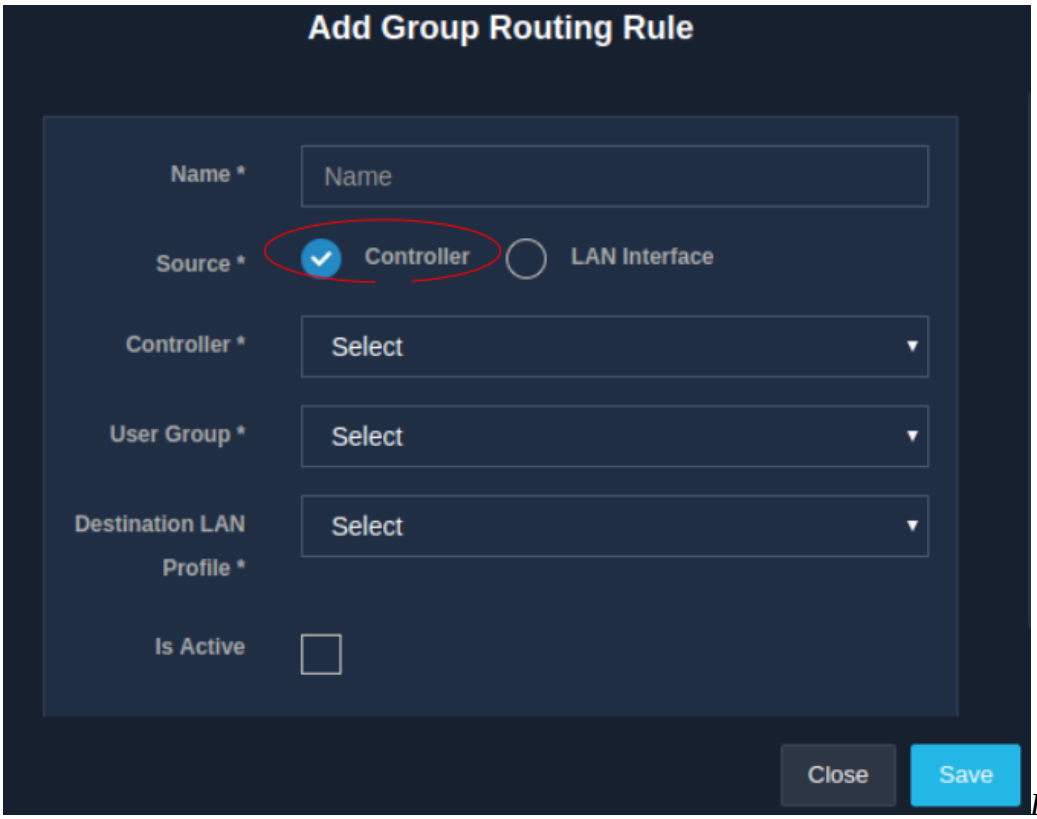


Fig 2.10.2.1 (a)

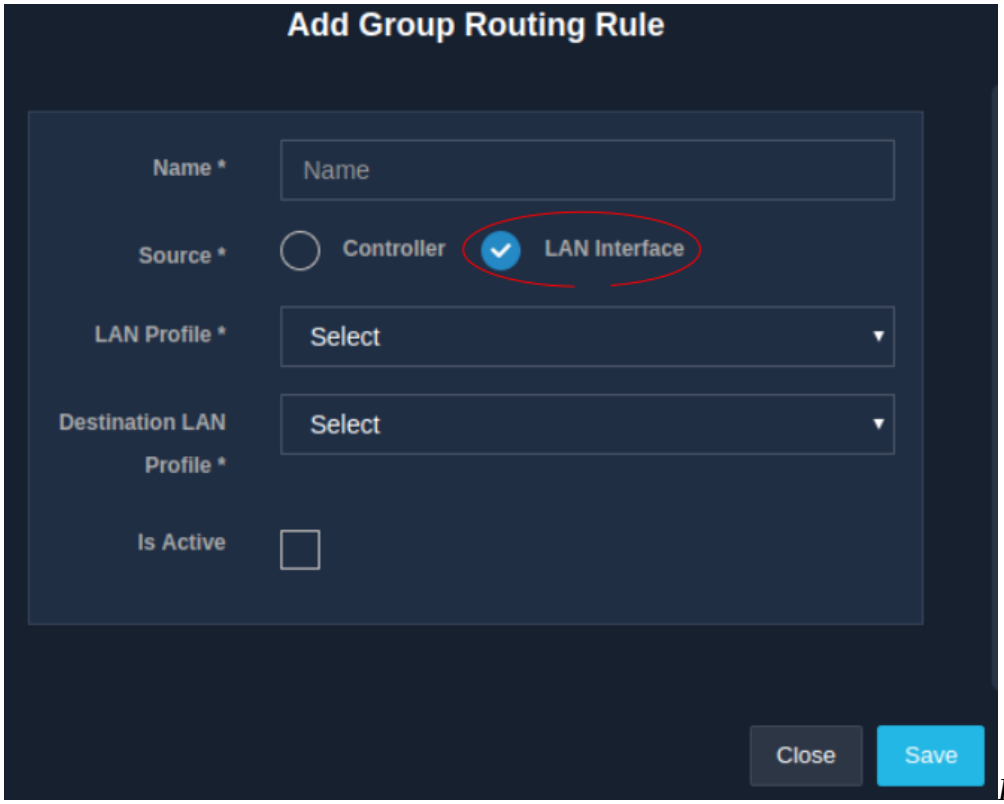


Fig 2.10.2.1 (b)

Fields	*Description*
Name	Enter the name of the rule.
Source*	Select the source, either LAN or controller. If the traffic from LAN side needs to access a specific LAN profile, then select the LAN interface source.
Controller	Select the controller profile on which the rule will be configured.
User Group	Select the user-group whose members will use the routing rule.
LAN Profile	Select the source LAN segment for the user-group.
Destination LAN Profile	Select the destination LAN segment for the group of users.
Is Active	Once the check-box is ticked-off, the rule will be applied effectively.

Table 2.10.2.1

Fill in the form with all the details, then click on the 'Save' button to add and apply the new rule.

Note: Depending on the source selected, that is either LAN or controller, the fields will change respectively.

2.10.2.2 List Group Routing Rules

All the routing rules configured for a specific group of users are listed down in a table. The routing rules will allow only a certain group of authenticated users to access the network segment. These settings are generally done to provide selective access to a subnet.

To view the list of group routing rules, go to the ‘Network’ module and then the ‘Routing’ section, followed by the ‘Group Routing’ sub-section. The list displayed with the name of the rule, the controller it is assigned to, the user group, the LAN profile, the destination LAN profile and whether the active status of the rule. The listing table also contains the ‘Operations’ column, giving the options to edit and delete the rules.

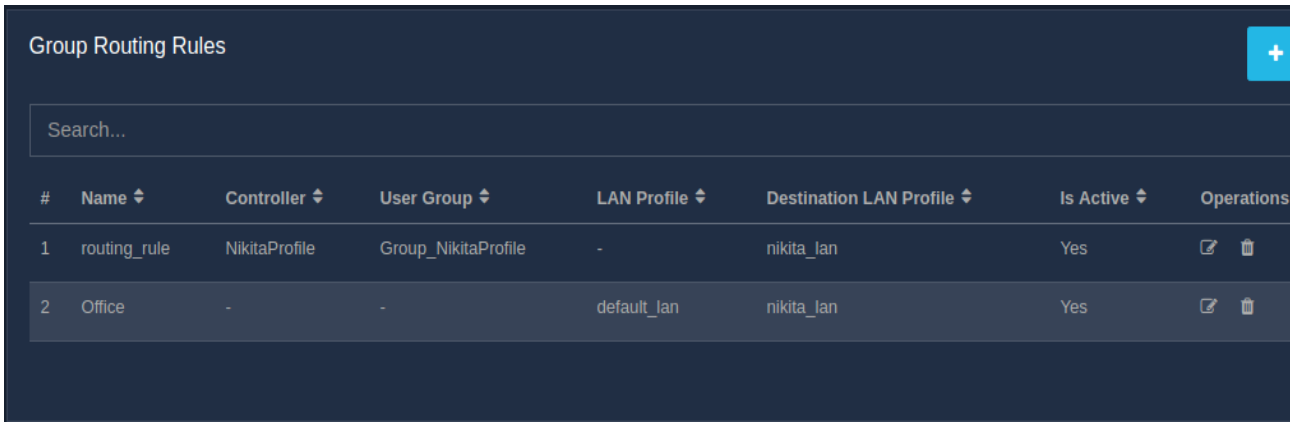


Fig 2.10.2.2

2.10.2.3 Edit Group Routing Rules

The edit feature allows an admin to modify or make changes to an already existing group routing rule. To modify a group routing rule, click on the edit icon present in the ‘Operations’ column in the ‘Group Routing’ sub-section of the ‘Routing’ section, that falls under the ‘Network’ module. A form appears on the window with the previously acquired information, to make the necessary changes. Refer.

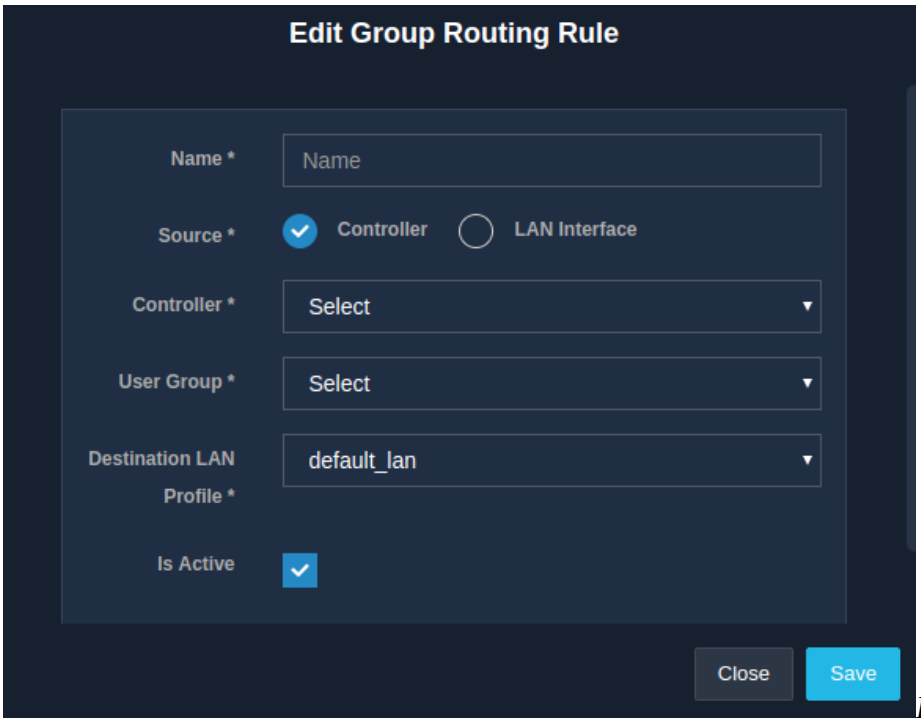


Fig 2.10.2.3 (a)

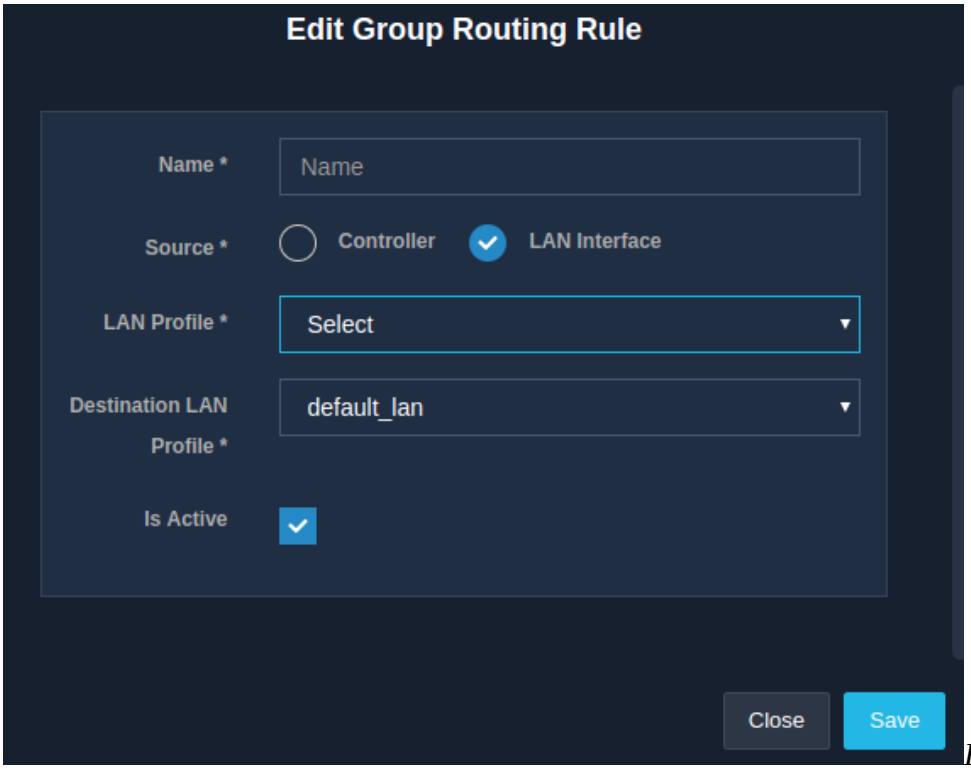


Fig 2.10.2.3 (b)

2.10.2.4 Delete Group Routing Rules

To delete a group routing rule, click on the delete icon present in the 'Operations' column in the 'Group Routing' sub-section of the 'Routing' section, under the 'Network' module. A message window appears displaying a message to confirm the delete action.

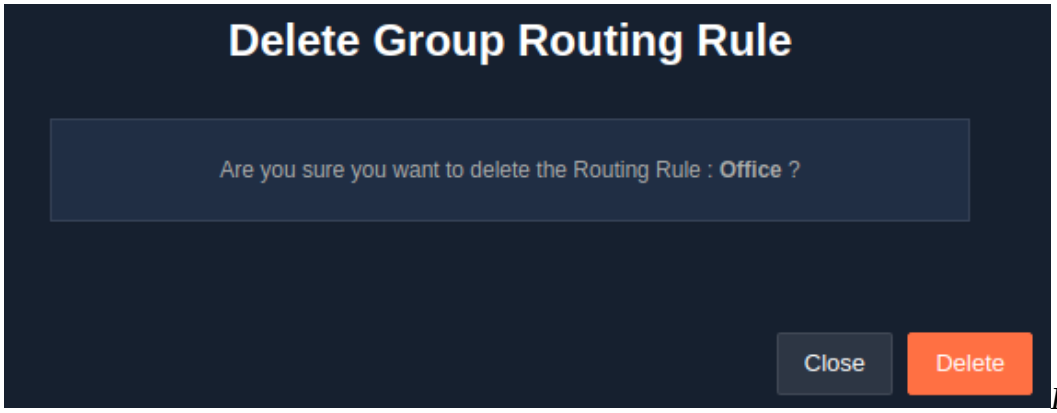


Fig 2.10.2.4

Click on the 'Delete' button to surely delete the rule.

3. Wireless

3.3 Wireless Client

This section displays the list of wireless clients connected/disconnected to the UniBox. Wireless clients are the devices that have obtained an IP address from the UniBox.

- This page displays all wireless clients connected/disconnected with the UniBox. Admin can search, paginate, and locate particular wireless client for details wireless view. Each row displays the information about the client including the MAC address, Tx/Rx rate, the RSSI value for the device, vendor of the device, access point name to which the client is connected and the SSID connected.
- Admin can view graphical RF history of the client by clicking on the + sign. The history is available for 2, 6, 12 and 24 hours. The graphs show the upload/download speed and signal strength over the given time interval. This view of the individual wireless client contains a time slot selection for data visualization to get more insight about wireless clients.
- Connected wireless client are those devices that are associated with the AP .
- Disconnected client means those clients which were connected to AP but are not connected with the AP from last 15 minutes.

3.3.1 List Wireless Clients

This page displays the list of wireless clients present in the UniBox. The tabular format displays the MAC Address, Rx Bit Rate, Tx Bit Rate, Time Last Seen, RSSI, Vendor Name, AP Name, SSID and the status of the client.

It also allows to search for the wireless client by providing a search option based on MAC Address and the AP Name. Click on the 'Search' button once the desired search criteria have been provided and the list of wireless clients will be displayed.

The list can be sorted in ascending or descending order using the icon on each column header.

Also the status (connected, disconnected) buttons are provided. Clicking on the ‘Connected’ button would then display the list of devices which are connected and having the status as ‘UP’. And on click of the ‘Diconnected’ button the devices with status ‘Down’ would be displayed.

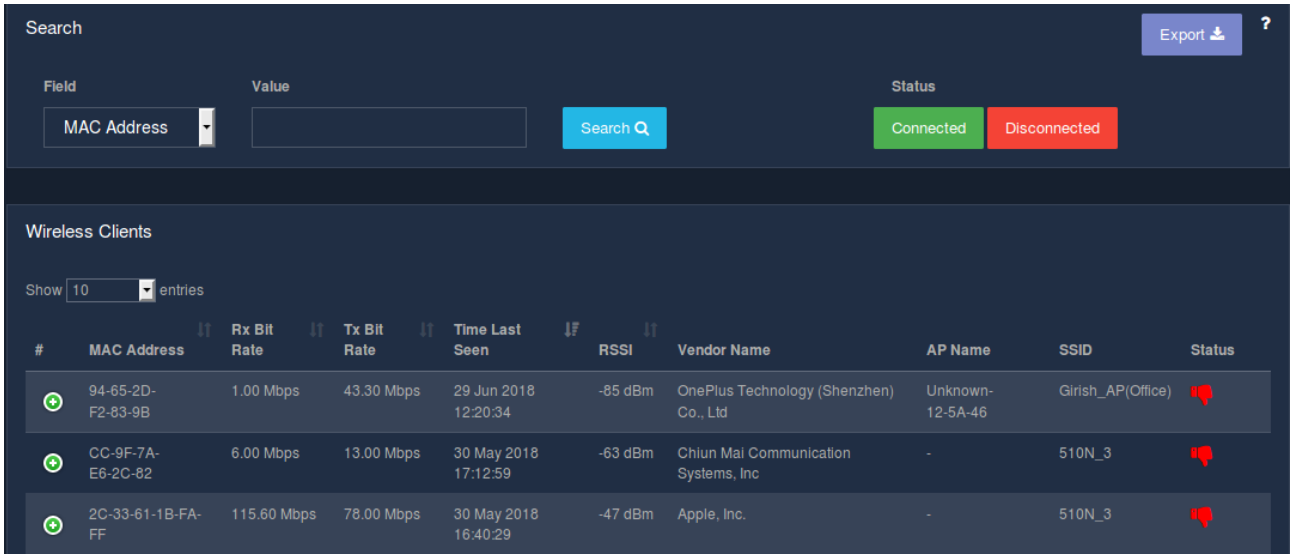
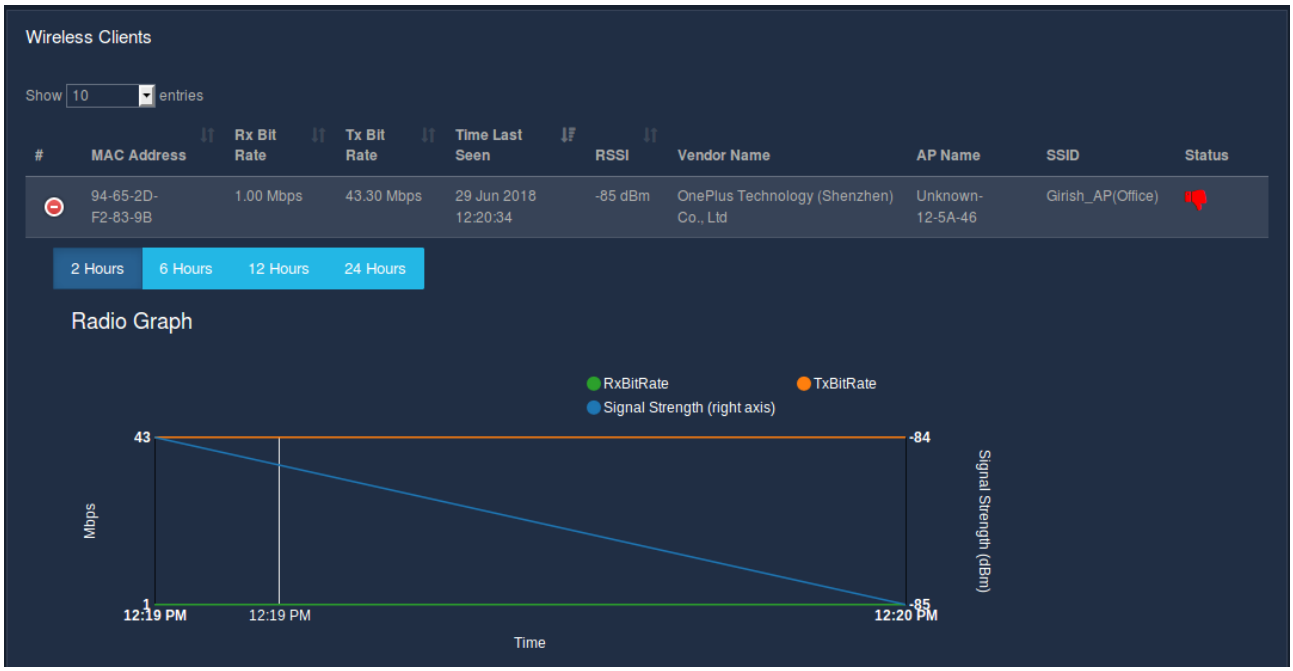


Fig 3.3.1

The (+) icon corresponding to the mac address displays the graph based on the data captured.



Fig

3.3.2 Export Wireless Client

This section allows to download the current list of the connected clients. The report is downloaded with the name WirelessClient.csv .

The file downloaded follows the following format:

- Mac Address
- RX Bit Rate
- TX Bit Rate
- Last Checking Time
- RSSI
- Vendor Name

- AP Name
- SSID
- Status

To export the list of wireless clients, click on the ‘Export’ button.

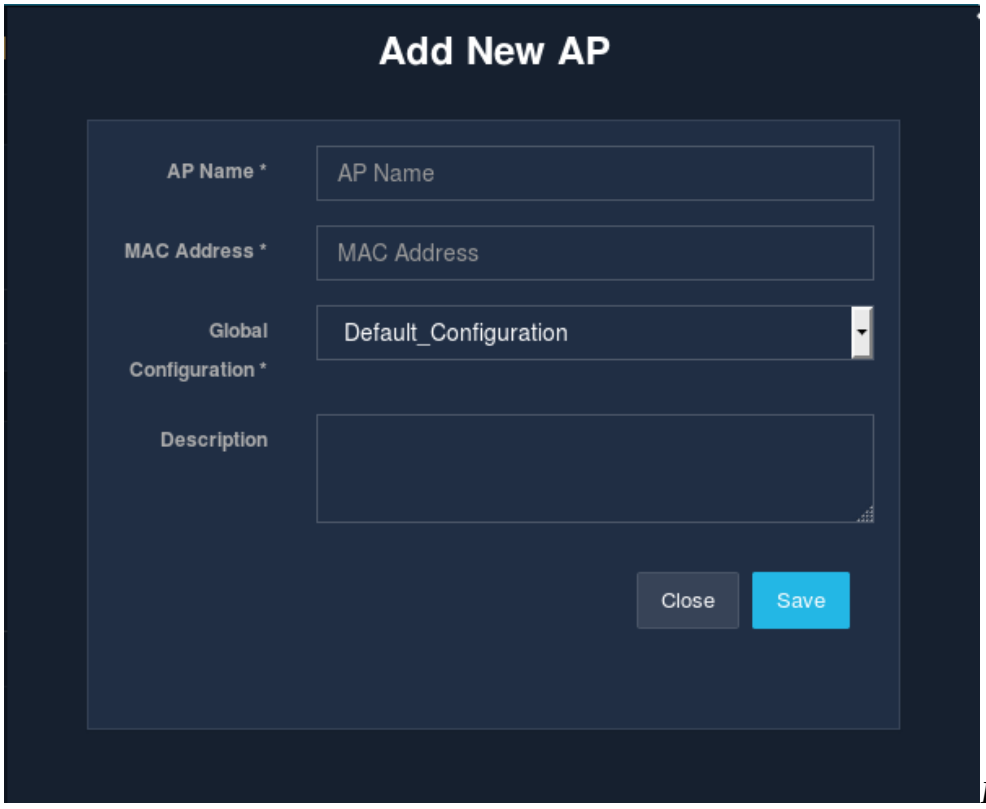
3.2 Manage AP’s

3.2.1 Creation

This page allows administrators to add a new AP for management. If Unibox is used within a wireless network, then administrators can provision all the access points in Unibox for management. Unibox will check the status of all APs periodically and will display the status of the AP. For AP Management AP Name and MAC address of the AP is required.

To add a new access point, click on the ‘**+**’ icon. A modal form will be displayed that collects the information required to create a new AP.

The fields marked with asterisk (*****) are mandatory.



Fig

Click on the ‘Save’ button to add a new AP.

Fields	*Description*
AP Name	Enter the name of AP.
Mac Address	Enter the MAC address of LAN port of the access point.

Global Configuration	Select the configuration to apply to the AP. The AP will get all the settings applied to the global configuration.
Description	Enter the description for AP.

Table

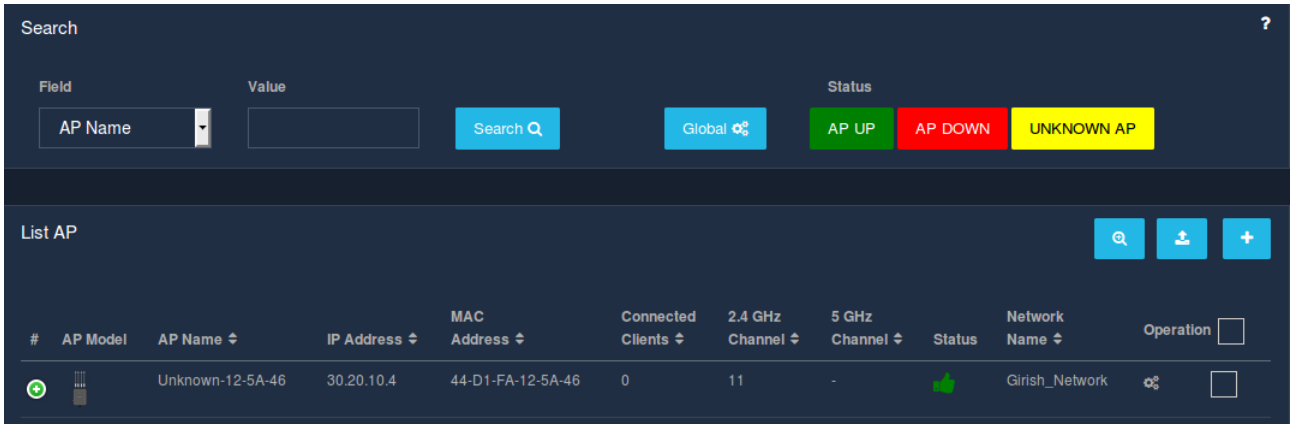
3.2.2 List AP's

This page displays the list of UniMax access points that are provisioned for central management. These APs can be either manually added to the list or can be provisioned automatically using the auto-discover feature.

Each line displays the AP information along with the current status of the AP. The first column displays the image (model) of the AP being managed. The name of the AP, private IP and MAC address of the AP are also displayed. The table also displays the number of clients connected to each AP along with the channel information for both 2.4 and 5 GHz radios. It also displays the status and the network name of the AP. The last column, i.e., the 'Operation' column, allows an admin to configure or delete the AP from the management.

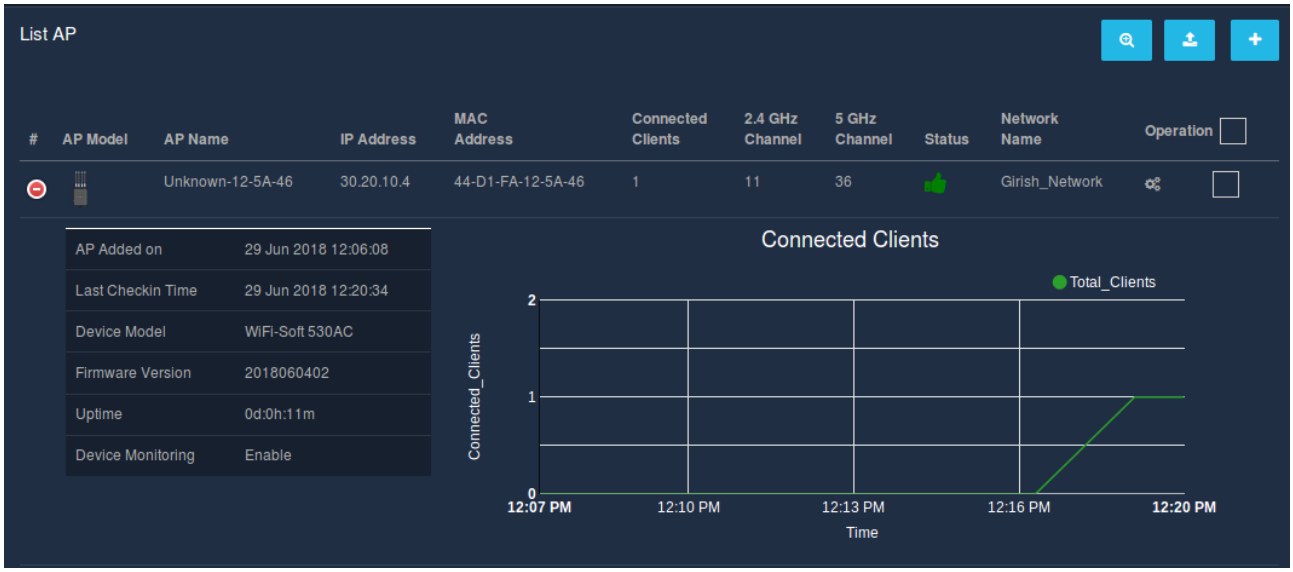
This section is also used for push configuration changes to all the managed APs. The admin can filter the AP list by clicking on one of the buttons; UP, DOWN and UNKNOWN.

Several buttons are available to set the default network configuration, view the auto discovered APs or import the list of APs from CSV file.



Fig

An admin can view more statistics including the time graph of each AP by click on the (+) sign on each line corresponding to each of the AP.



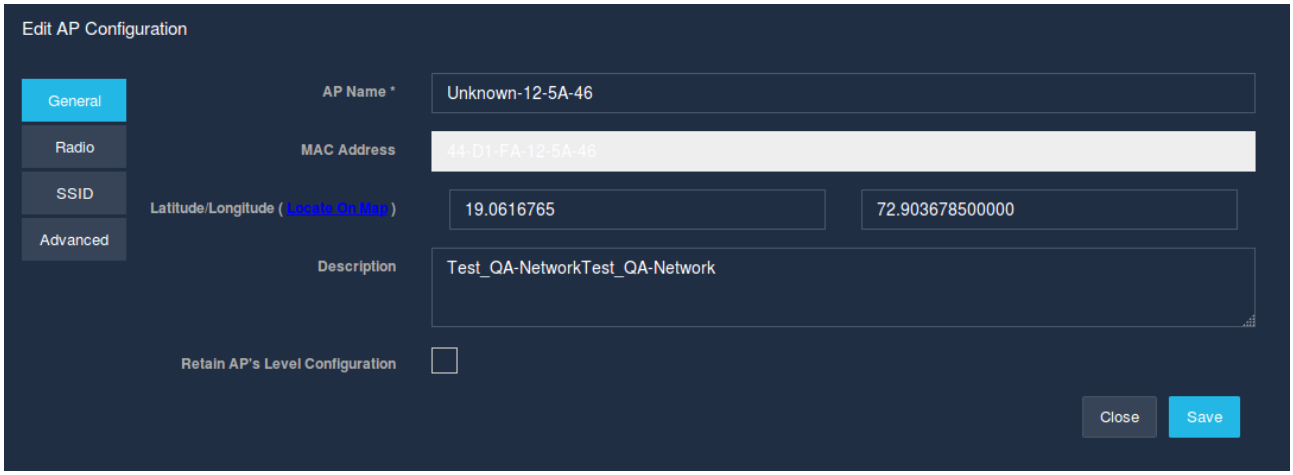
Fig

3.2.2 Edit Configuration

This page allows the administrator to edit the Access Point information. To change the access point information, change the necessary attributes and click the submit button.

The edit AP configuration allows the administrator to edit the different subsections in the AP section. The edit AP configuration is sectioned into four sub-sections:

- **General**



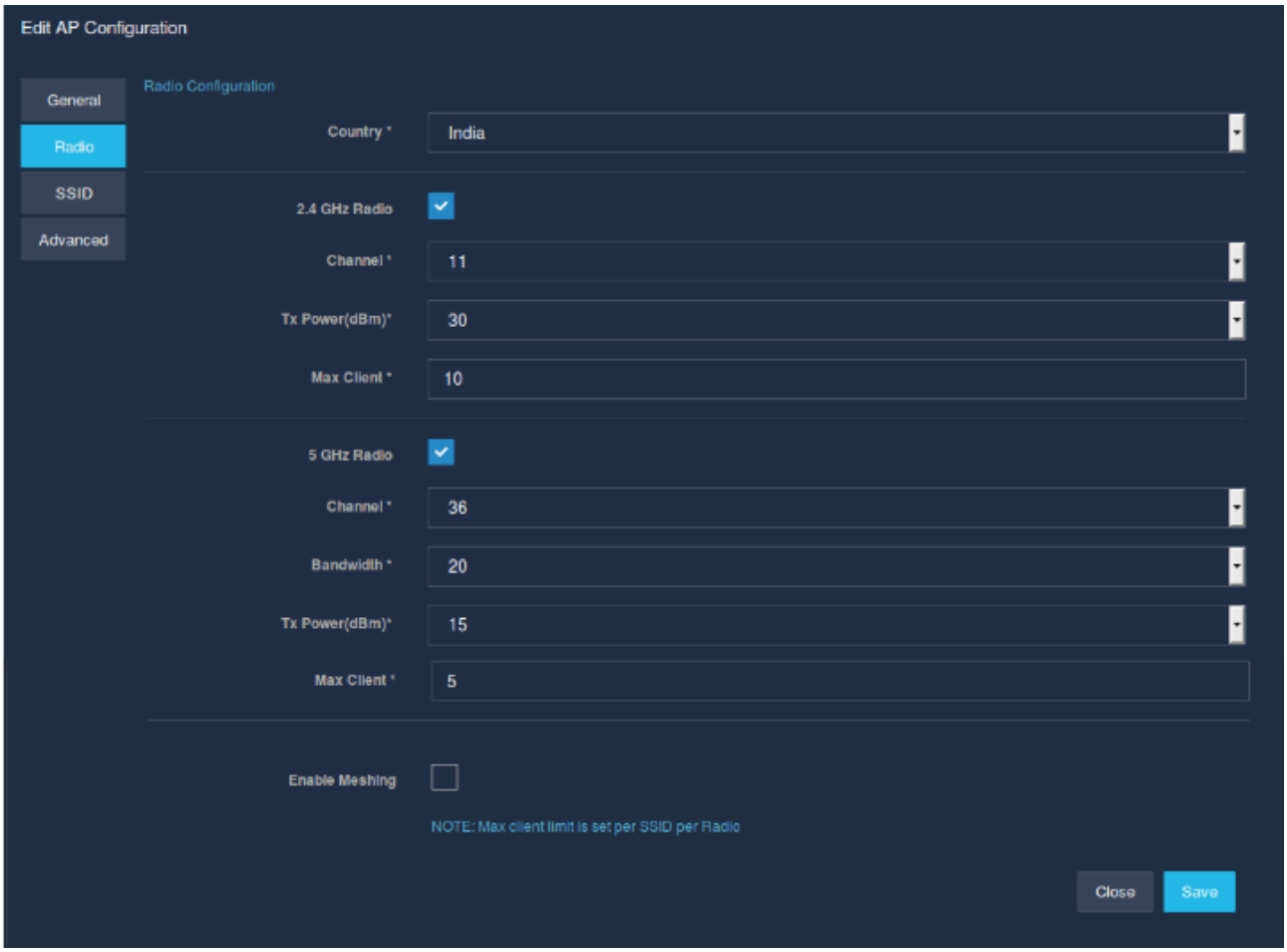
Fig

Fields	*Description*
AP Name	Enter/Edit the name of the AP.
MAC Address	Enter the MAC address of the access point. This field is uneditable. To change the MAC address, you need to delete and re-add the AP.
Latitude/Longitude	Enter the latitude and longitude of the AP or select from the google map.
Description	Enter the description for AP.

Retain AP’s Local Configuration	Check this box for overriding the default configuration with the AP's configuration.

Table

- **Radio**



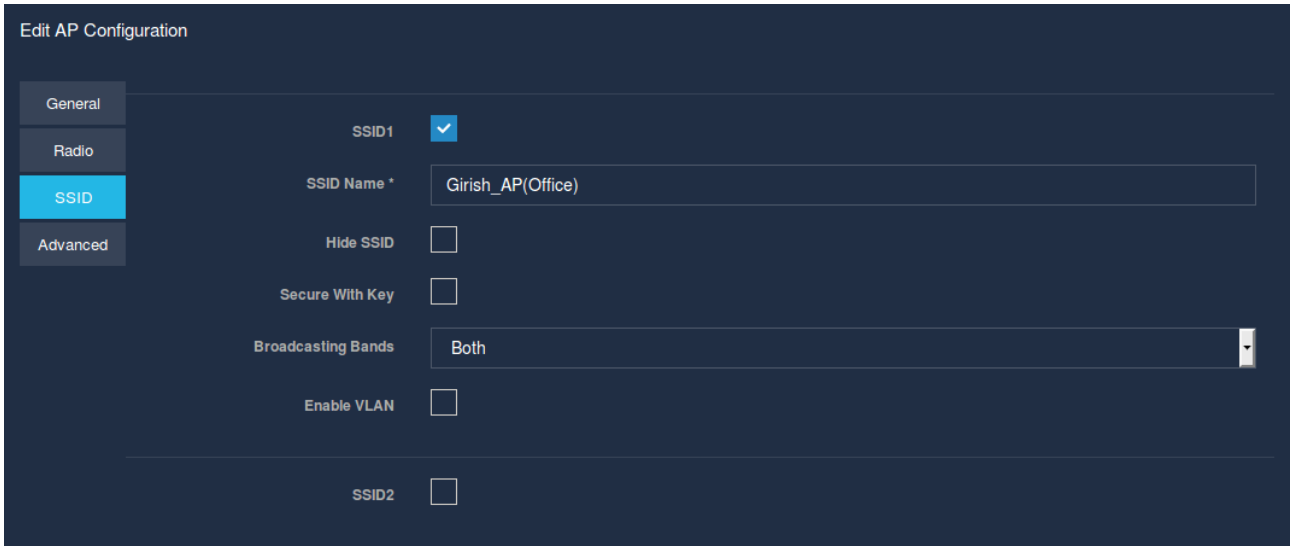
Fig

Fields	***Description***
Country	Select the country in which your AP is located. The available channels will change based on the selected country.
2.4GHz	If the AP has 2.4 GHz radio, select this option.
5GHz	If the AP has 5 GHz radio, select this option.
Channel	Set the channel for operating the given radio. If the Auto option is selected, the AP will automatically decide the best channel for operating.
Tx Power	Set transmit power for the selected frequency band in DBm.
Max Client	Enter the maximum number of clients that can connect on the selected band. AP will refuse additional device once this limit is reached.

Bandwidth	Select the desired bandwidth (only in case of 5Ghz).
Enable Meshing	To enable WiFi meshing, check the mesh option. A wireless mesh network (WMN) is a mesh network created through the connection of wireless access points installed in each network user's locale. Generally recommended for dual or higher band radios. It is important that all APs must be on the same frequency band for meshing to work.

Table

- **SSID**

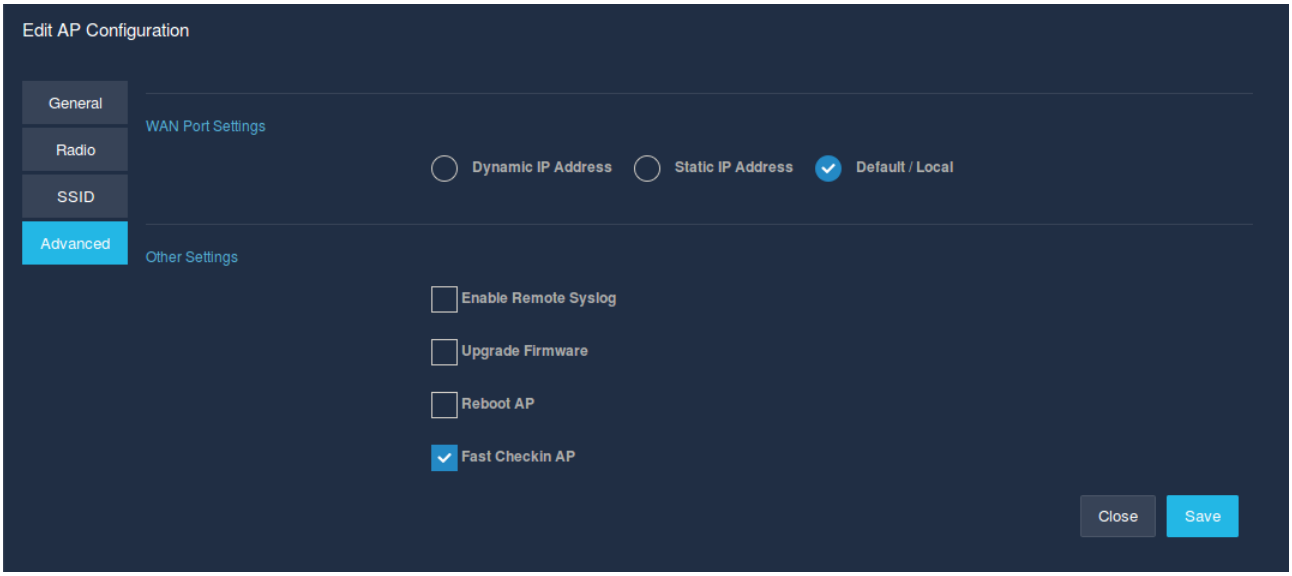


Fig

Fields	***Description***
SSID1	On ticking-off the checkbox, the data needed to set the SSID will be captured.
SSID Name	Set the broadcast name of the network.
Hide SSID	If checked, the AP will not advertise the SSID. Clients will have to enter the SSID manually to connect to the AP.
Secure with Key	Check this option to enable WPA2 security key.
WPA2-PSK Key	Enter 8 characters or longer key for securing the network. Only PSK keys are supported.
Broadcasting Bands	Select broadcasting band (2.4, 5 or both) for the SSID
Enable VLAN	Set ID of VLAN for tagging. All the traffic connecting to the AP on the given band will get tagged with the configured VLAN ID.

Table

- **Advanced**



Fig

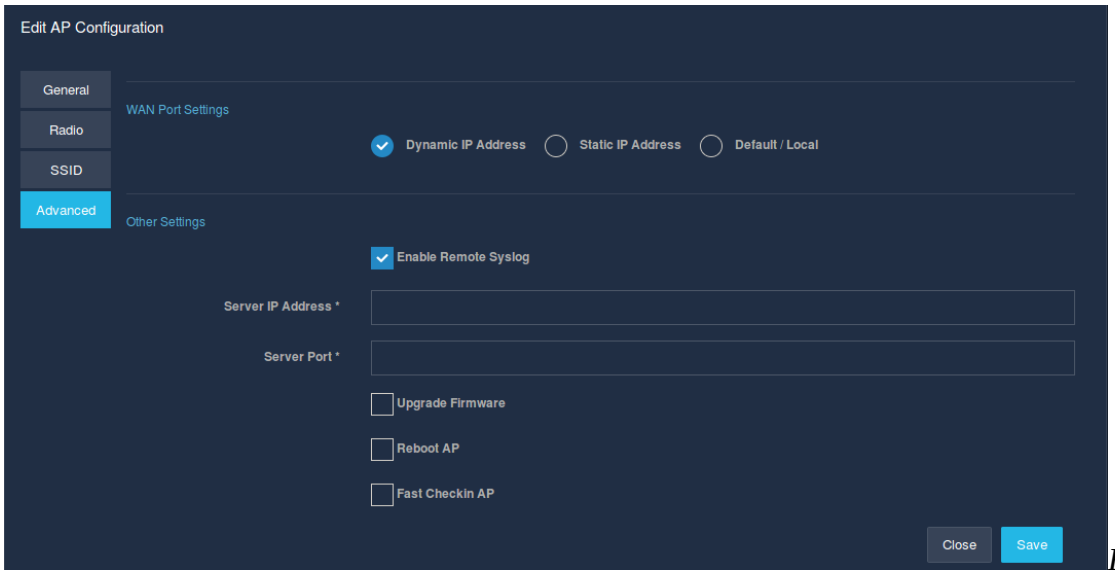
The advanced WAN port settings are categorized into three sections:

- Dynamic IP Address
- Static IP Address
- Default/Local

Select whether the APs WAN port will be on static, dynamic or local IP. Generally it is advisable to leave the AP on a dynamic IP.

In case of dynamic IP address and default or local, the following fields appear:

- Enable Remote Syslog

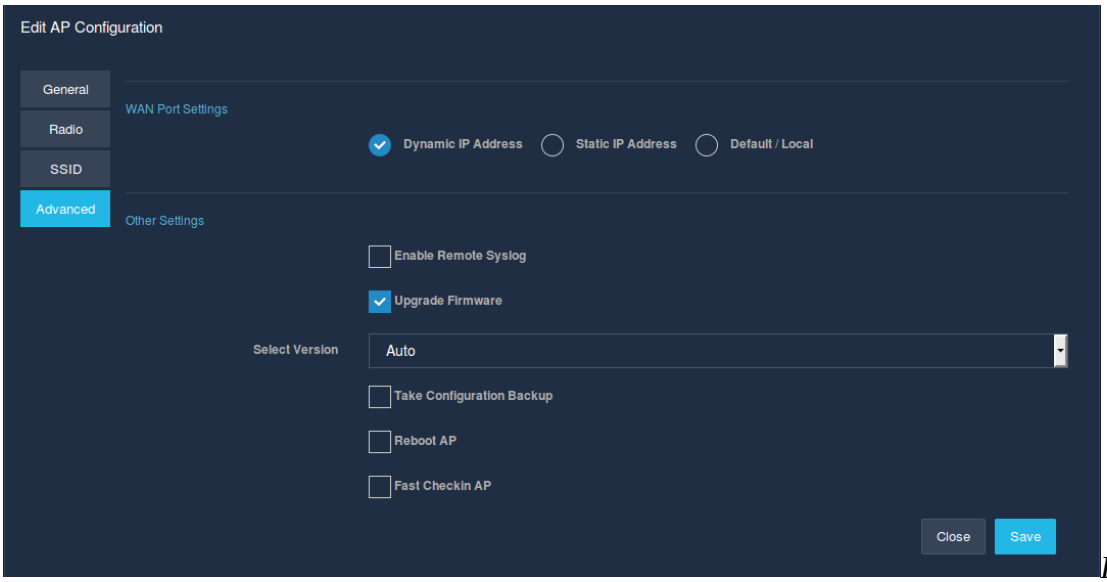


Fig

Fields	*Description*
Server IP Address	Enter a valid IP address of the server.
Server Port	Enter the port number of the server.

Table

- Upgrade Firmware

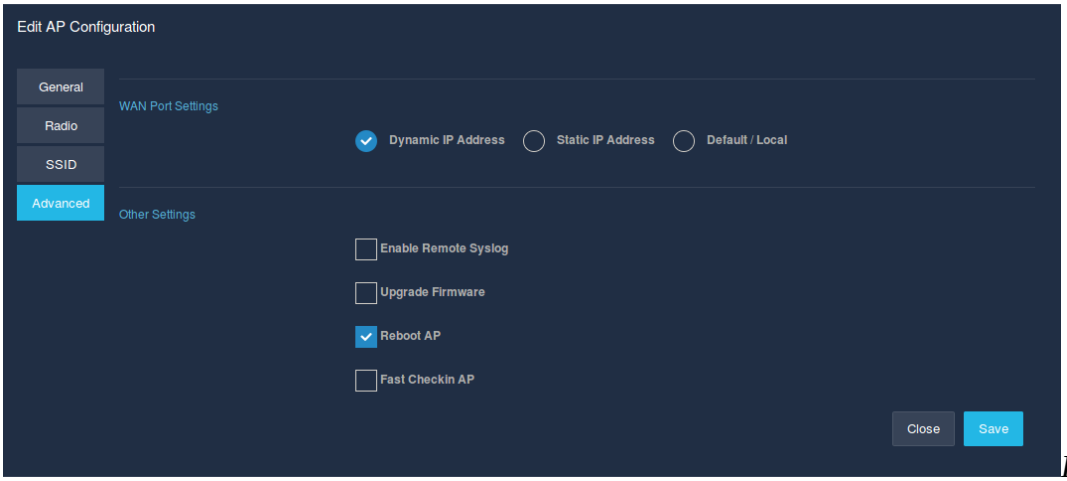


Fig

Fields	Description
Select Version	Select the version.
Take configuration Backup	Check the checkbox if there is a need of saving the existing configuration backup.

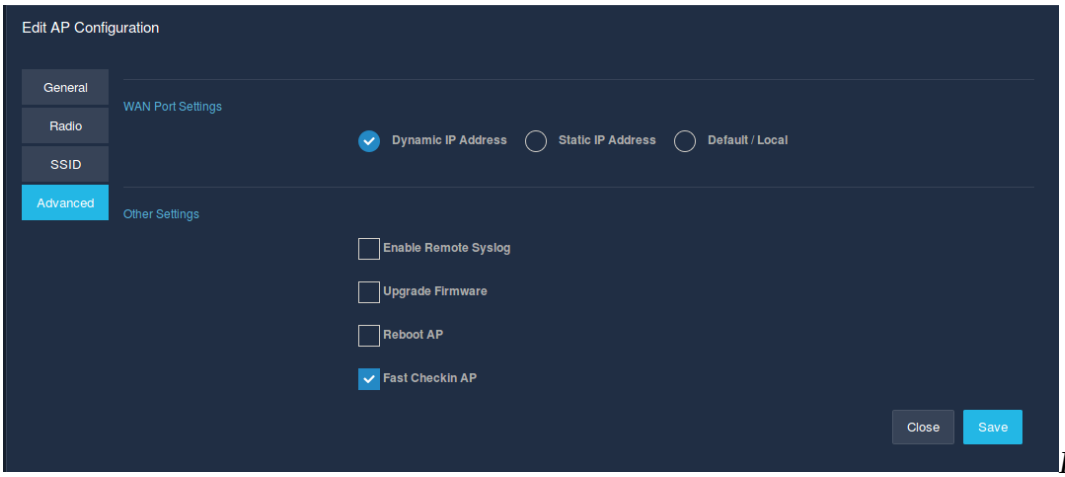
Table

- Reboot AP



Fig

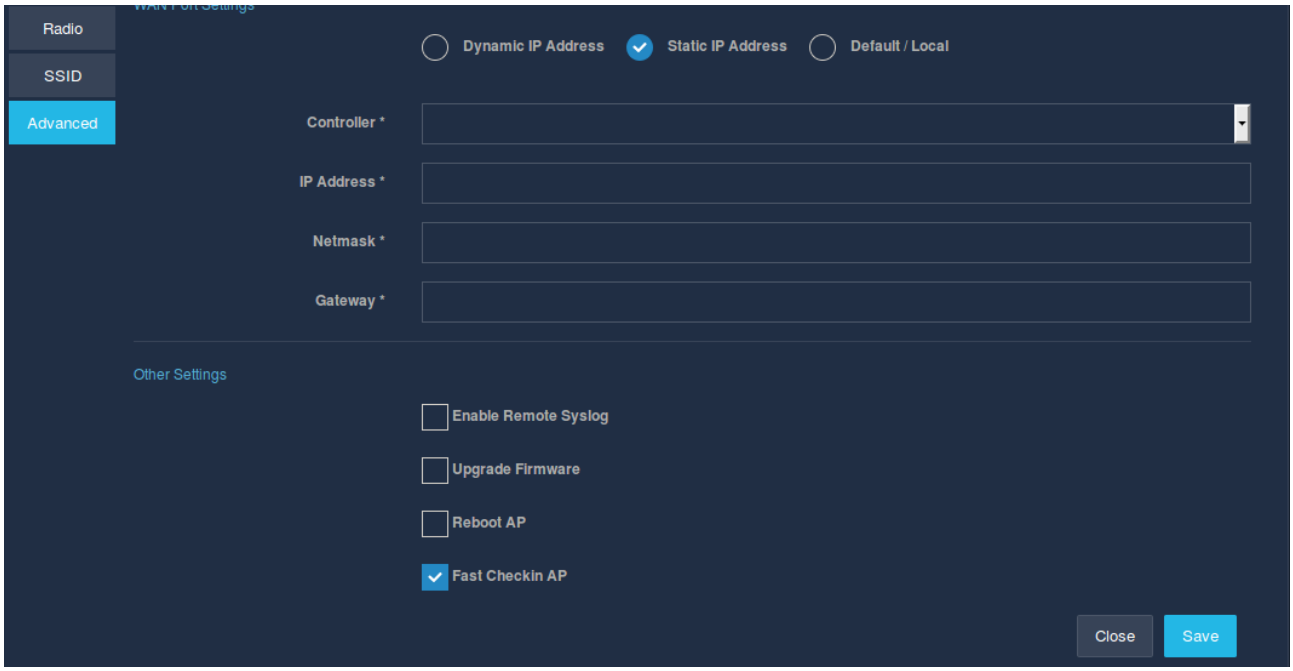
- Fast Checkin AP



Fig

Enable this option during troubleshooting the AP. This will enable faster checking of the AP. Revert back the change once the debugging is complete.

When we enable the static IP address, it prompts for entering the data in the following fields which are mandatory:



Fig

Fields	***Description***
Controller Profile	Select the controller profile for static IP.
IP Address	Enter the IP Address.
Netmask	Select the subnet mask.
Gateway	Enter the gateway IP.

Table

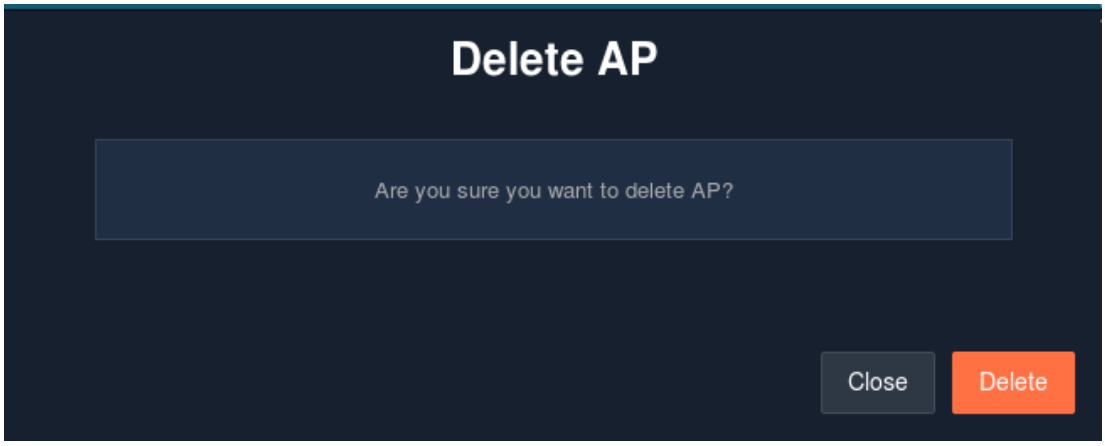
Click the ‘Save’ button to save the new AP configuration.

3.2.3 Delete AP Configuration

This page deletes an existing Access Point from the management list. All the information about the AP including the configuration information and monitoring will be lost. Please note that this will not change any settings on the AP and the AP will continue to operate on the last known configuration.

Click on the 'delete' icon, in the 'Operations' column, to delete an existing AP configuration. Once clicked, a message asking for the confirmation of the delete operation pops up.

If you are sure, go ahead and click on the 'Delete' button.



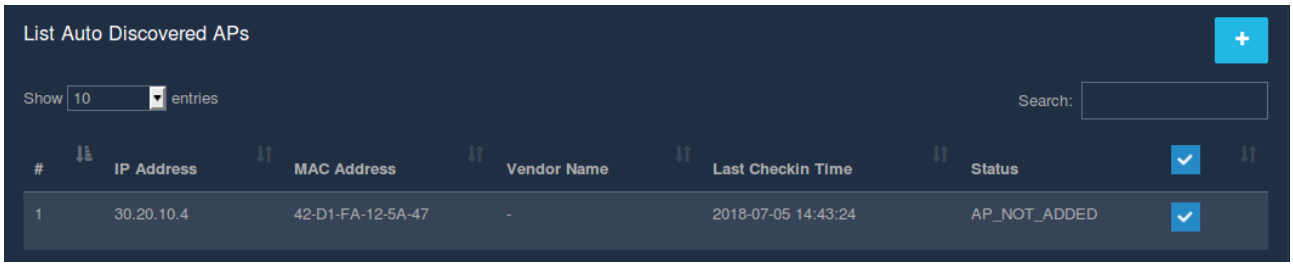
Fig

3.2.4 Auto Discover AP

This page displays the list of APs that UniBox has auto-discovered and have not been provisioned for management. All managed UniMax access points use a special protocol to advertise their presence on the network. UniBox discovers the UniMax APs and checks whether they are already added for management.

If the APs are not managed, UniBox will display them in the list. An admin can review the APs and can provision them for management.

This page displays all the APs which are under Unibox but not authenticated and provisioned for Management. The list displays the IP Address, MAC Address, Vendor Name, Last Check-in Time and the status. To add, click on '**+**' button.



Fig

3.2.5 Import AP

The file to be imported should be in CSV format. The file should contain the name and

MAC address of the AP. The MAC address of the AP should be separated by dash.

Fig

Fields	***Description***
Global Configuration Profile	Select the global configuration profile.
File to import	Select the valid csv file that is to be imported.

Table

Click on the 'Import' button to import the file in the database.

3.2.6 Global Configuration

This page displays all the global configurations.

The table displayed consists several information like Network Name, Created Date and Description.

The page provides an option to edit or delete a global configuration. The global configuration contains the default settings that will be applied to all APs under management.

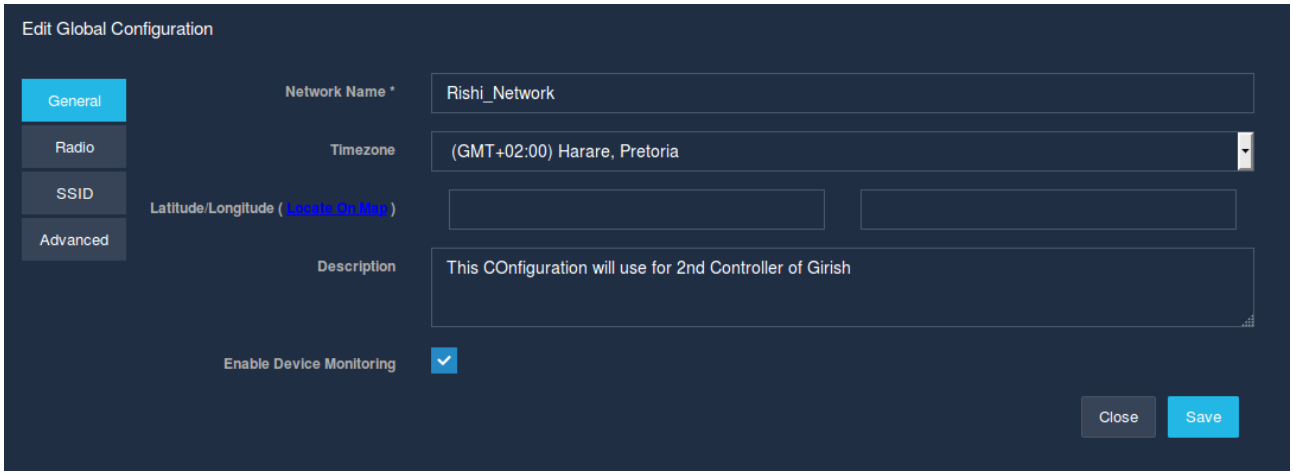
Fig

The administrator is provided with the operations like add, delete and edit the global configuration.

3.2.6.1 Edit Global Configuration

This page allows the administrator to change an existing global configuration.

The 'Operations' column in the list allows an admin to make changes to the global configuration. To edit a global configuration, click on the edit icon. The changes made will be applied only when the changes are saved. So click on 'Save'.

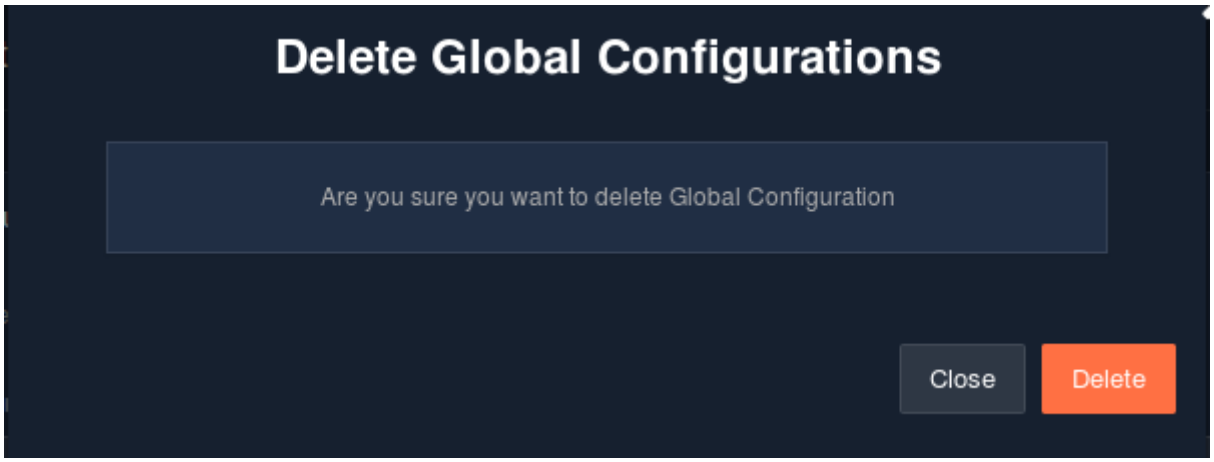


Fig

3.2.6.2 Delete Global Configuration

This page deletes an existing global configuration.
Click on the 'delete' icon, in the 'Operations' column, to delete an existing global configuration. Once clicked, a message asking for the confirmation of the delete operation pops up.

If you are sure, go ahead and click on the 'Delete' button.

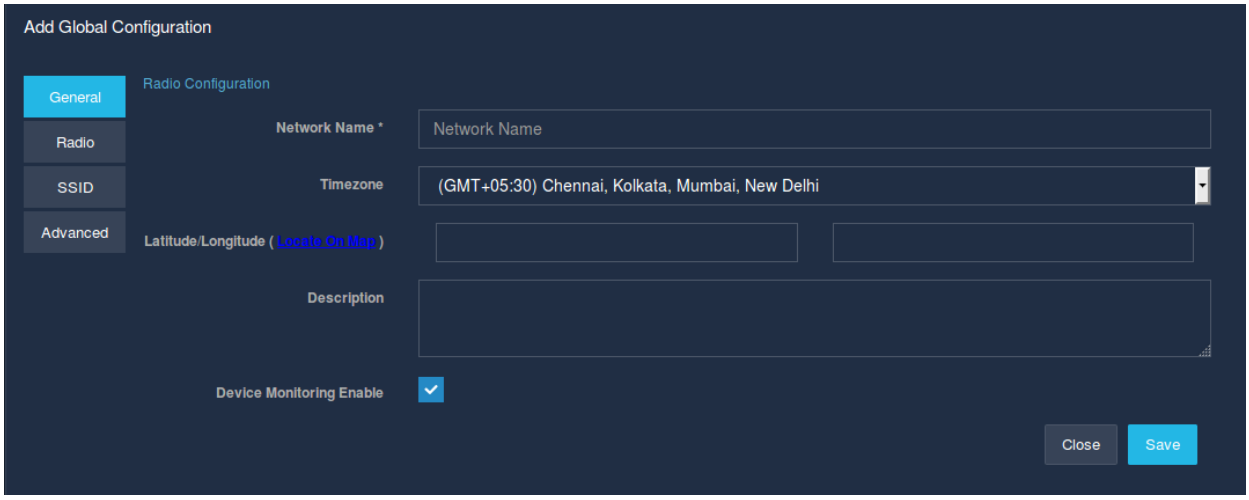


Fig

3.2.6.3 Creation

Click on the '**+**' icon to create or add a new global configuration in the Unibox. A data capture page will be displayed that collects the information required to create a new global configuration. Click on the 'Save' button to save the data into the database.

The fields marked with asterisk (*****) are mandatory.



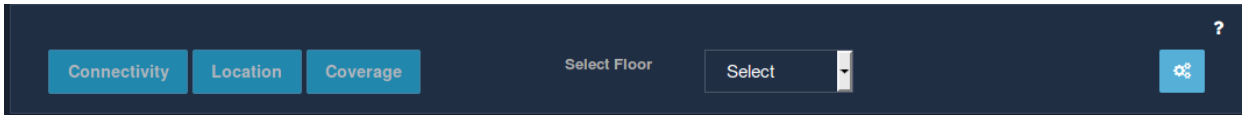
Fig

Click on the 'Save' button to save the global configuration. A new global configuration will be added in the Unibox.

3.3 Heatmap

This section provides the administrator a detailed view of the radiation pattern from each AP (access points) that are configured with the Unibox. This page is sectioned into 3 parts:

- Connectivity
- Location
- Coverage

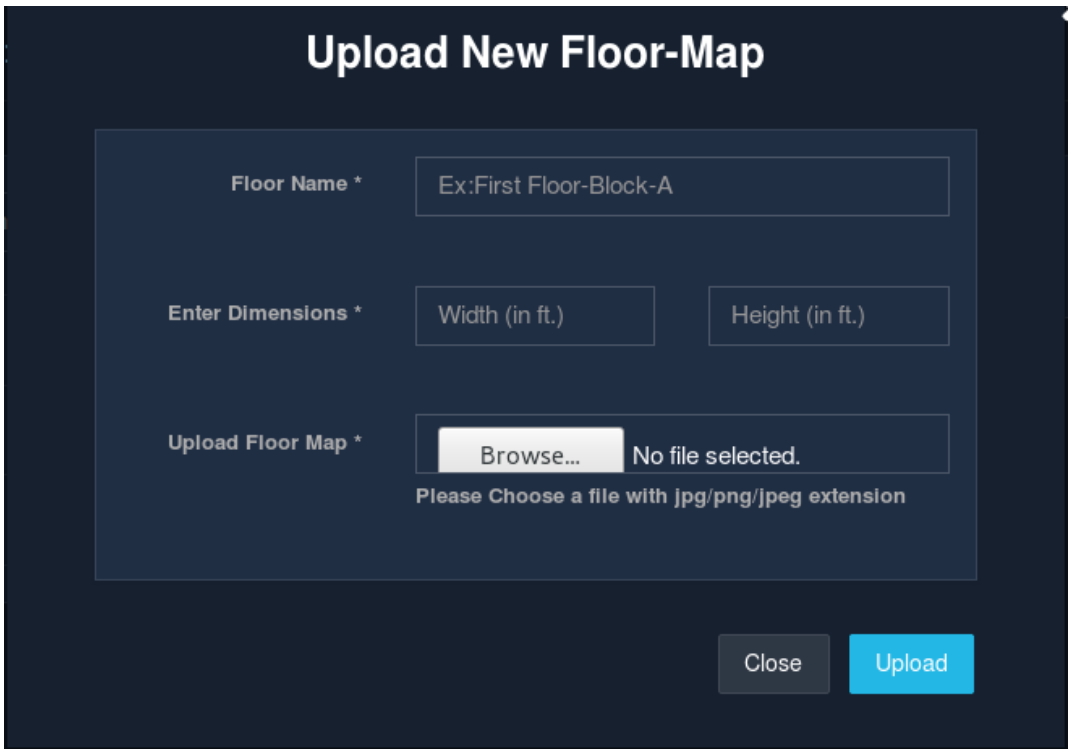


Fig

The above features will only be enabled, only when you select a floor. In order to add a new floor map, click on the 'Configure' button placed in the right. This button will redirect to the dashboard section. Click on the '**+**' icon to add a new floor map. A modal will then appear that consists of the following fields:

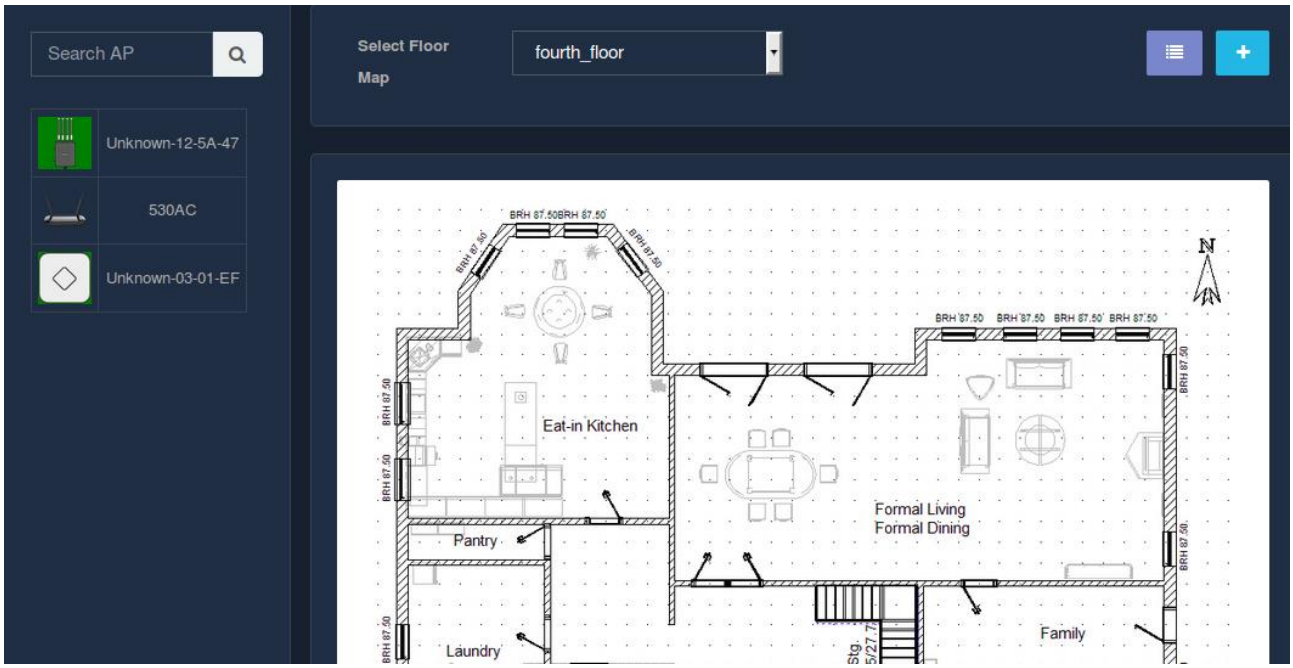
Fields	***Description***
Floor Name	Enter a unique name to the floor.
Enter Dimensions	Enter the dimensions in terms of height and width.
Upload Floor map	Upload the map of the floor where the AP will be located.

Table



Fig

Click on the 'Upload' button to add a new floor map in the Unibox. Once the floor map has been uploaded, select the floor that has just been added. The image would appear in the center like below:



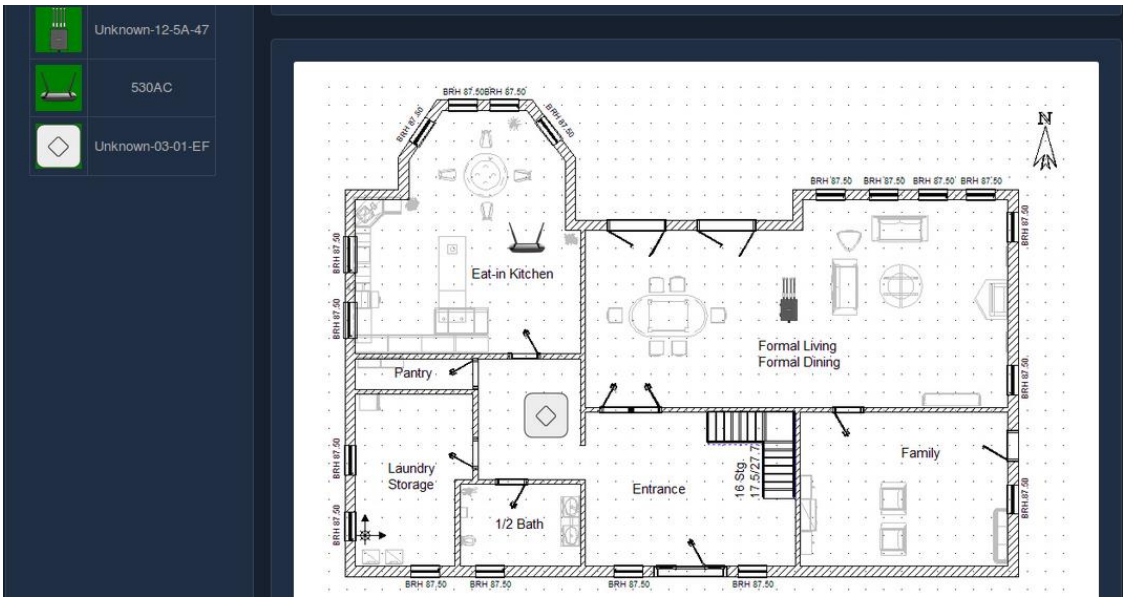
Fig

Now click on the AP's provided in the left corner. You can place these AP's wherever you wish to on the selected floor. There is also a search option provided for the AP's. All you have to do is 'Drag and Drop'. Select the type of AP , drag it and drop it to the required position on the floor.

In order to make the process simple and easy, heatmaps have been implemented in a way that :

- No two floors should have the same image (floor map).
- The same AP should not be placed more than once on a floor.
- If you change the floor through the dropdown and drag and drops the same AP which is already used for any other floor in the Unibox, will result into popping-up of the confirmation message asking you whether you are sure of moving the AP from previous to this new floor. If you are sure about moving the AP, click on the 'Yes' button.

After you drag and drop the AP's, the floor map would appear something like this:



Fig

The three major features are explained below :

- <u>Connectivity</u>:

This feature gives the administrator an understanding about the number of devices connected to the AP on a given floor. Basically, a circle is generated near the AP indicating the devices connected. If you hover the mouse on the AP, it will show the number of devices connected. Three different colors are used to represent the number of the devices connected to the AP, namely,

  - Green – A green circular area indicates the number of devices connected are between 1-2.
  - Yellow – This color indicates that the number of devices connected is between 2-4.
  - Red – A red circle is generated if the number of devices connected are 5 or greater than 5.

The below screenshot shows 3 APs out of which only 1 AP has the connectivity area shown. Since to the rest of the two, there are no devices connected.

Fig

- Location:

This feature is basically to get the location of the user/device. It helps you in tracking the user via the location. Each of the user's location is marked accordingly on the floor map.

- Coverage:

Coverage basically indicates the range at which the signal can be reached. Each of the AP's would have different coverages dependent on the type of AP. The coverage is represented by 3 different colors:

  - Green: The circular area filled with green indicates a strong signal. So all the devices close to the AP will have a strong signal and will be under the area filled with green.
  - Yellow: Yellow represents average/medium signal strength. The devices falling in this range would have a slightly weaker signal than that of the ones falling under green.
  - Red: The red area indicates a weak signal. These are the devices located far from the AP. Due to which the signal quality reduces.

Fig

The above screenshot represents 3 different AP's placed on the same floor. Each of these APs have different coverages. Hence the diameter of the circle differs.

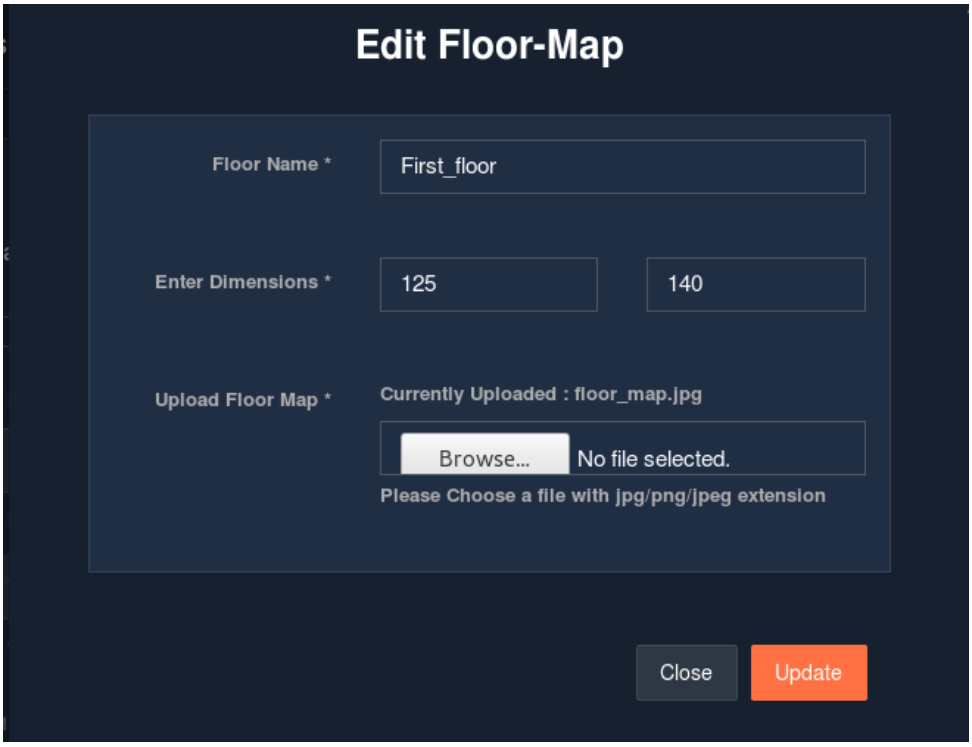
3.3.1 List Floor Map

This section allows the administrator to view the list of floor maps created in the Unibox. The table displayed lists down the floor name,floor map name,floor map width,floor map height,created date and the date at which it was last updated. It also allows to perform the searching operation.

Fig

3.3.1.1 Edit

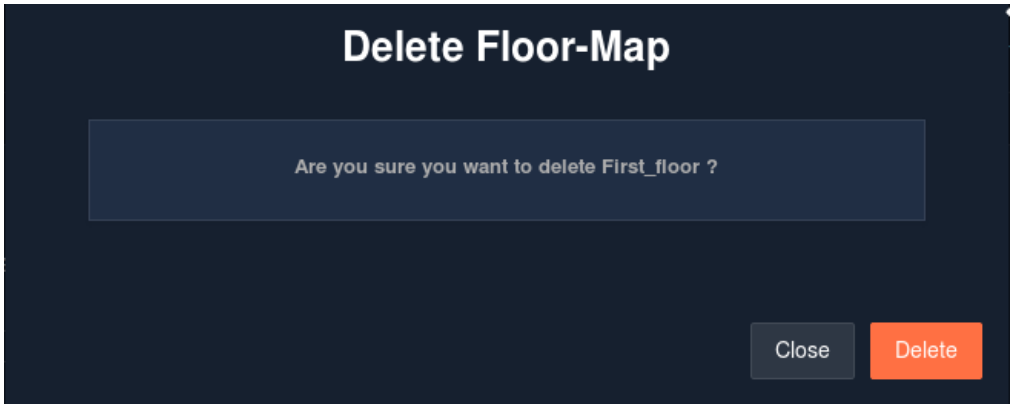
This page allows an administrator to change an existing heat map information. The 'Operations' column in the list allows an admin to make changes to a floor map. To edit an existing floor map, click on the edit icon. A modal is displayed which then captures all the updated information. The changes made will be applied only when the changes are saved. Click on 'Update'.



Fig

3.3.1.2 Delete Floor Map

This option allows the admin to delete an existing floor map from the database. Floor maps once deleted, cannot be restored. To delete the floor map, click on the 'Delete' button in the 'Operations' section. A confirmation message pops up to confirm the delete action. Once sure, click on the 'Delete' button.



Fig

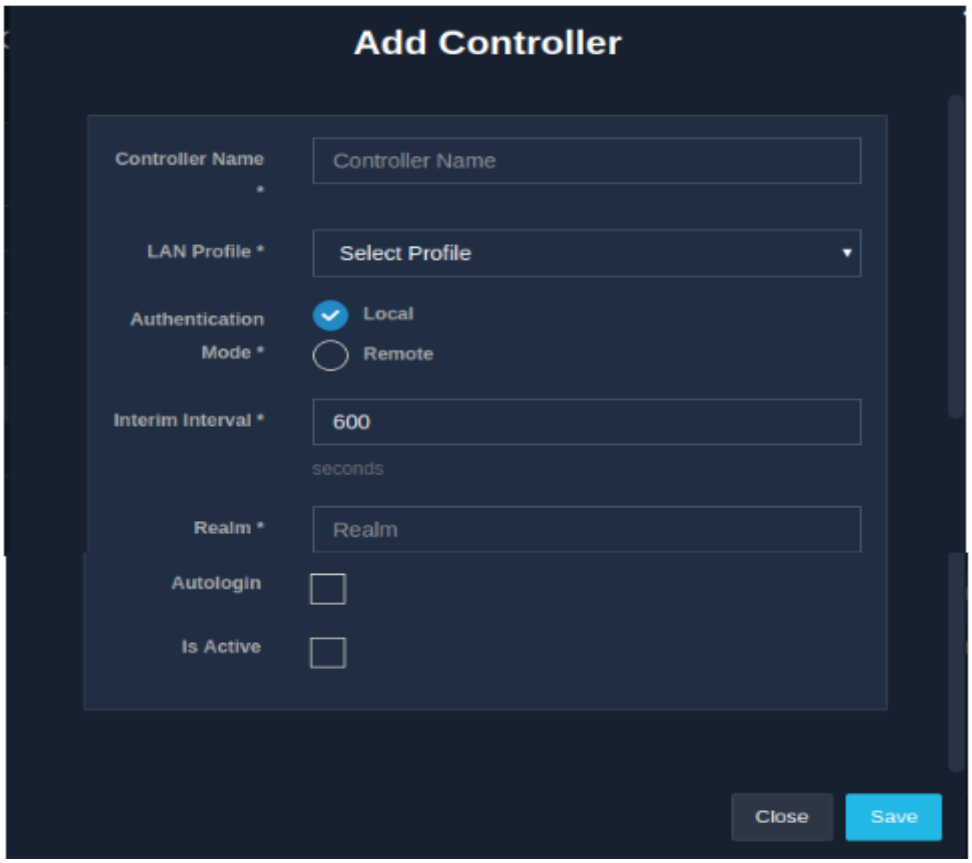
4. AUTHENTICATION

4.1 Controllers

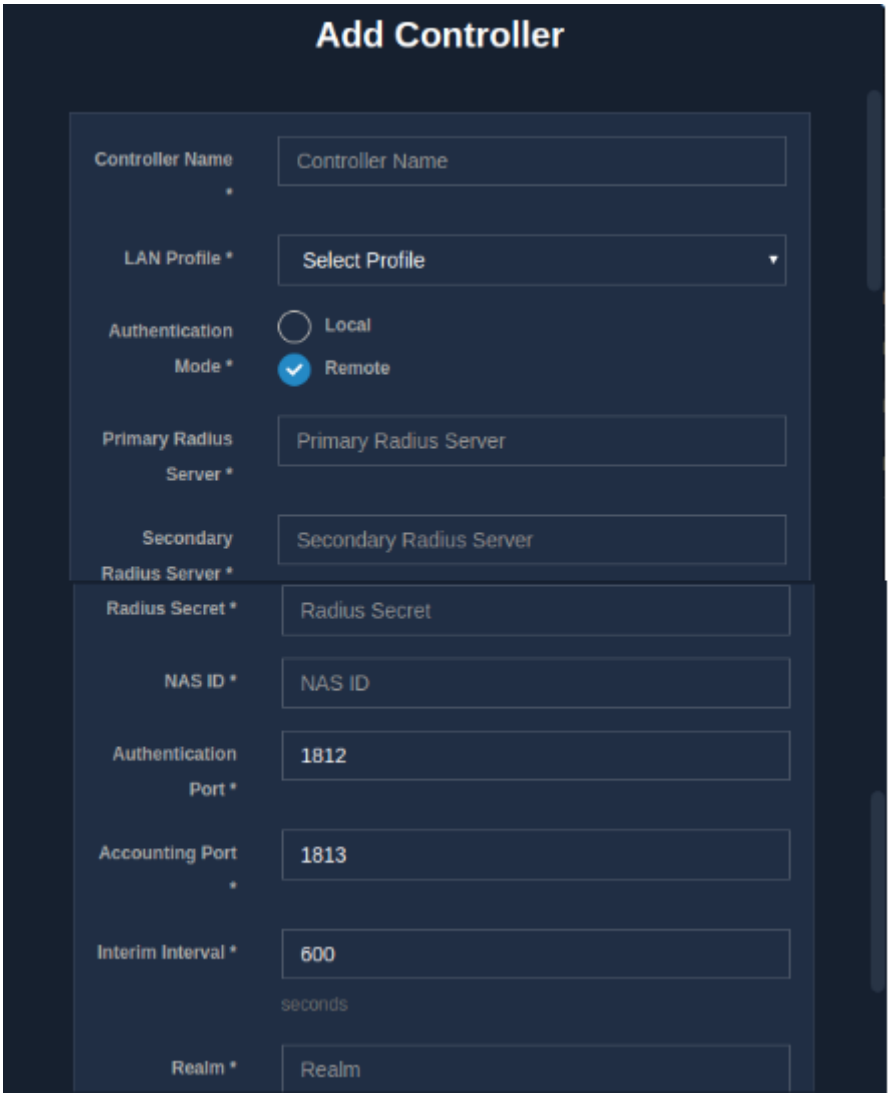
Controllers is an authentication service in UniBox. UniBox v3.0 supports the execution of multiple authentication services and captive portals on the same appliance. Each authentication service is controlled by the controller profile in UniBox. The controller is associated with the LAN profile and will create a hotspot service on the LAN port. Each controller profile will work independently of the other.

4.1.1 Creation

Select the 'Controllers' section from the 'Authentication' module present in the sidebar. Click on the '**+**' icon to create or add a new controller profile. A modal form will be displayed that collects the information required to create a new controller profile.



Fig



Fig

Fields	***Decsription***
Controller Name	Enter a name for the controller profile.
LAN Profile	Select the LAN profile associated with the profile.
Authentication Mode*	Select one of the authentication modes.
Primary Radius Server #	For remote mode, enter the IP address of the primary radius server.
Secondary Radius Server #	For remote mode, enter the IP address of the secondary radius server.
Radius Secret #	For remote mode, enter the radius secret.
NAS ID #	For remote mode, enter the NAS ID.
Authentication Port #	For remote mode, enter the authentication port. Default: 1812.
Accounting Port #	For remote mode, enter the accounting port. Default: 1813.
Interim Interval	Enter the interim interval in seconds
Realm	This is an identifier, also called a prefix, that is appended to the username, delimited by '@'. Username: Sam

	Realm:Sam@1234 **There can be NO space or special character while entering a realm.**
Auto-login	If the checkbox is checked, the auth service will enable MAC login. MAC login enables automatic authentication of a device using its MAC address. In case of Auto-login, the captive portal is not displayed.
Is Active	Tick the checkbox to activate the profile.

Table

NOTE:

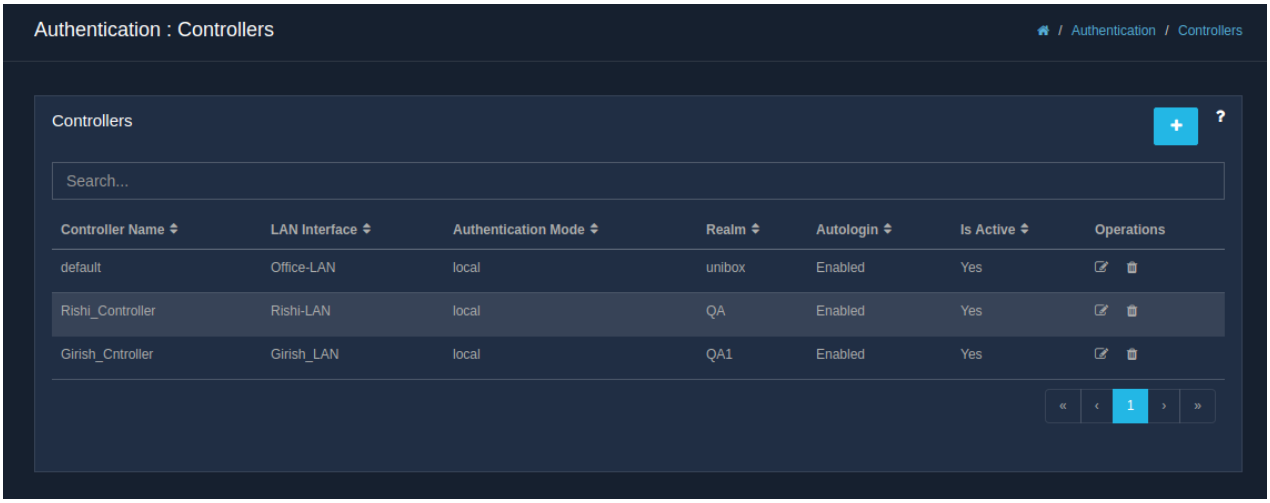
* Authentication modes are of two types:
    - Local mode: In this mode, the authentication happens locally.
    - Remote mode: In this mode, external authentication services are used.

All these fields are only displayed under the remote authentication mode.

Click on 'Save'. A new controller profile is created!

4.1.2 List Controller Profiles

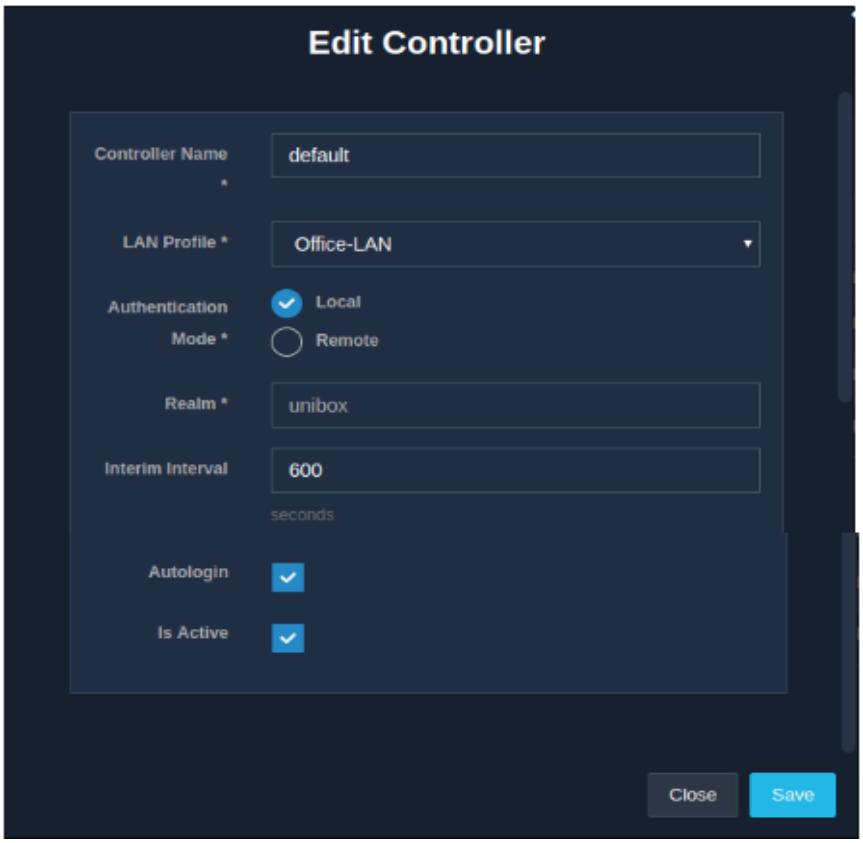
The 'Controllers' section under the 'Authentication' module, displays the list of controller profiles that exist in the system. Along with the controller name, the list displays the details related to a controller, which includes the LAN interface associated with the profile, its authentication mode, realm, auto-login function and whether the controller profile is active or not. Also, it includes the 'Operations' column where a controller profile can be edited or deleted.



Fig

4.1.3 Edit Controller Profile

The 'Operations' column in the list allows an admin to make changes to a controller profile. To edit an existing controller profile, click on the edit icon. A modal form is displayed which is similar to the one displayed for creating a new controller. Refer

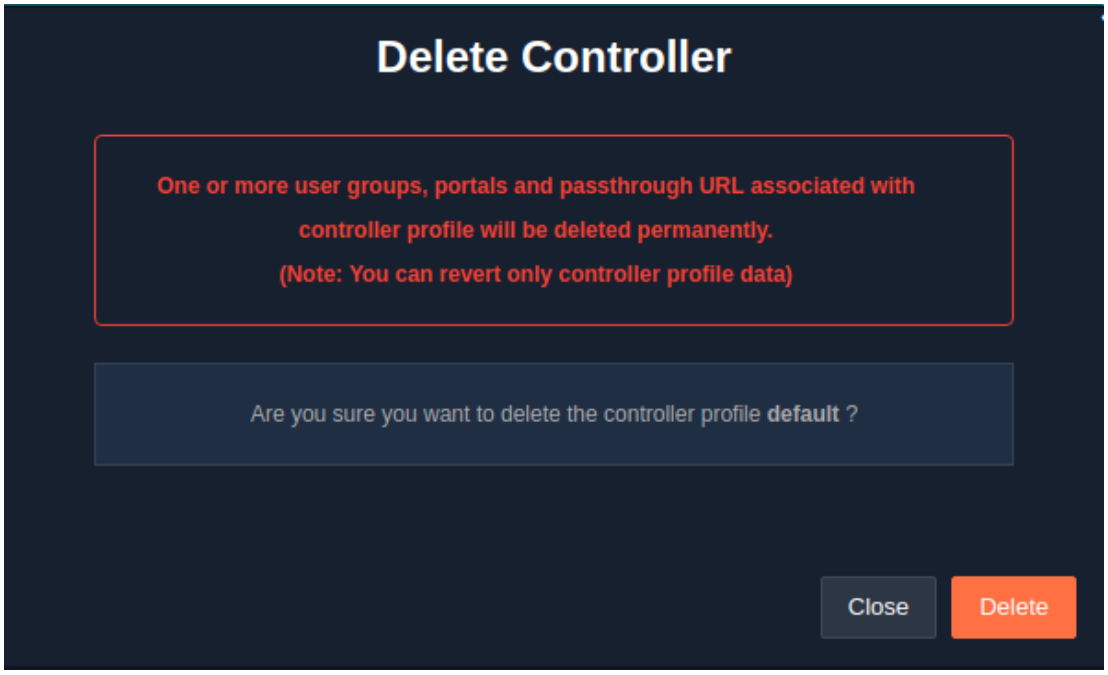


Fig

The changes made will be applied only when the changes are saved. So click on 'Save'.

4.1.4 Delete Controller Profile

Click on the 'delete' icon, in the 'Operations' column, to delete a controller profile. Once clicked, a message asking for the confirmation of the delete operation pops up. A controller profile can be deleted only if it is not assigned to any captive portal.



Fig

Once the profile is deleted, the hotspot service on the port will seize to exist. If you are sure, go ahead and click on the 'Delete' button.

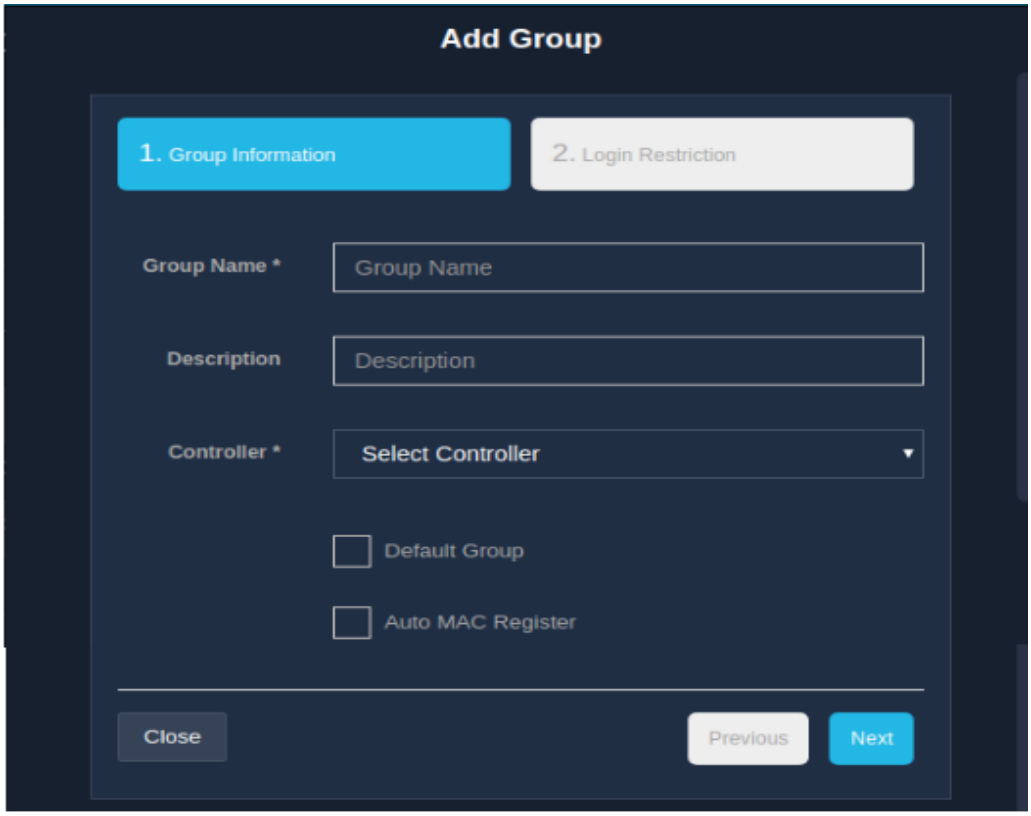
4.2 Groups

The 'Groups' module allows an admin to define user groups in Unibox. This provides an admin the facility to assign rules and restrictions to a group of users, instead of assigning it individually to a number of users which is too tiresome and time-consuming.

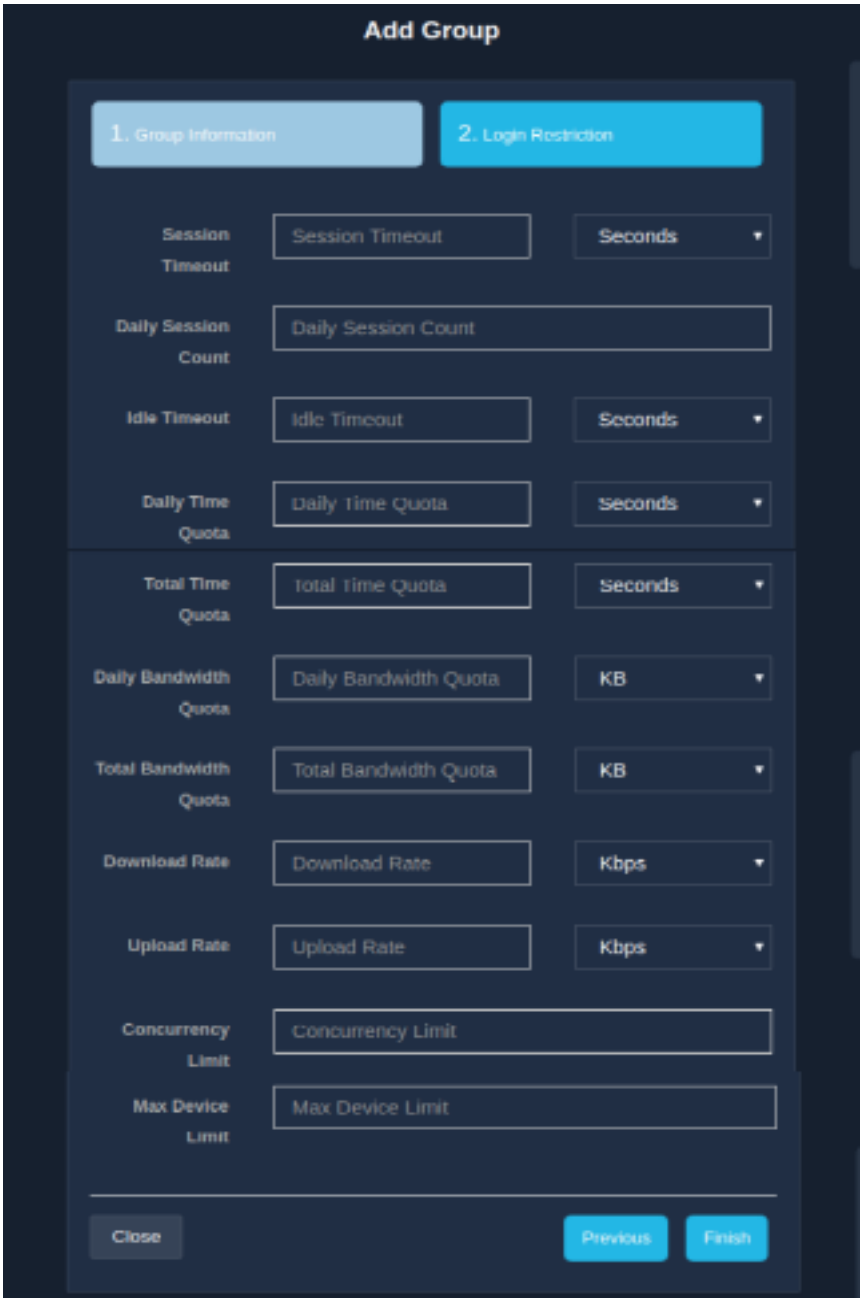
4.2.1 Creation

Select the 'Groups' section under the 'Authentication' module in the sidebar. Click on the '+' icon to create a new group. A form is displayed which is sectioned into two parts:

- 'Group Information' which collects the information required for creating a group.
- 'Login Restrictions' which gathers all the restrictions to be applied to the group.


Add Group
1. Group Information
2. Login Restriction
Group Name *
Group Name
Description
Description
Controller *
Select Controller
Default Group
Auto MAC Register
Close
Previous
Next

Fig


Add Group
1. Group Information
2. Login Restriction
Session Timeout
Session Timeout
Seconds
Daily Session Count
Daily Session Count
Idle Timeout
Idle Timeout
Seconds
Daily Time Quota
Daily Time Quota
Seconds
Total Time Quota
Total Time Quota
Seconds
Daily Bandwidth Quota
Daily Bandwidth Quota
KB
Total Bandwidth Quota
Total Bandwidth Quota
KB
Download Rate
Download Rate
Kbps
Upload Rate
Upload Rate
Kbps
Concurrency Limit
Concurrency Limit
Max Device Limit
Max Device Limit
Close
Previous
Finish

Fig

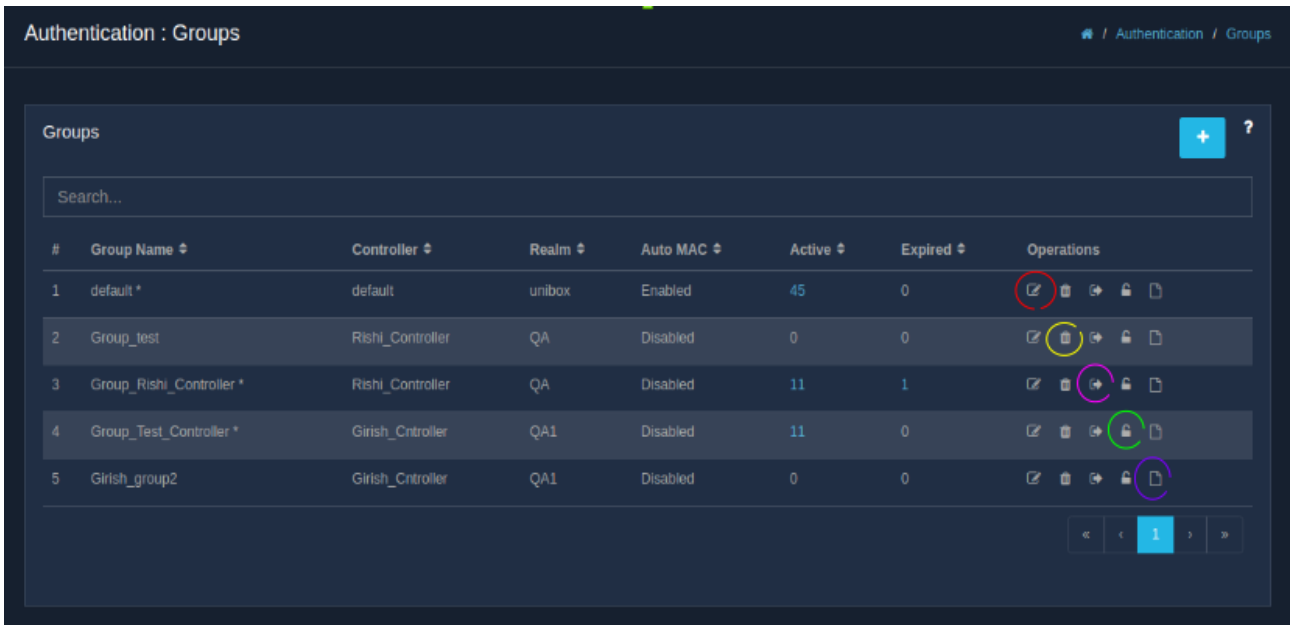
Fields	*Description*
Group Name	A unique name for the user group.
Description	Brief description about the group.
Controller	Select the controller to which the group belongs to.
Default Group	Tick the checkbox if the group is to be a default one. So when the users register, they will be assigned to this group by default.
Auto MAC Register	Tick the checkbox to enable. If enabled, MAC address of the user gets registered during the first authentication request and eventually used for login on subsequent attempts.
Session Timeout	Enter the session timeout for the users in a group. After the session timeout, the user's session will be closed. Time can be set in **seconds**, **minutes** or **hours**.
Daily Session Count	Enter the daily session count for the users in a group per day
Idle Timeout	Enter a time period for users which will close the user's session if the connection is kept idle for the given time period.
Daily Time Quota	Set a time limit which will allow the users to remain online for that specific time period per day. Time can be set in **seconds**, **minutes** or **hours**.
Total Time Quota	Set a total time usage quota which will allow the users to remain online only for that specific time period.
Daily Bandwidth Quota	Set a data usage limit which will allow the users to remain online only until the specified data is consumed by the user per day.
Total Bandwidth Quota	Set a total data usage quota which will allow the user to remain online until the specified data is consumed. The value set is the addition of all the previous data usages.
Download Rate	Enter the bandwidth download rate/ speed for the users in a group. Select the unit for download rate, which can be in **Kbps**, **Mbps** or **Gbps**.
Upload Rate	Enter the bandwidth upload rate/ speed for the users in a group. Select the unit for upload rate, which can be in **Kbps**, **Mbps** or **Gbps**.
Concurrency Limit	Enter the concurrency limit. Concurrency limit controls the number of sessions that can be active at the same time for a particular user. Enter a concurrency limit.
Max Device Limit	This limit decides the total number of devices a given user can use to login. This limit counts both the online and offline devices.

Table

Click ‘Finish’ and you have a new group.

4.2.2 List Groups

When clicked on the ‘Groups’ section under the ‘Authentication’ module in the sidebar, a list of all the existing groups is displayed. Besides the group name, the list displays the details related to the groups like the controller profile, realm and the settings of Auto-MAC register. It also displays the number of active and expired users in each group. The list also maintains an ‘Operations’ column, which gives out several options to the admin.



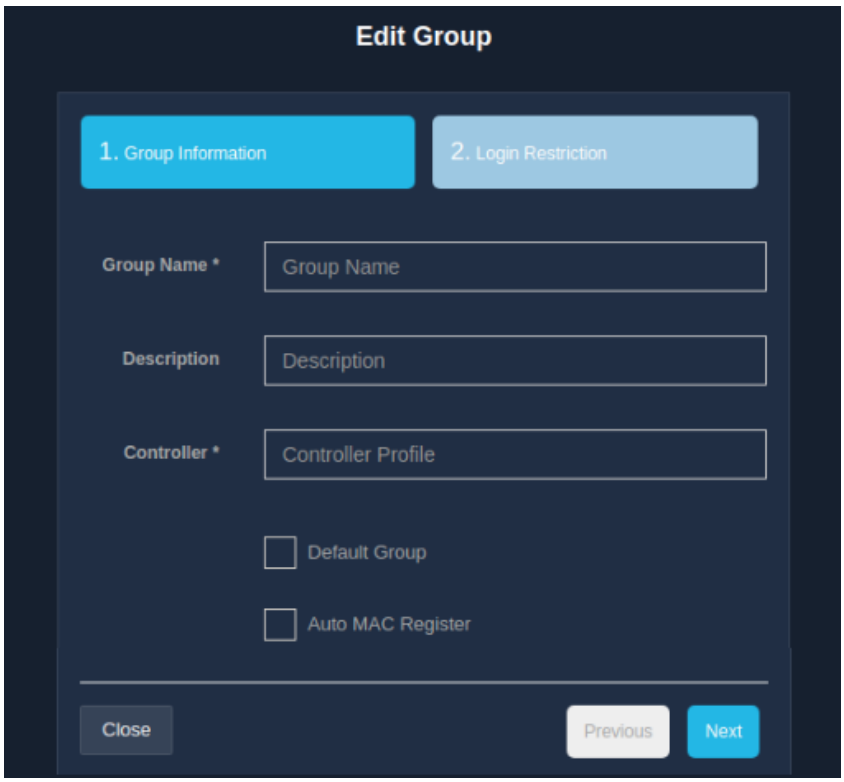
Fig

The ‘Operations’ column in the listing table facilitates the admin with several actions that can be performed on the user groups, namely,

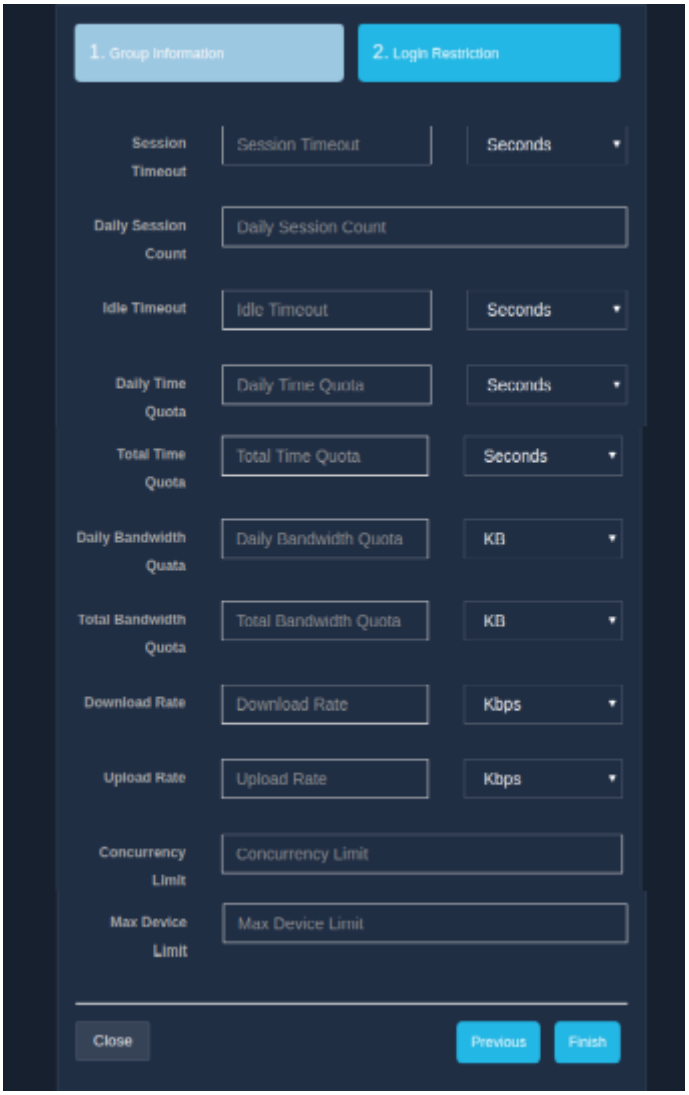
- Edit
- Delete
- Clear Auto-login
- Reset Password
- Export Group Activity

4.2.3 Edit Group

The ‘Edit’ option allows an admin to make changes to the information of the existing user groups. Click on the edit icon in the ‘Operations’ column to edit a user group. A form, similar to the one that was displayed while creating a new group, will be displayed. Refer


Edit Group
1. Group Information
2. Login Restriction
Group Name *
Group Name
Description
Description
Controller *
Controller Profile
Default Group
Auto MAC Register
Close
Previous
Next

Fig

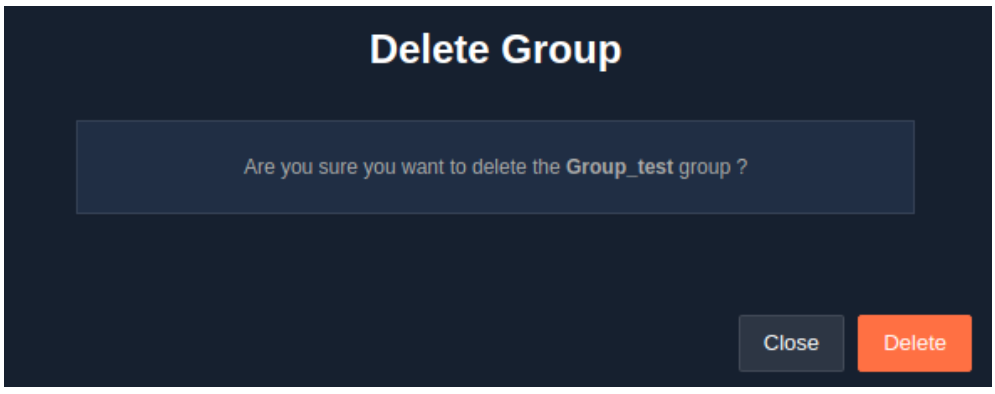


Fig

Click on ‘Finish’ to save and apply all the changes made.

4.2.4 Delete Group

An admin is given the option to delete a user group if he/she wants to. To delete a user group, click on the delete icon in the ‘Operations’ column. A message pops up to confirm the delete operation.

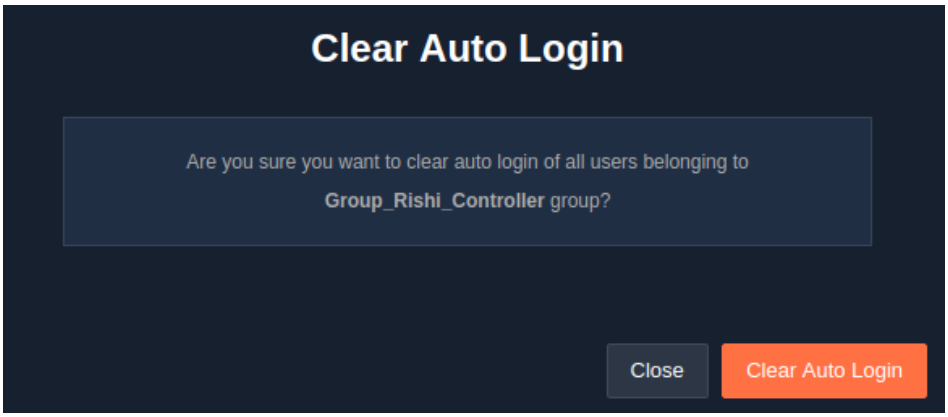


Fig

If sure, click on ‘Delete’ button.

4.2.5 Clear Auto-Login

This option allows the admin to clear auto-login MAC of all the users in a group. Once the MAC addresses are cleared, the MAC login entries for all the users belonging to the user group will be cleared. The users will be prompted to login from the captive portal again. All you have to do to clear auto-login is to click on the icon for clearing the auto-login in the ‘Operations’ column. A message page pops up to confirm the clear auto-login action.

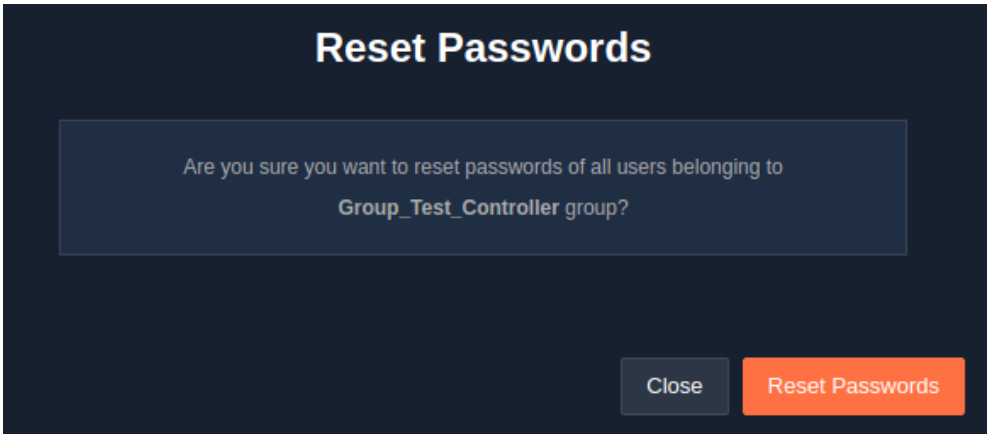


Fig

If sure, click on ‘Clear Auto Login’ button.

4.2.6 Reset Passwords

An admin is provided with a feature which allows him/her to reset passwords of the users in a group. After resetting, new passwords will be generated for users. To reset passwords, click on the icon meant for resetting passwords in the ‘Operations’ column. A confirmation message page is displayed to confirm the reset action.



Fig

Click on the ‘ Reset Password’ button if you are sure.

4.2.7 Export Group Activity

This option allows an admin to export all the users' activity report for backup purpose. The code report is exported in PDF or CSV format. Click on the icon assigned to export group activity. A page is displayed where one has the option to export either a summarized or detailed group activity report. Summarized report will provide the summary of group activity. The detailed report will provide the details of each activity for the users in the group.

Fig

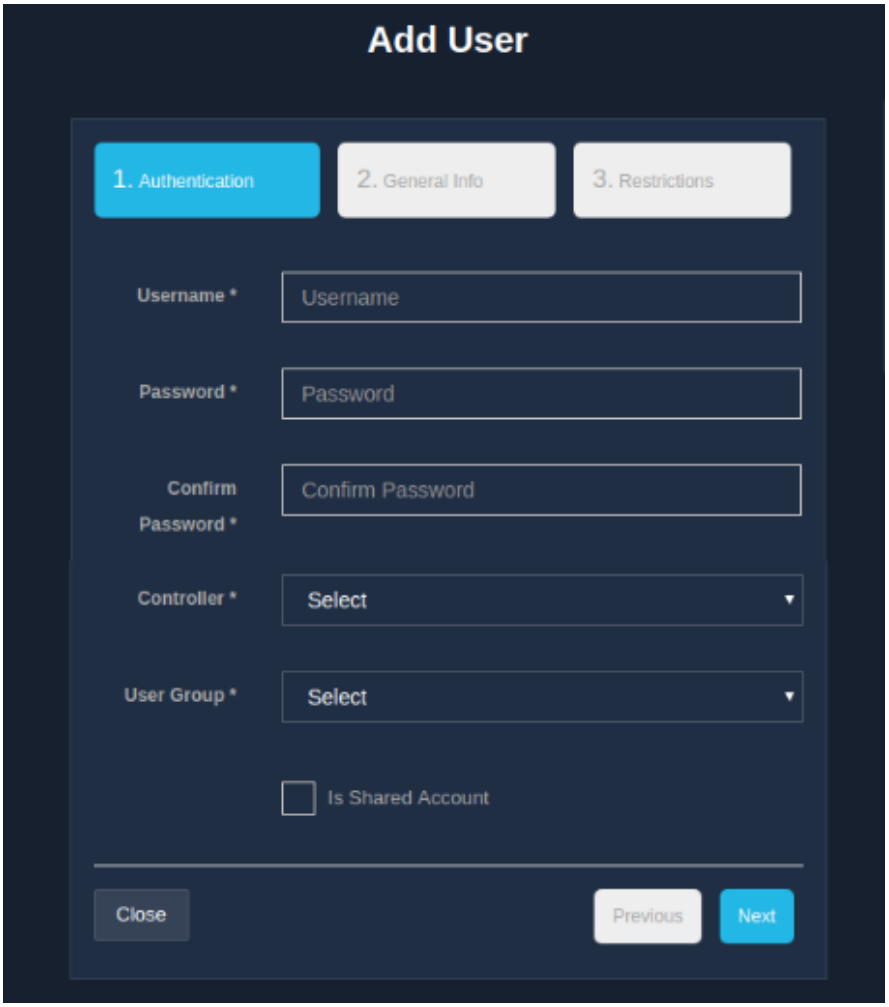
4.3 User Management

4.3.1 Users

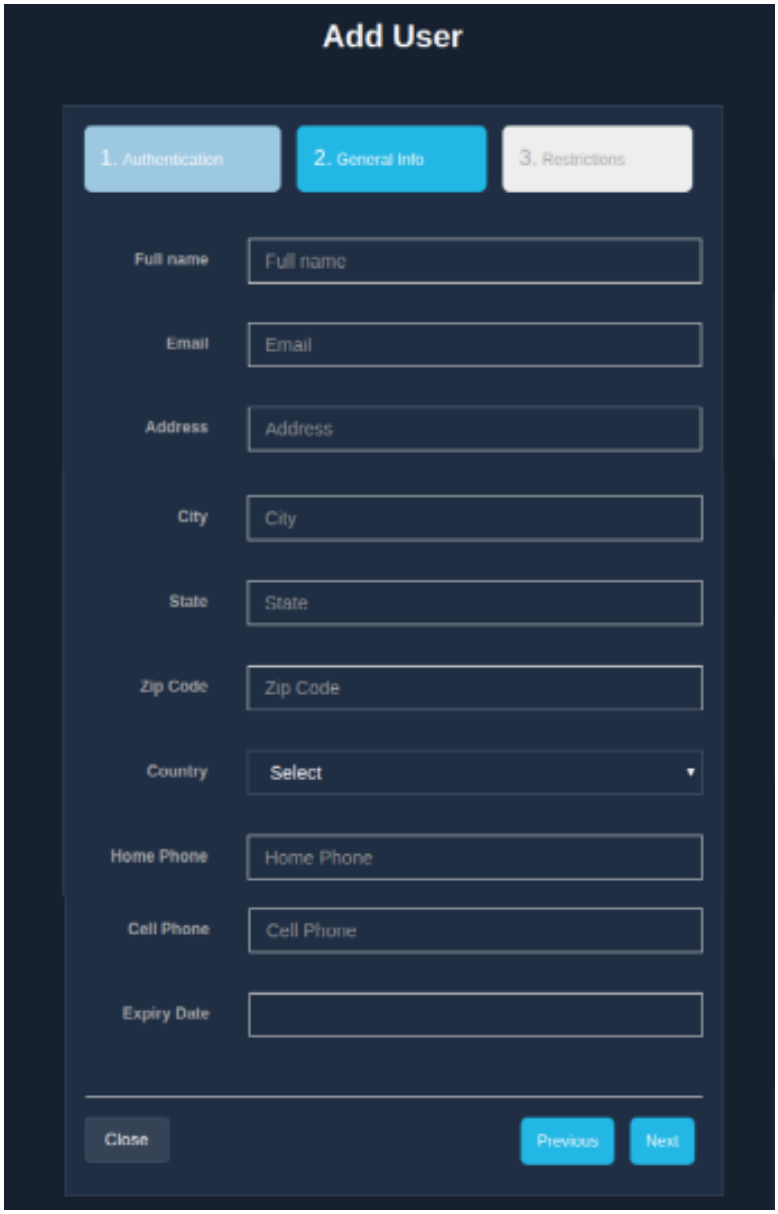
4.3.1.1 Creation

An admin gets to create new users, free or paid, in the database. To create a new user, select the 'Authentication' module followed by the 'User Management' sub-module and then click on the 'Users' section. Finally, click on the '**+**' icon. A form is displayed, sectioned into three parts:

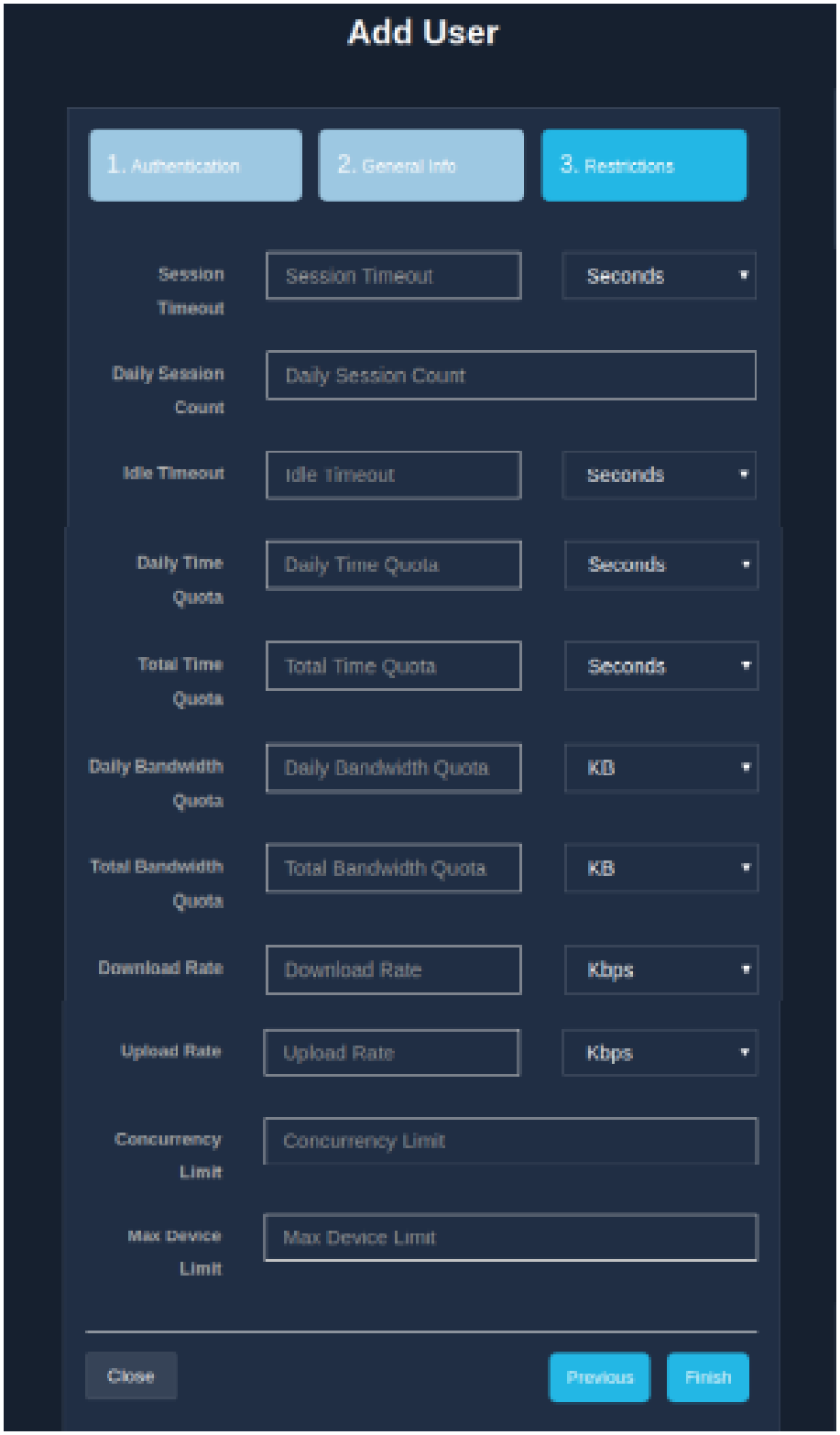
- Authentication
- General Info
- Restrictions


Add User
1. Authentication
2. General Info
3. Restrictions
Username *
Username
Password *
Password
Confirm Password *
Confirm Password
Controller *
Select
User Group *
Select
Is Shared Account
Close
Previous
Next

Fig


Add User
1. Authentication
2. General Info
3. Restrictions
Full name
Full name
Email
Email
Address
Address
City
City
State
State
Zip Code
Zip Code
Country
Select
Home Phone
Home Phone
Cell Phone
Cell Phone
Expiry Date
Close
Previous
Next

Fig


Add User
1. Authentication
2. General Info
3. Restrictions
Session Timeout
Session Timeout
Seconds
Daily Session Count
Daily Session Count
Idle Timeout
Idle Timeout
Seconds
Daily Time Quota
Daily Time Quota
Seconds
Total Time Quota
Total Time Quota
Seconds
Daily Bandwidth Quota
Daily Bandwidth Quota
KB
Total Bandwidth Quota
Total Bandwidth Quota
KB
Download Rate
Download Rate
Kbps
Upload Rate
Upload Rate
Kbps
Concurrency Limit
Concurrency Limit
Max Device Limit
Max Device Limit
Close
Previous
Finish

Fig

Fields	*Description*
Username	Enter a unique username. Must be of atleast 3 characters and should not contain spaces. UniBox will automatically append a suffix to the username.
Password	Enter the password for the user. Must be of at least 6 characters.
Confirm Password	Re-enter and confirm the above entered password.
Controller	Select the specific controller to which the user will belong to.
User Group	Select the user group to which the user will belong to.
Is Shared Account	Tick the checkbox if the username is to be shared among multiple users, i.e., the same username will be used to login from multiple devices at the same time.
Fullname	Enter the fullname of the user.
Email	Email address of the user. It should be unique.
Address/ City/ State/ Zipcode	Enter the address information of the user.
Country	Select country from the drop-down menu.
Home Phone	Enter the home phone number of the user.
Cell Phone	Enter the cell phone number of the user.
Expiry Date	Enter the expiry date. Use the calendar by clicking on the calendar icon to enter the date. The user account will automatically expire on the set date.
Session Timeout	Enter the session timeout for the user which closes the user's session after the timeout period. Time can be set in **seconds**, **minutes** or **hours**.
Daily Session Count	Enter the daily session count for the users which will not allow the user to login for the remaining hours once the number of daily sessions exceed.
Idle Timeout	Enter a time period for users which will close the user's session if the connection is kept idle for the given time period.
Daily Time Quota	Set a time limit which will allow the users to remain online for that specific time period per day. Time can be set in **seconds**, **minutes** or **hours**.
Daily Bandwidth Quota	Set a data usage limit which will allow the users to remain online only until the specified data is consumed by the user per day.
Total Time Quota	Set a total time usage quota which will allow the users to remain online only for that specific time period.
Total Bandwidth Quota	Set a total data usage quota which will allow the user to remain online until the specified data is

	consumed. The value set is the addition of all the previous data usages.
Download Rate	Enter the bandwidth download rate/ speed for the users in a group. Select the unit for download rate, which can be in **Kbps**, **Mbps** or **Gbps**.
Upload Rate	Enter the bandwidth upload rate/ speed for the users in a group. Select the unit for upload rate, which can be in **Kbps**, **Mbps** or **Gbps**.
Concurrency Limit	Enter the concurrency limit. Concurrency limit controls the number of sessions that can be active at the same time for a particular user. Enter a concurrency limit.
Max Device Limit	This limit decides the total number of devices a given user can use to login. This limit doesn't take concurrency into consideration.

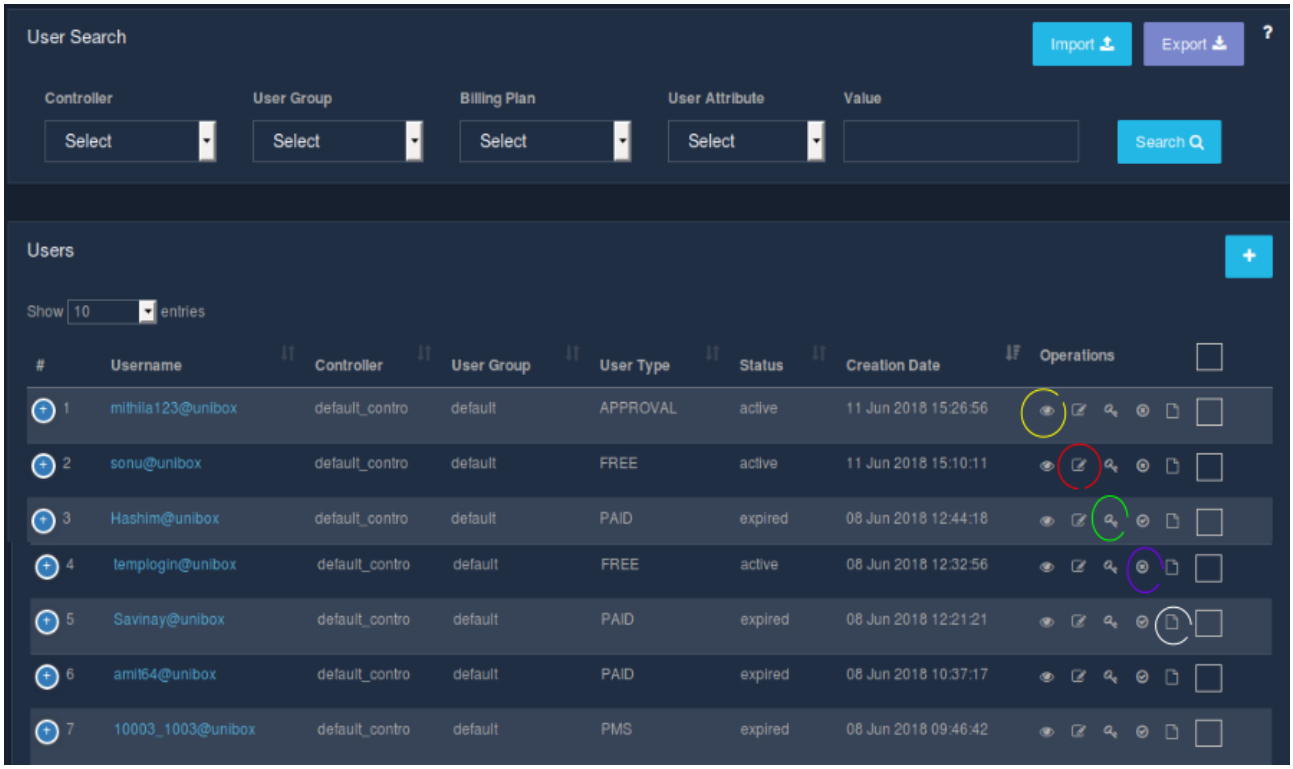
Table

Once the form is filled, click on the 'Finish' button. And there! A new user is created.

4.3.1.2 List Users

When the 'Users' section is selected under the 'User Management' sub-module, a list consisting of all the local users in the UniBox database is displayed. The list displays the details related to the corresponding to the username such as the controller assigned, the user group the user belongs to, the user type, i.e., free, paid or voucher based user, status and also the creation date.

Adjacent to the username, there is a "+" icon which expands into more information about the user.



Fig

The list also contains an ‘Operations’ column, which provides several options to the admin, like:

- View
- Edit
- Change Password
- Expire
- Export User Activity

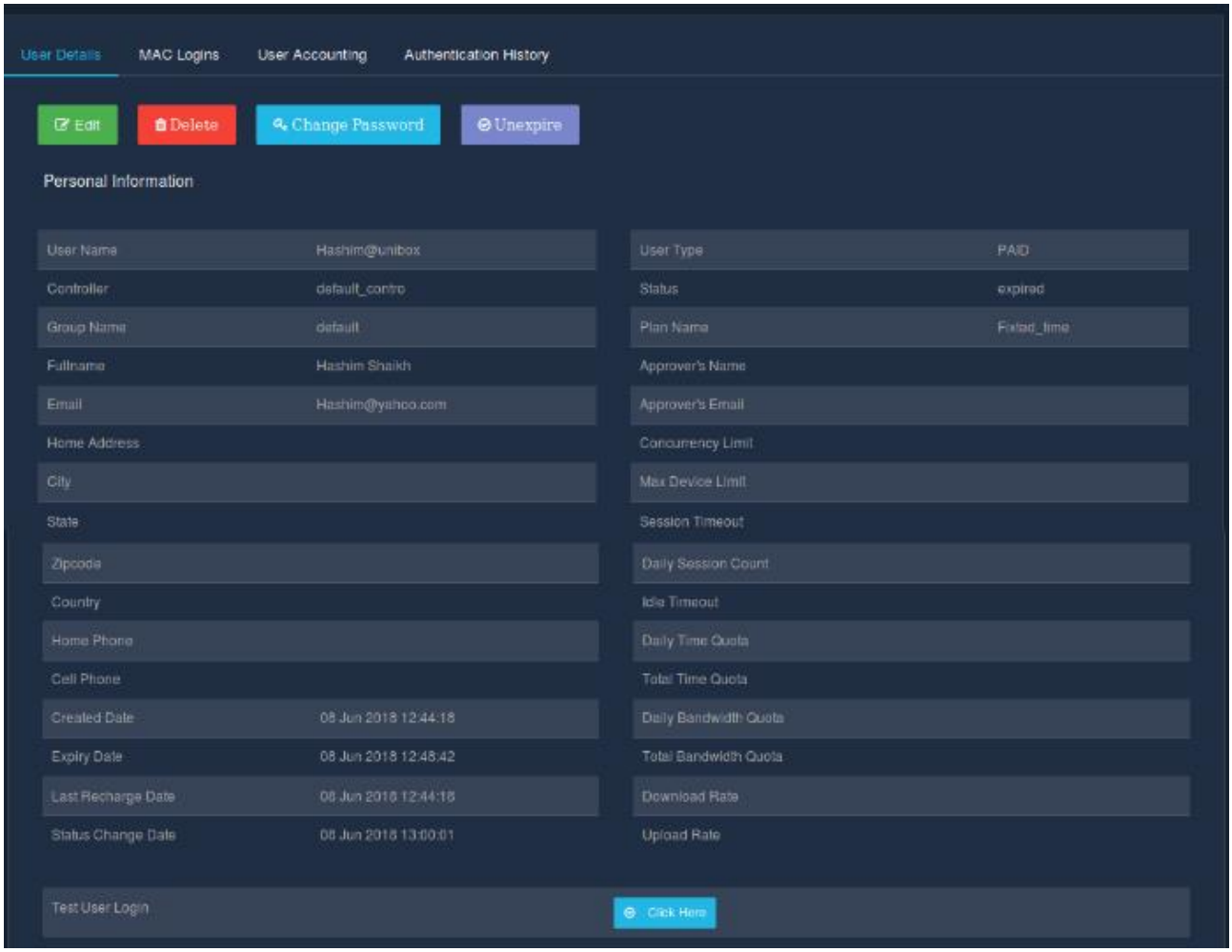
In the list page, there is also the feature to search for one or more users based on the various search criteria, namely,

- Controller: Specific controller profile for search.
- Group name: Specific group name to search.
- Billing Plan: Billing plan for paid users.
- User Attribute: Search on the basis of user attributes.
- Value: Using values or partial names to search.

4.3.1.3 User Details

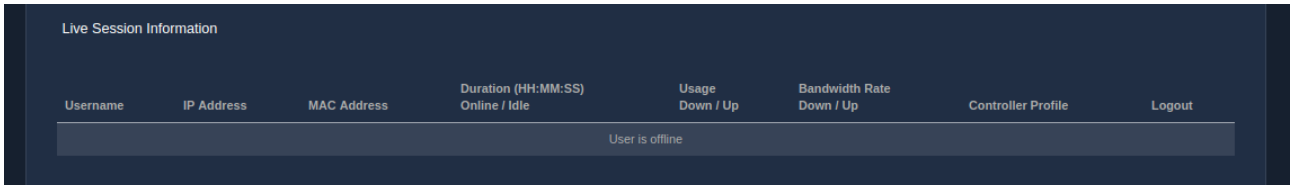
An admin can view the details and also the session data for a given user. To view the details of a user, admin can click on either the username or the view icon in the ‘Operations’ column of the listing table. The ‘User Details’ section contains several details related to a user, categorized into 6 parts:

- Personal Information: Displays the general information about the user, such as email, address, user type and other extended attributes, if any.



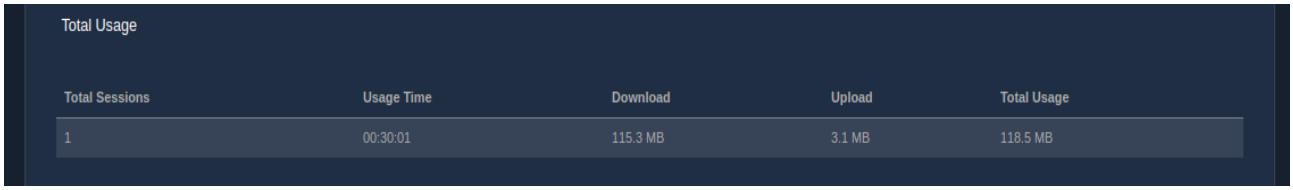
Fig

- Live Session Information: Indicates whether the user is online or offline.



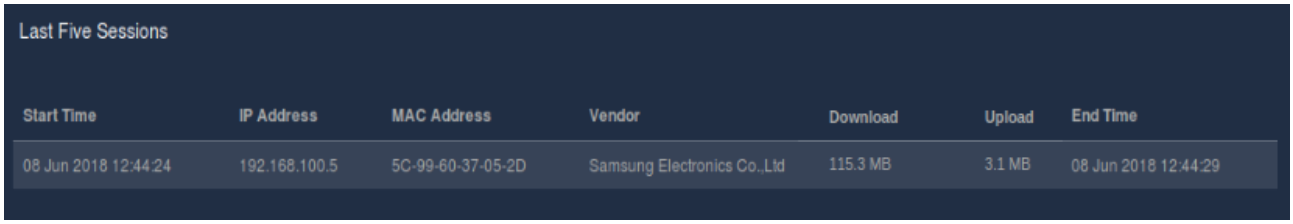
Fig

- Total Usage: Shows the total usage of data by the user till now.



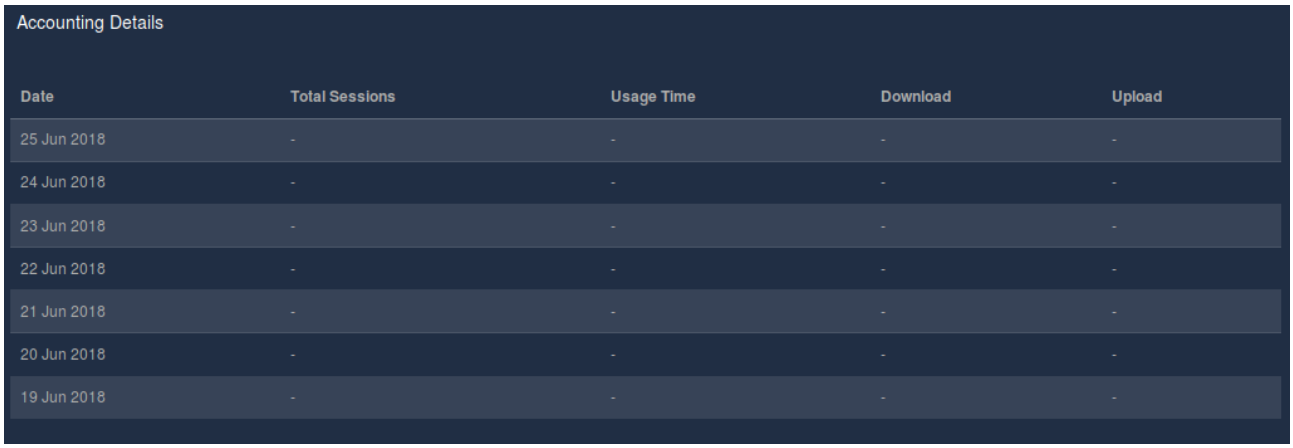
Fig

- Last Five Sessions: Displays details of past five sessions.



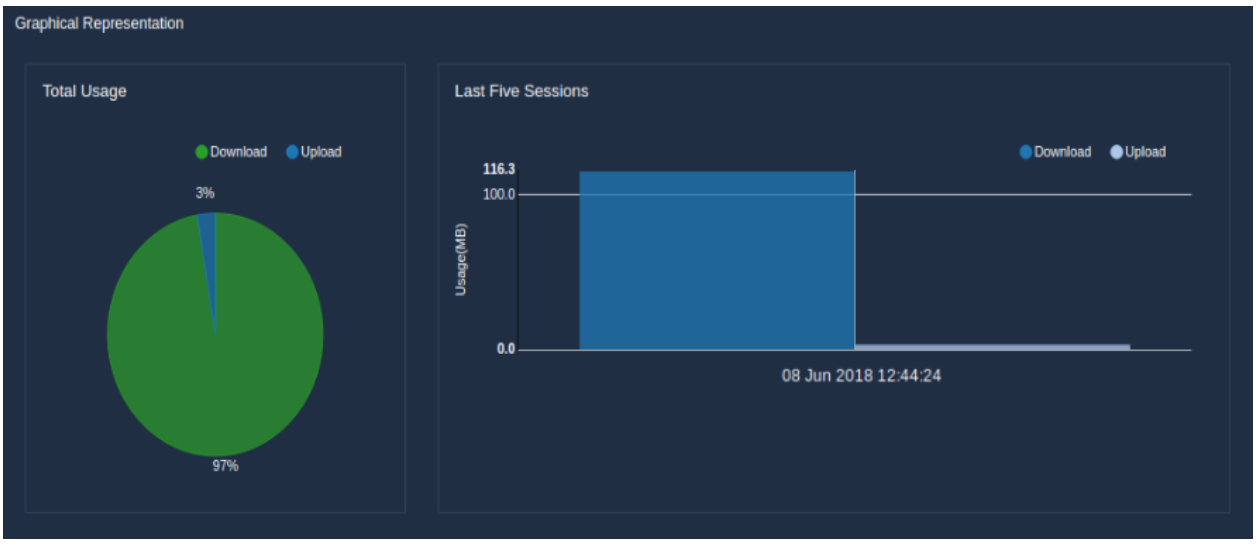
Fig

- Accounting Details: Presents a summarized information on user accounting over the last seven days. It includes details like total number of sessions, total usage, upload and download for each day of the week.



Fig

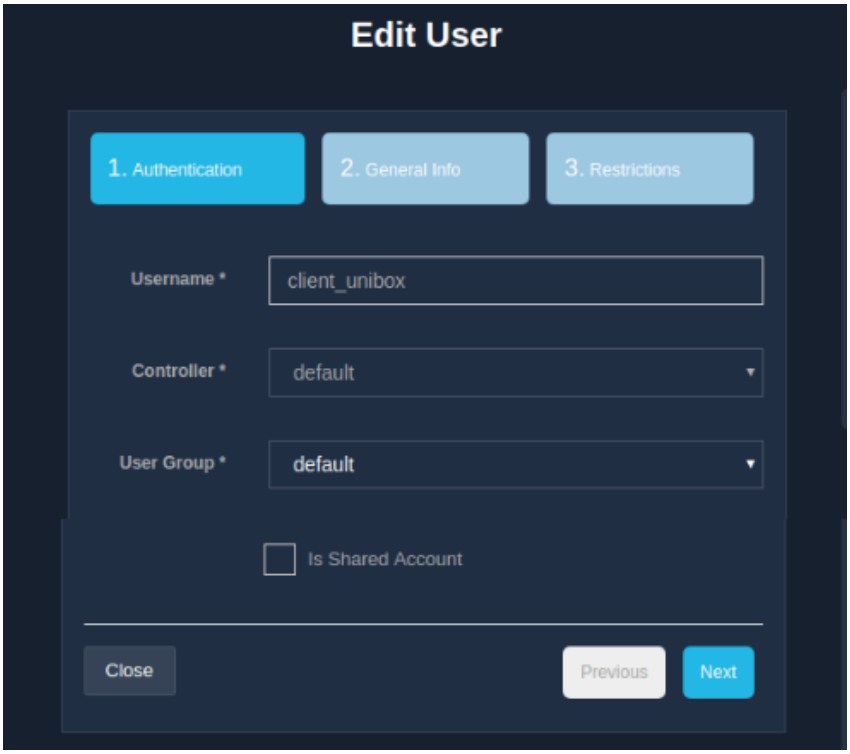
- Graphical Representation: Representing the usage ratio and Upload/Download for last five sessions.



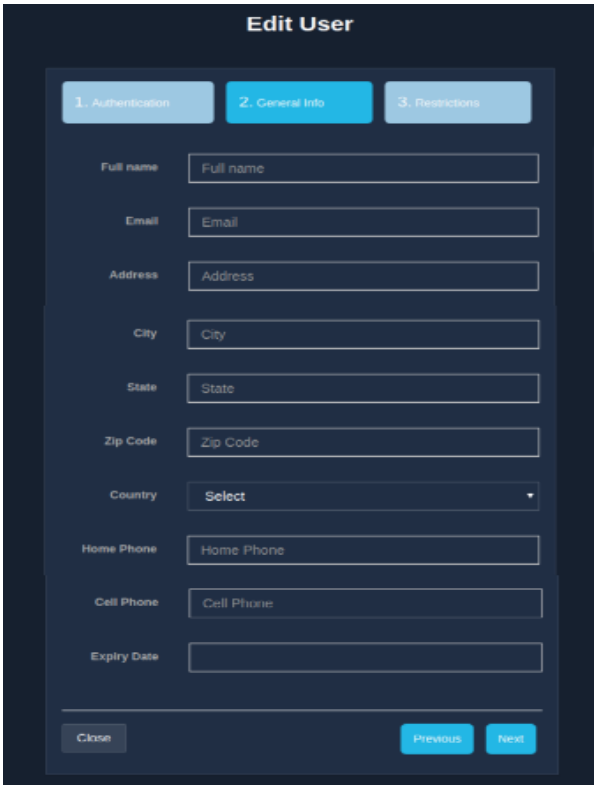
Fig

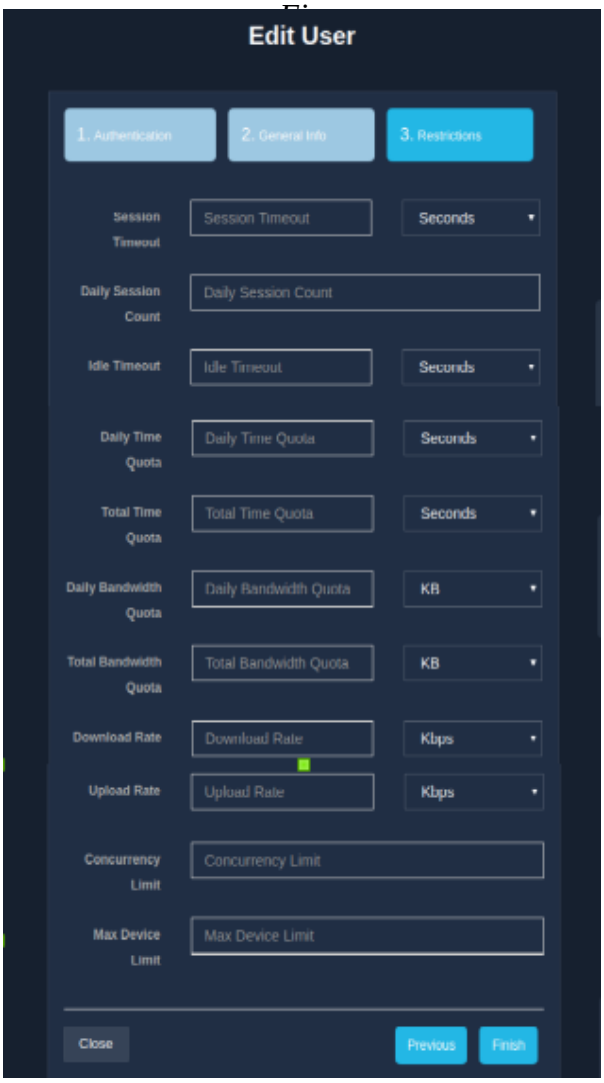
4.3.1.4 Edit User

The option to edit a user's information can be found either in the 'Operations' column or in the 'User Details' section. When the edit icon in the 'Operations' column or the 'Edit' button in the 'User Details' section is clicked, a form is displayed which is similar to the create user form. Refer


Edit User
1. Authentication
2. General Info
3. Restrictions
Username *
client_unibox
Controller *
default
User Group *
default
Is Shared Account
Close
Previous
Next

Fig


Edit User
1. Authentication
2. General Info
3. Restrictions
Full name
Full name
Email
Email
Address
Address
City
City
State
State
Zip Code
Zip Code
Country
Select
Home Phone
Home Phone
Cell Phone
Cell Phone
Expiry Date
Close
Previous
Next

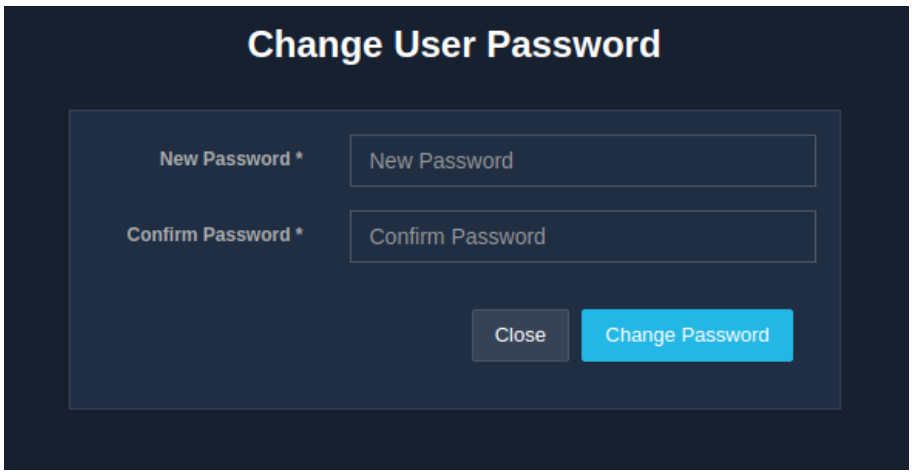

Edit User
1. Authentication
2. General Info
3. Restrictions
Session Timeout
Session Timeout
Seconds
Daily Session Count
Daily Session Count
Idle Timeout
Idle Timeout
Seconds
Daily Time Quota
Daily Time Quota
Seconds
Total Time Quota
Total Time Quota
Seconds
Daily Bandwidth Quota
Daily Bandwidth Quota
KB
Total Bandwidth Quota
Total Bandwidth Quota
KB
Download Rate
Download Rate
Kbps
Upload Rate
Upload Rate
Kbps
Concurrency Limit
Concurrency Limit
Max Device Limit
Max Device Limit
Close
Previous
Finish

Fig

Once the changes are made, click on ‘Finish’ to save the changes made.

4.3.1.5 Change Password

An admin is given the option to change the passwords of the users existing in the UniBox, which can be found either as an icon in the ‘Operations’ column or as ‘Change Password’ button in the ‘User Details’ section. When clicked on either of them, a page is displayed which asks for the new password and also to confirm the new password.



Fig

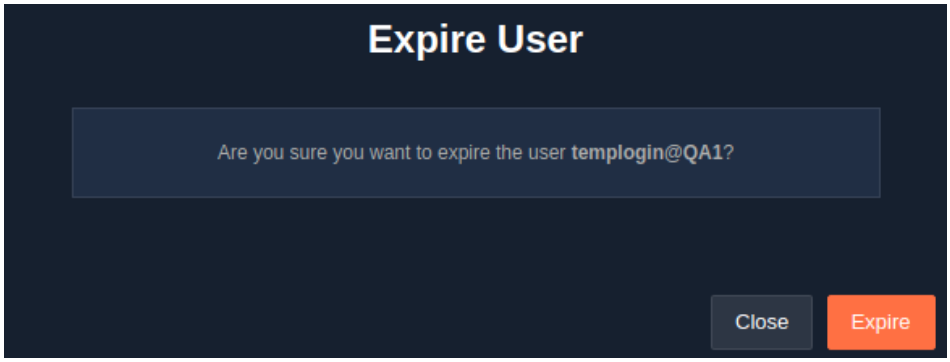
After putting in the new password, set the change by clicking on the ‘Change Password’ button.

4.3.1.6(a) Expire User

A feature to manually expire a user is provided to an admin. Once the user is expired, the user will not get access to the internet. Unlike the delete option, a user can be unexpired by an admin at a later point in time. So to temporarily block a user’s access, this option can be used.

In the expired state, all user details will remain intact. However, after 3 months of inactivity, an expired user’s details are automatically cleaned up by the system.

The option to expire a user can be found in the ‘Operations’ column as an icon or in the ‘User Details’ as an ‘Expire’ button. Click on any one of them, a message pops up to confirm the expire action.



Fig

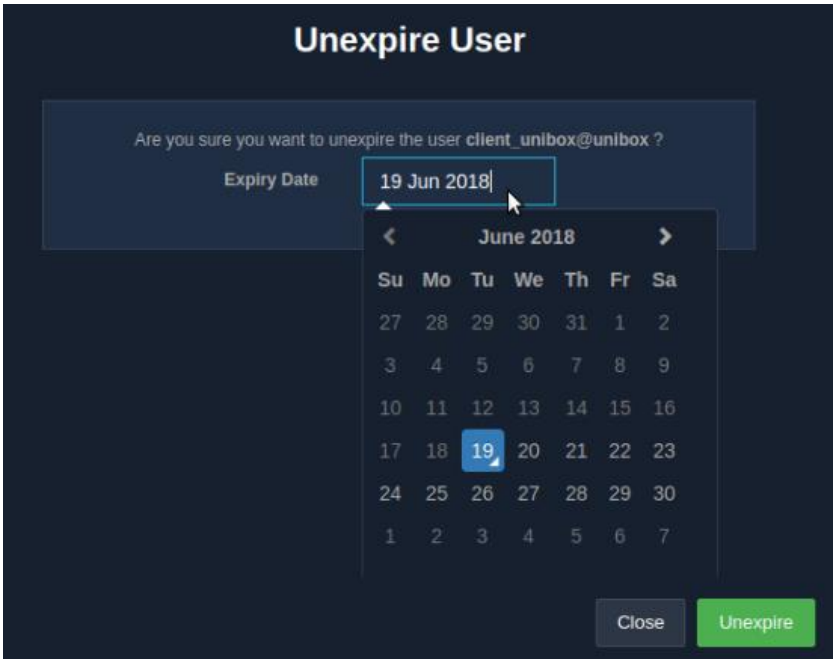
Click on the ‘Expire’ button, if sure.

4.3.1.6(b) Unexpire User

An admin can unexpire an expired user, i.e., grant access to the internet to the user by reactivating the user account. This option is provided to allow the admin to extend the user's time or manually recharge the user's account.

It is important for the admin to set expiry dates to the users. If no expiry date is set, the user will get access to the service indefinitely.

To unexpire a user, click on the icon meant to unexpire a user in the 'Operations' column or the 'Unexpire' button in the 'User Details' section. A page is displayed to confirm the unexpire action.



Fig

Click on the 'Unexpire' button, if sure. But before that set an expiry date, using the calendar provided.

4.3.1.7 Export User Activity

This option allows an admin to export an individual user's session activity report. The report is exported in PDF or CSV format. Click on the icon assigned for exporting user activity. A page is displayed where the admin can choose to export from the two types of reports:

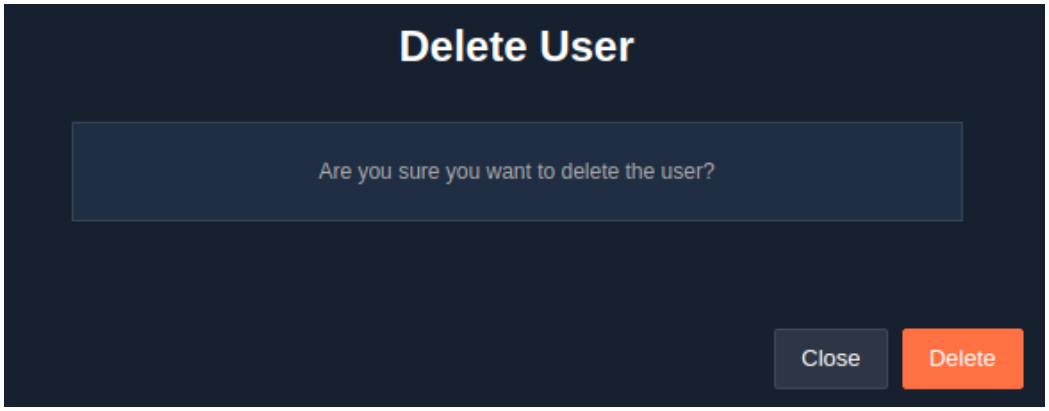
- Summarized User Activity Report- Shows the summary of user's activity per day.
- Detailed User Activity Report- Shows information of all the sessions of the user.

Fig

4.3.1.8 Delete User

This option allows the admin to delete any existing user from the database. While performing the delete action on a user, keep in mind that all the user information, including session data and transactions will be lost. Users once deleted, cannot be restored.

To delete the user, click on the 'Delete' button in the 'User Details' section. A confirmation message pops up to confirm the delete action. Once sure, click on the 'Delete' button.



Fig

NOTE: To expire or delete multiple users at once, click on the checkboxes corresponding to those users that are to be expired or deleted.

4.3.1.9 Export Users

This section allows an admin to export user information, under a selected group, for backup purposes. The report is exported in CSV file.

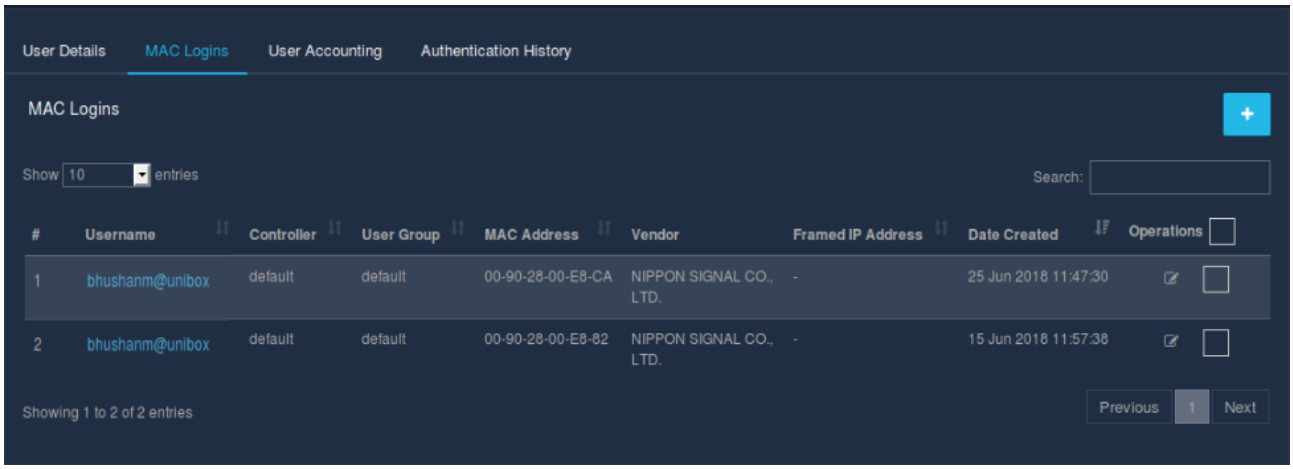
4.3.1.10 Import Users

This option import users from the provided CSV file. Existing users will get updated while importing all users. Imported users will be under their respective user group. All imported users will be in active state and the admin can change the states later. On clicking the 'Import' button, a page is displayed to gather the required information for import.

Fig

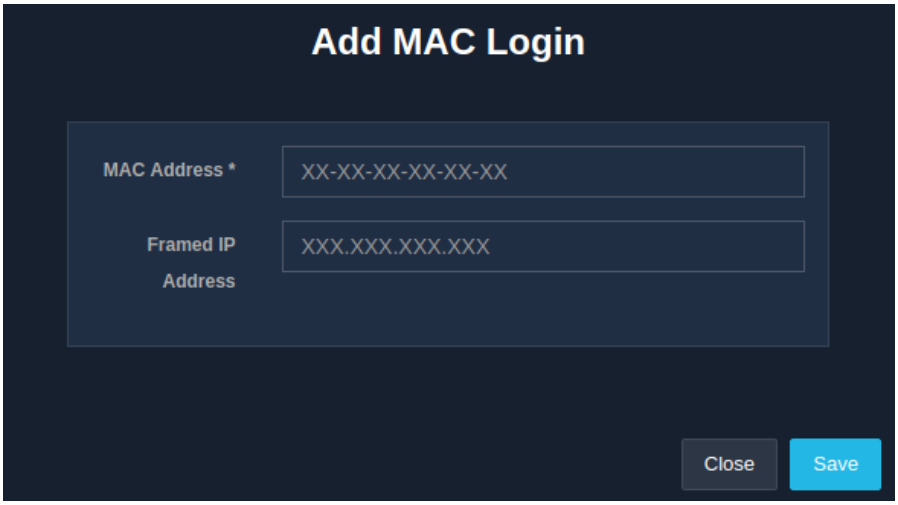
4.3.1.11 MAC Logins

This feature displays all the MAC addresses used by the users during login. When the auto-MAC capture is enabled on the controller profile, UniBox automatically captures the user's MAC addresses for future logins. The page displays the username, controller, user-group, MAC address, vendor, framed IP address, creation date. The list is sorted according to the latest registered MAC addresses.



Fig

An admin can also add a new MAC login, by clicking on the '**+**' icon. A modal form is displayed wherein the MAC address and framed IP address are to be entered. Click 'Save' once the details are entered.



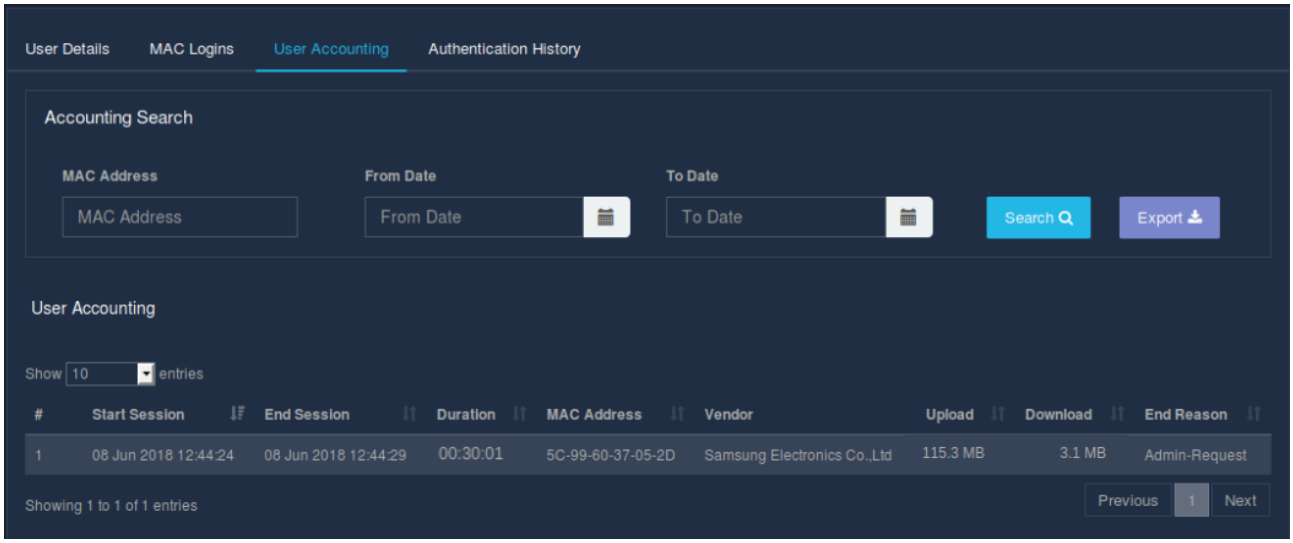
Fig

The MAC address entries can be deleted by using the delete buttons.

4.3.1.12 User Accounting

This page displays the session information for a given user. The information table displays session start time, end time, total duration in seconds, MAC address of the user's computer, vendor, uploaded bytes, downloaded bytes, and reason for terminating session.

A search option is available to search for sessions based on user's MAC address or a given time period.



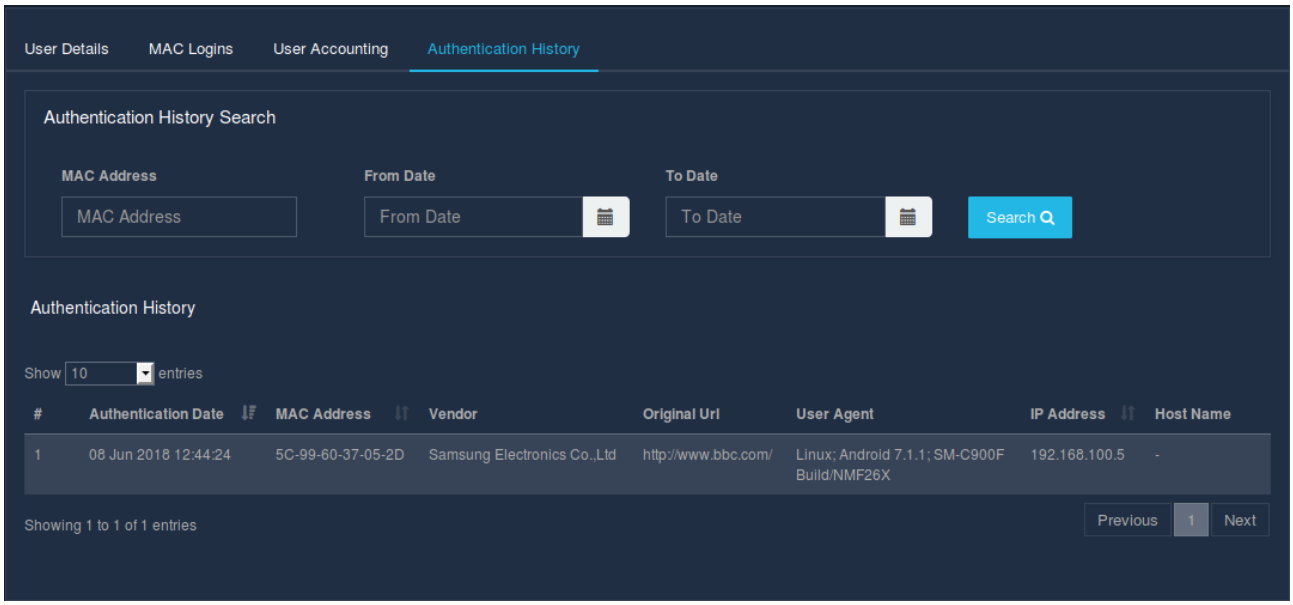
Fig

Fields	*Description*
MAC Address	The MAC address of user's computer.
From	The start date for searching accounting details.
To	The end date for searching accounting details.

Table

4.3.1.13 Authentication History

This page displays the user agent and the authentication history of a given user. Besides displaying the authentication date, MAC address of the user's computer, vendor, original URL, user agent, IP address and host name for a given user are also displayed.



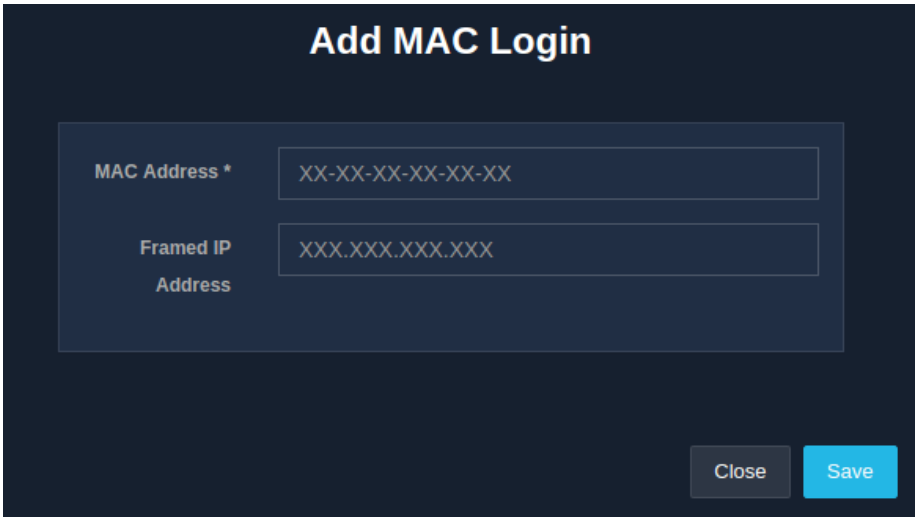
Fig

4.3.2 MAC Logins

4.3.2.1 Create / Add MAC Login

An admin is allowed to add a new MAC address entry. To add a new device in the MAC Login list, click on the 'MAC Logins' section under 'User Management' sub-module in 'Authentication' module. Now, click on the '**+**' icon in the 'Operations' column. A page is displayed that asks for MAC address and framed IP address.

The Framed IP address will be assigned to the device during authentication. Use this feature to assign static IP to the particular device.



Fig

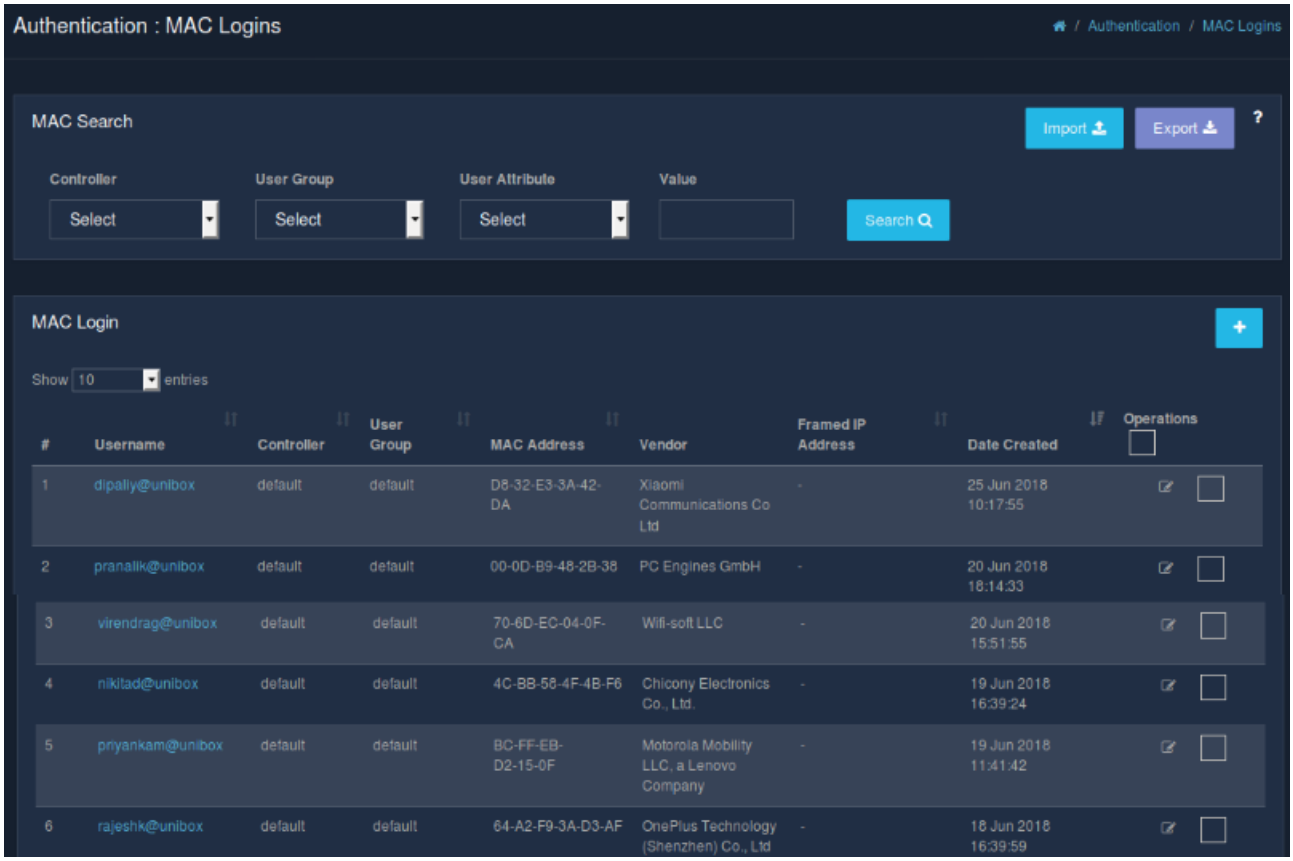
Fields	Description
MAC Address	Enter a valid MAC address in the format mentioned.
Framed IP Address	Enter the IP address to assign the device. This will be static IP assigned to the device.

Table

Once filled, click on the 'Save' button and the device will be added to the respective user's MAC device list.

4.3.2.2 List MAC Login

All the MAC addresses added or captured for the users or devices can be seen in the list. MAC addresses listed in this section will be allowed to login automatically when the auto login feature is enabled. The list displays the username, controller profile, user group, MAC address, device vendor, framed IP, creation date of the MAC address entry.



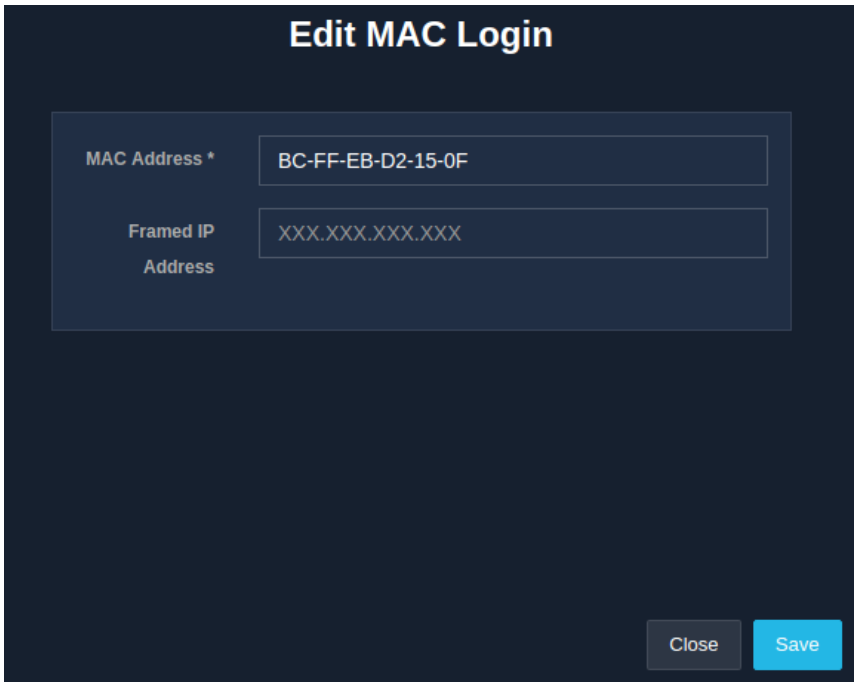
Fig

The search option allows to search MAC on the basis of controller, user group, user attributes, value.

4.3.2.3 Edit MAC Login

An admin is provided the facility to make changes to an existing MAC login. To change a MAC login information, click on the edit icon in the 'Operations' column against the respective MAC address. A pop-up

window appears that contains existing MAC information, where admin can change both MAC address and framed IP address. Refer.

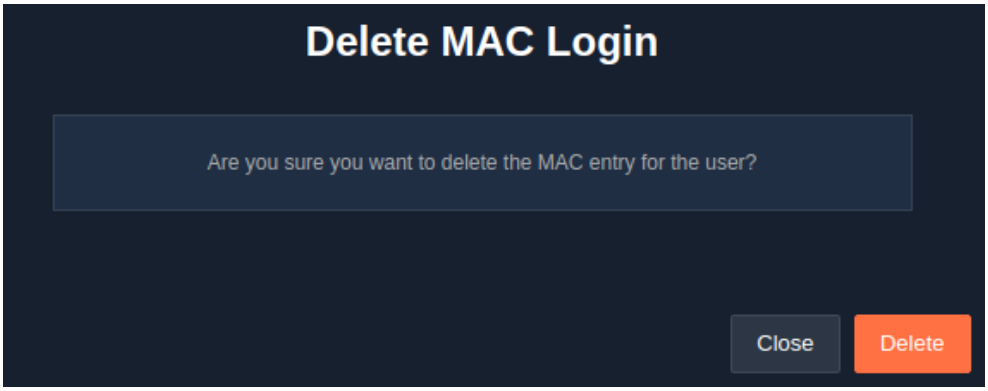


Fig

Click on the 'Save' button to update the settings and apply the changes made.

4.3.2.4 Delete MAC Login

To delete a MAC login, simply click on the checkbox against the respective username or MAC address. A confirmation window pops up to confirm the delete action.



Fig

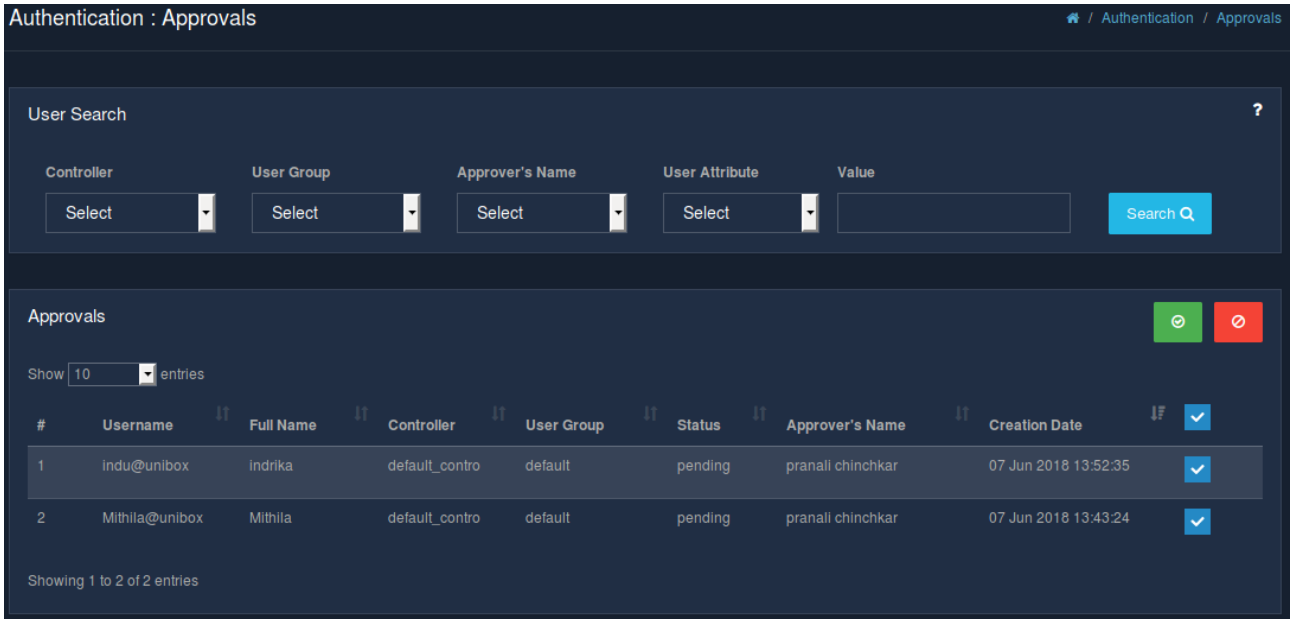
4.3.3 Approvals

UniBox presents a unique feature which allows administrators to provide two-step user registration process. A new user will be allowed to register for an account online through the captive portal. However, the user's account will not be approved immediately. Instead the user account will be activated only once the administrator approves the user. Additionally the administrator can assign the user to appropriate user group and assign right permissions to the users.

4.3.3.1 List Approval Users

All the users who need to be approved are listed in the approval table. The admin has the option to either approve or deny a user's registration. If a user approved, the user's account is activated in the system and the user is able to login. If denied, the user is marked denied and is not able to login.

To see the list, select the 'User Management' sub-module in the 'Authentication' module in the sidebar and click on the 'Approvals' section.



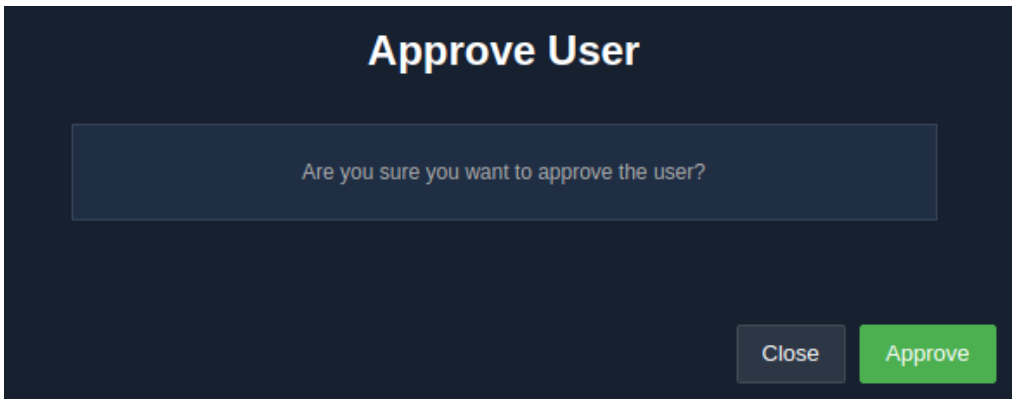
Fig

The admin can also search for a specific user record based on the search categories like controller, user group, approver's name, user attributes, value.

4.3.3.2 Approve Users

An admin can approve the users. Once the admin approves the user, the user automatically gets removed from the approval table and its status changes from pending to active.

To approve users, click on the checkbox corresponding to the user. Then click on the **green coloured approve icon**.

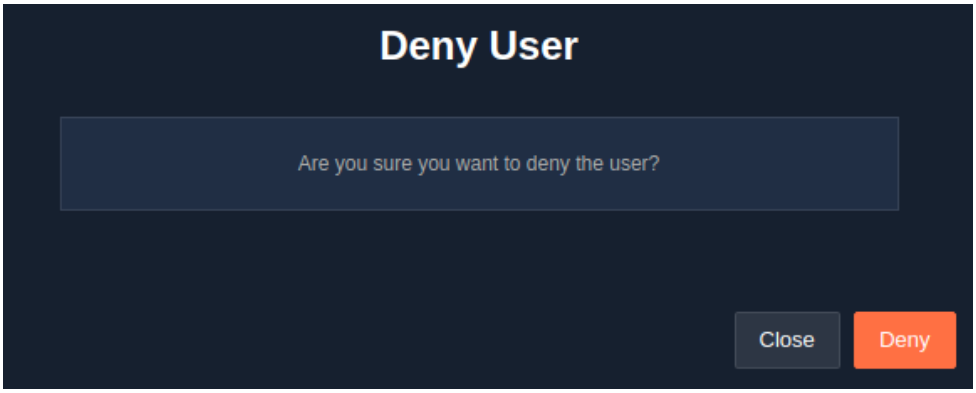


Fig

4.3.3.3 Deny Users

This section allows an admin to deny the registration of a user. Once the admin denies the user, the user's state change from pending to be denied. Denied users will not be allowed to login. These records may be purged after a few days.

To deny users, click on the checkbox corresponding to the user to be denied. Then click on the **red coloured deny icon**.



Fig

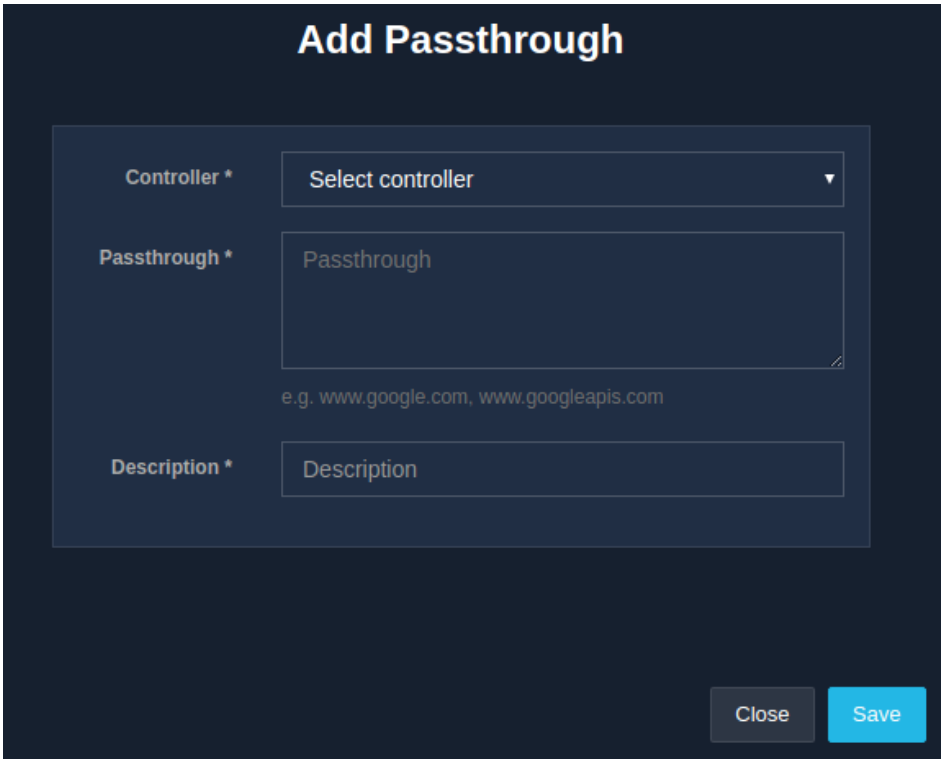
Then finally click on the 'Deny' button to decline the user.

4.4 Passthrough Domain

4.4.1 Creation

An admin is provided the facility to define a new passthrough or wall-garden domain in UniBox. Users can access the passthrough domains without authentication. Only the domain name of the domain needs to be entered.

To define a new passthrough, click on the 'Passthrough Domain' section in the 'Authentication' module. Then click on the '+' icon and a window slides down for the information to be entered to create a passthrough.



Fig

Fields	*Description*
Controller	Select the controller profile.
Passthrough Domain	Enter the domain name. You can also enter an IP address instead of the domain name. To add a wildcard domain, enter * before the domain name. Eg: *.wifi-soft.com
Description	Give a brief description of the domain.

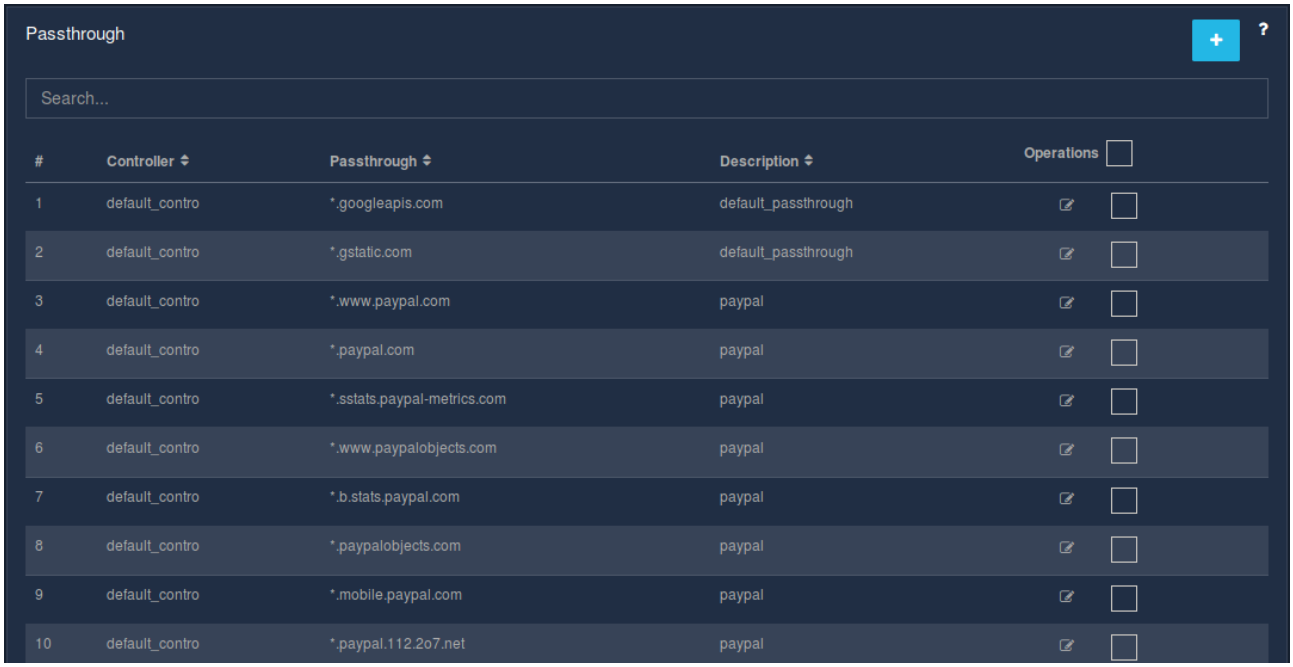
Table

If an external portal page is used for authentication, then the admin needs to define all the domains required to load the portal page in the passthrough list.
Similarly for social media logins, please enter the required domains in the passthrough list. Unibox provides all the required URLs for each social media login method for your reference.

4.4.2 List Passthrough Domain

All the passthrough domains present in the UniBox are listed for the admin to see. A passthrough domain or URL can be accessed by all clients without authentication.

To see the list of all the passthrough domains, click on the 'Passthrough Domains' section in the 'Authentication' module.



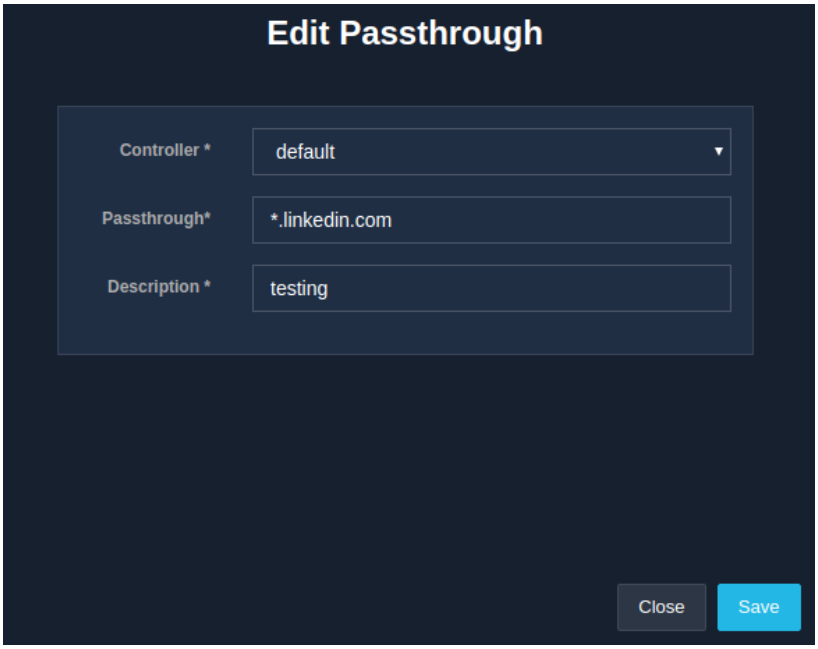
Fig

If an external login portal is configured, then the domain of the external web server would be configured in passthrough domains in addition to all the other URLs that might be listed on the login page.

To search for a domain, only the domain name must be entered.

4.4.3 Edit Passthrough Domain

An admin is allowed to edit an existing passthrough or wall-garden domain in UniBox. To add a wildcard domain, you need to add * before the domain name. Eg., *.wifi-soft.com. To edit a passthrough domain, click on the edit icon against the corresponding domain. A window appears that provides a form to make the required changes. Refer

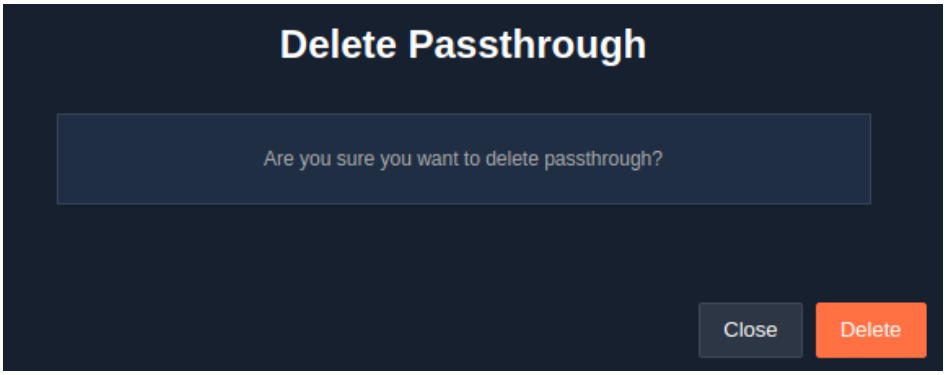


Fig

Once the changes are filled in, simply click on 'Save' to apply all the changes made.

4.4.4 Delete Passthrough Domain

To delete an existing passthrough domain entry, simply click the checkbox against the corresponding to the domain entry. Click on the **red coloured delete icon**. Once the entry is deleted, users will not be allowed to access the domain without authentication, if authentication mode is enabled.



Fig

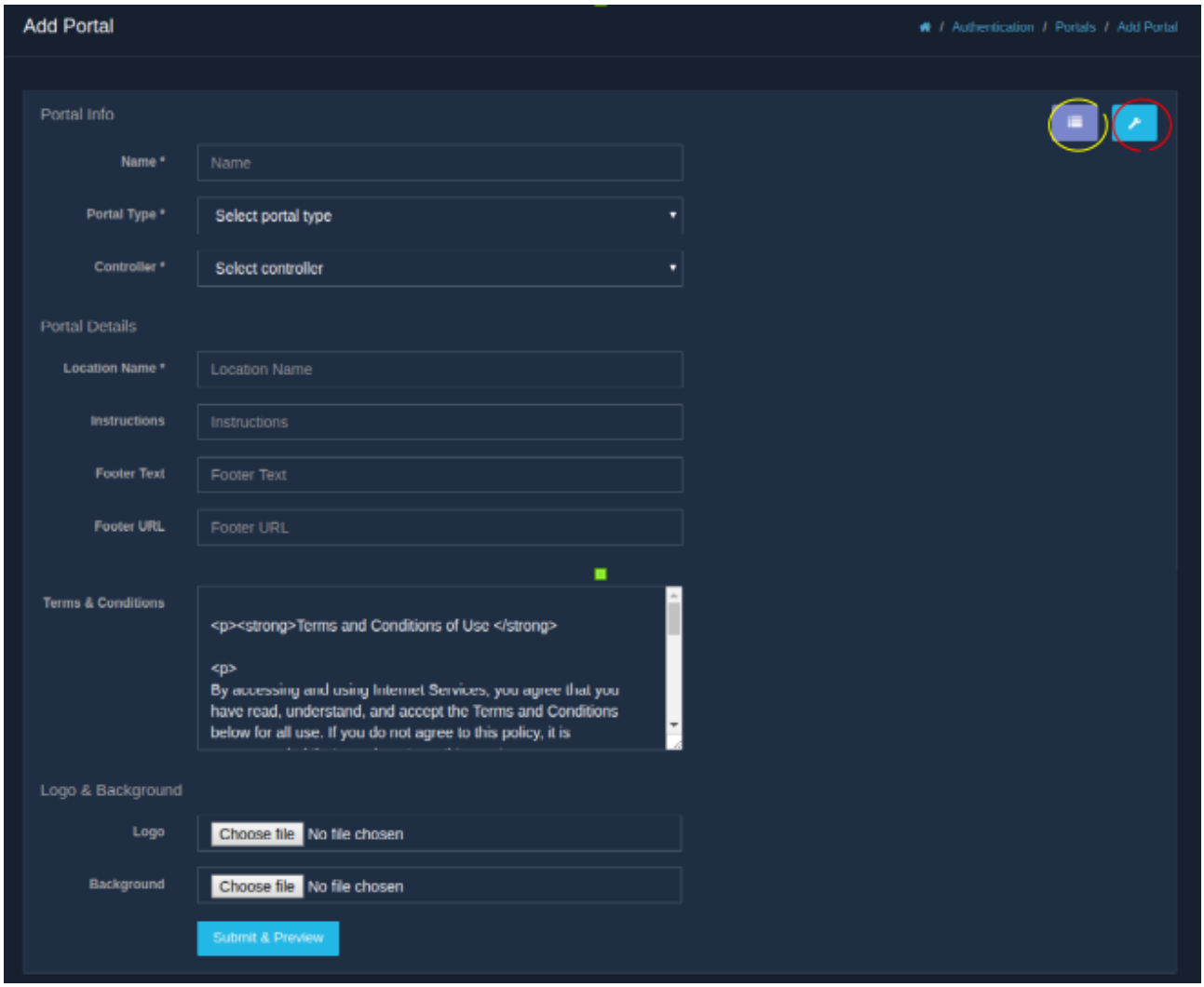
To perform multiple deletions, click on the required checkboxes and then simply click on the delete icon.

4.5 Portals

4.5.1 Create / Add Portal

Unibox provides comprehensive feature to create new portal pages. The admin can choose one template from a list of various templates to create a new portal page of choice. UniBox creates a copy of the portal template using the options selected and saves it to the local disk.

To add or create a new portal, select the ‘Portals’ section under the ‘Authentication’ module. Then, click on the ‘**+**’ icon. A page displays a form to gather information required to create a new portal.



Fig

Fields	***Description***
Name	Name of the portal page.
Portal Type	Select the portal type. See the description of various types of portal templates available. The portal type will determine the login method for the users.
Controller	Select the controller profile associated with the portal.
Location Name	Enter the location name. The name will be displayed on the portal.
Instructions	Enter the instructions for the end user. The instructions will guide the user on steps to login.
Footer Text	Enter the footer text. Eg.: Powered by Company Name.

Footer URL	Enter the footer URL.
Terms & Conditions	Enter the terms and conditions, else the default terms and conditions would be set.
Logo	Select the file for the logo. The logo will appear on the top of the portal page.
Background	Select the file for background. The background will appear behind the login section and cover the whole browser area.

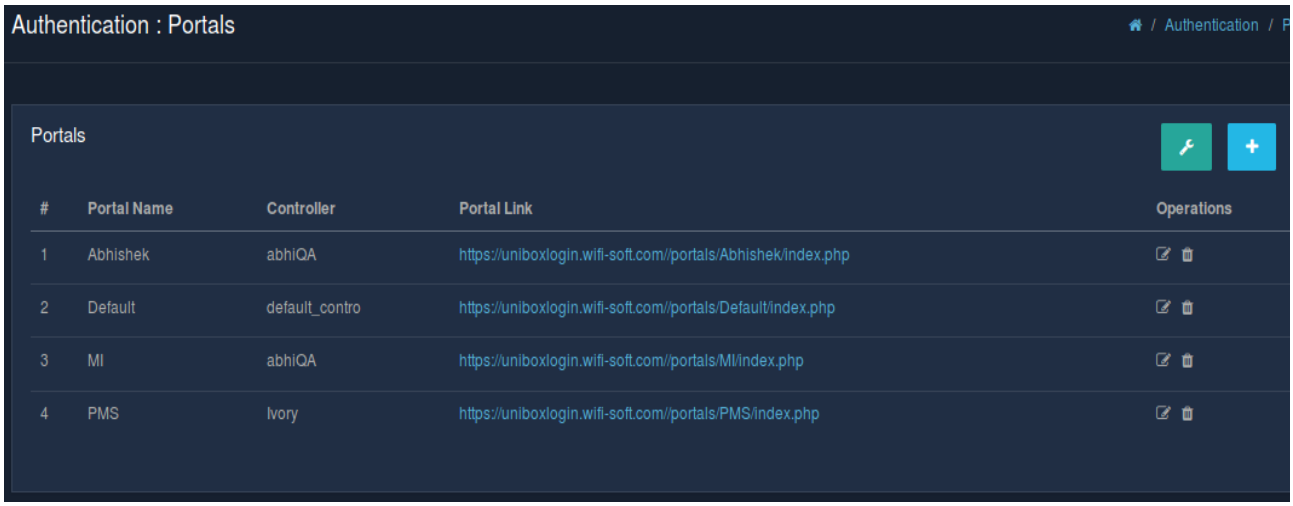
Table

Click on 'Submit & Preview' and there you have a new portal page.

4.5.2 List Portals

All the different existing portals are listed in a table. Each of the portals is assigned to a hotspot controller profile, among the different controller profiles present in the system. Multiple portals can be assigned to a single controller profile. However, at a given time only one of them could be in active state.

To view the list of portals, select the 'Portals' section under the 'Authentication' module. The list of all the different portals is displayed which contains the portal name, the controller the portal belongs to, the portal link and the 'Operations' column.



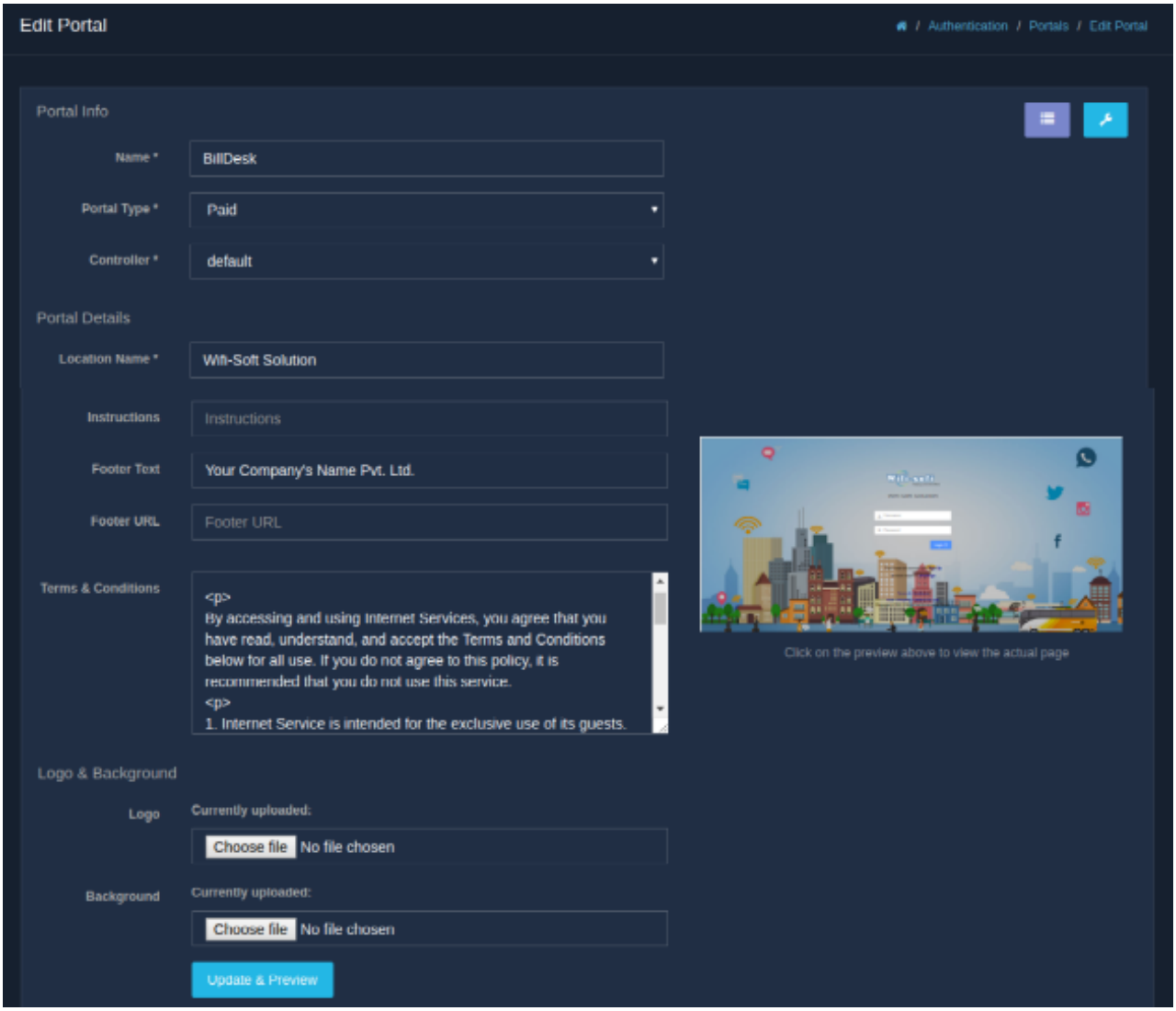
Fig

Note: All the portals are hosted inside the UniBox so these portals are not accessible from outside UniBox. To access them from remote sites, one needs to change the domain name of the portal with the public IP of UniBox.

4.5.3 Edit Portals

An admin can make changes to existing portal pages. The admin can change the portal template to offer different login methods to the end users. All the customizations will automatically apply to the new template. UniBox will replace the old copy of the template page with the new one.

To edit a portal, go to the 'Authentication' module and select the 'Portals' section. Then click on the edit icon, in the 'Operations' column, that corresponds to the portal that needs to be edited. A page displays a form, similar to the one that was displayed to create a new one, where the changes could be made. Refer



Fig

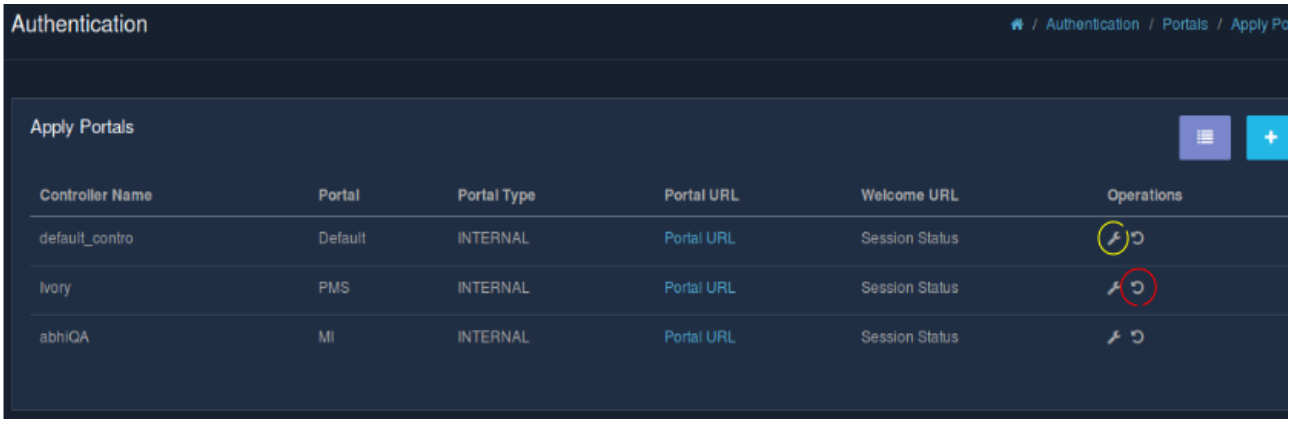
Click on the 'Update & Preview' button to apply all the changes made.

4.5.4 Apply Portals

4.5.4.1 List Active Portals

This section displays all the active portals. Every portal has a controller profile associated with it. At a given time, only one portal can be set to a controller profile.

To view all the active portals, click on the apply portal icon. A page appears that displays the list of all the active portals which includes details like controller name, portal, portal type, portal URL, welcome URL and the 'Operations' column.



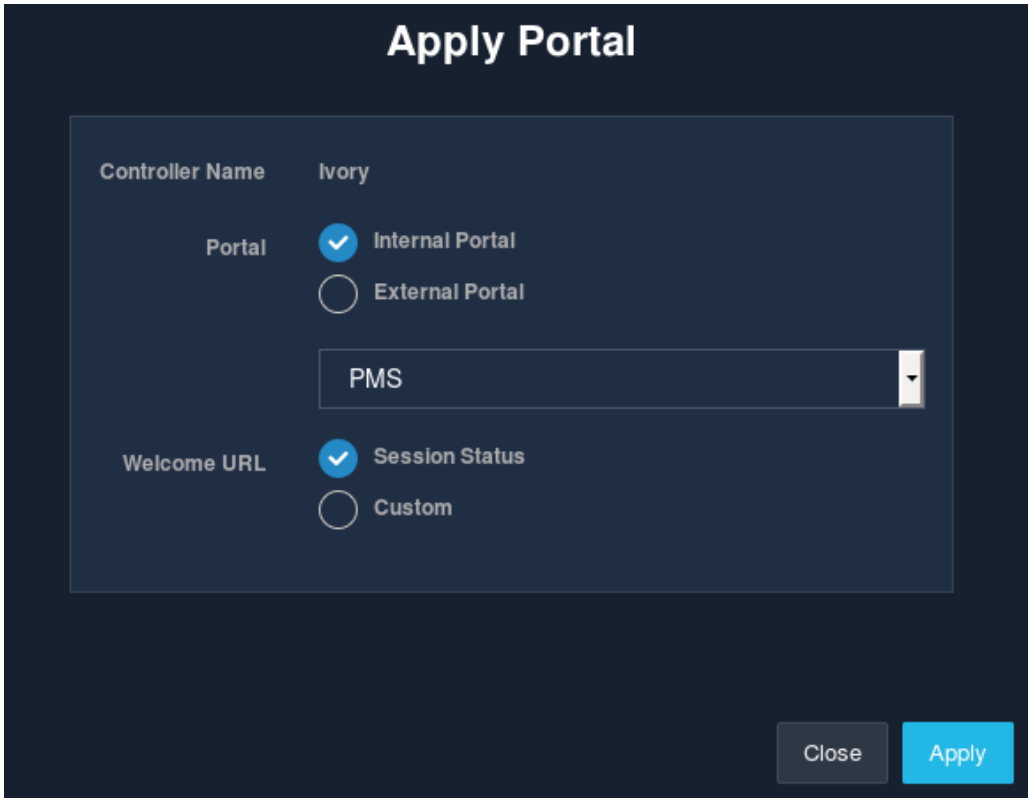
Fig

4.5.4.2 Apply Portal

The portal section allows admin to create a new portal. However, the portal will be only activated once it is applied to the specific controller profile.

This section allows an admin to set or apply a portal for a given controller profile. Click on the apply portal icon, in the 'Operations' column under the 'Portals' section, and a window appears that has options for:

- Portals: either internal or external portals, and
- Welcome URL: either session status or custom.



Fig

Fields	*Description*
Controller Name	The controller profile's name would already be displayed.
Internal Portal	Select one of the designed internal portal pages. Only one of the designed pages can be active at a time.
External Portal	Enter the URL of the external portal page. Please note that the external URL needs to be added to the passthrough list for UniBox to load the page on the user's machine. The admin needs to create the external portal using the UniBox API and should be tested separately.
Session Status	The user will be redirected to session status page that displays the statistics of the user's session on successful login.
Custom	The user will be redirected to a custom URL on successful login. If left blank, the user will be redirected to the page that the browser originally requested.

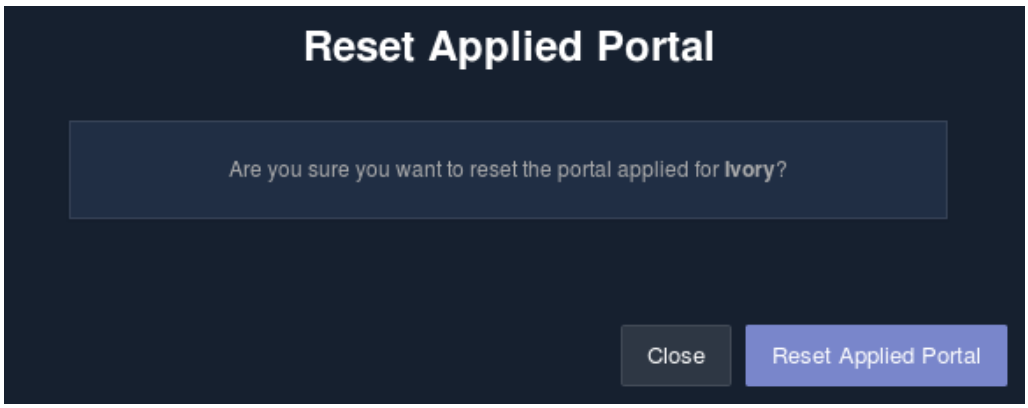
Table

Click on 'Apply' to save all the settings and apply the portal.

4.5.4.3 Reset Applied Portal

An admin is given the option to reset an existing portal from the controller profile. Once the portal is reset, the controller profile will lose the captive portal. Admin can also select another pre-configured portal for a controller profile.

To reset a portal, click on the apply portal icon, in the 'Operations' column under the 'Portals' section. Then in the list of all the active portals, click on the icon that is meant for reset portal present in the 'Operations' column. A message window pops up to confirm the decision to reset.



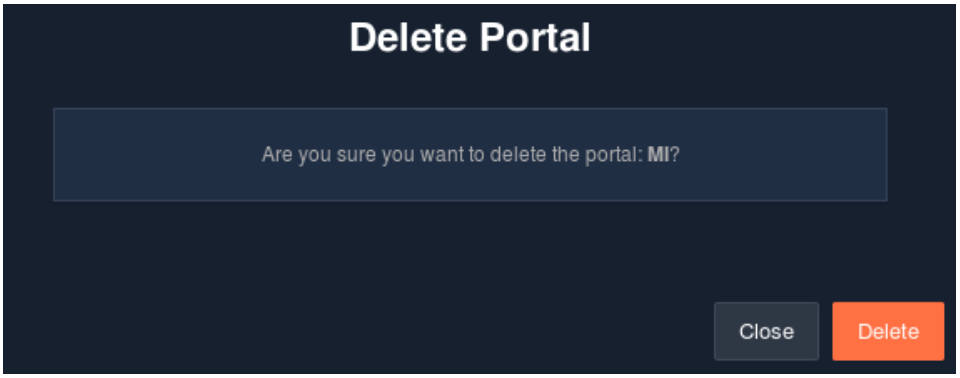
Fig

Click on the 'Reset' button, if sure.

4.5.4.4 Delete Portal

An existing internal portal can be deleted from the UniBox. If the portal page is active, i.e., it is assigned to a controller profile, then the admin would not be able to delete the portal page. Once a portal page is deleted, UniBox will automatically delete all the images, texts and customizations associated with the portal page.

To delete an existing internal portal, select the 'Portals' section under the 'Authentication' module. Then click on the delete icon in the 'Operations' column. A message window pops up to confirm the delete action.



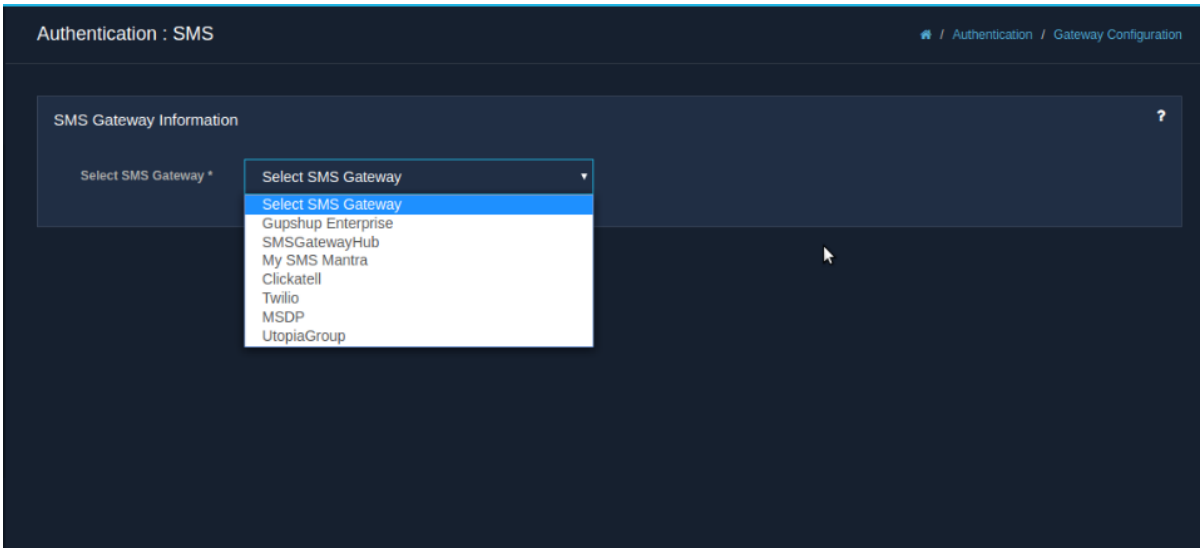
Fig

Click on the 'Delete' button to delete. And done! The portal is deleted.

4.6 SMS

SMS gateway is a feature which allows an admin to configure the settings for providing SMS based authentication. SMS gateway is used during SMS or OTP (i.e., two-factor) login and also for the approval portal. UniBox supports various SMS gateways and so an admin is provided with several options to choose from. All the settings for the SMS gateways need to be obtained from the provider.

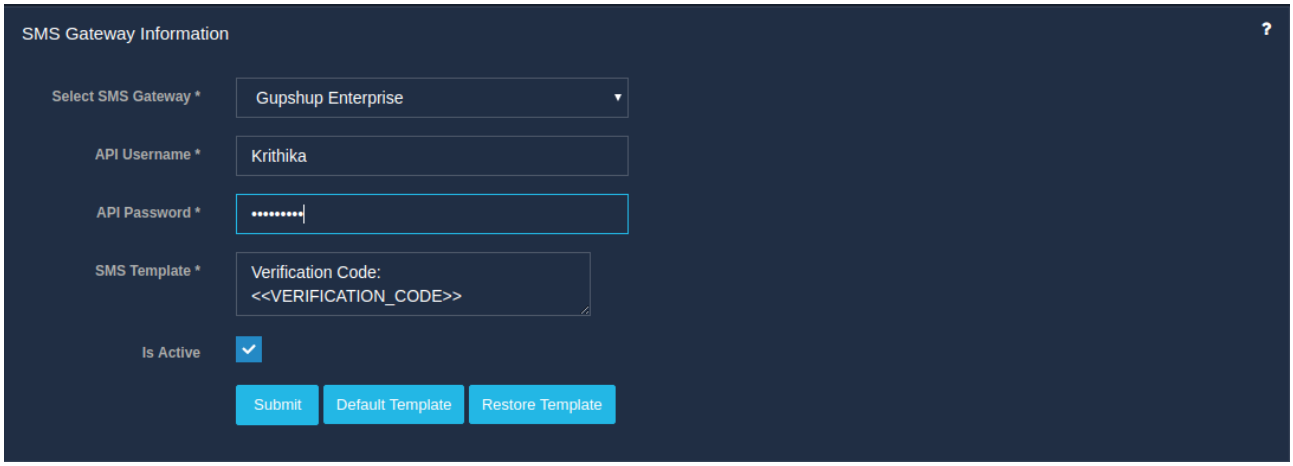
When the 'SMS' section from the 'Authentication' module is selected, a page is displayed which requires SMS gateway information. First and foremost, select an SMS gateway from the options available in the drop-down menu.



Fig

All the fields under each type of SMS gateway will be defined below:

4.6.1 Gupshup Enterprise

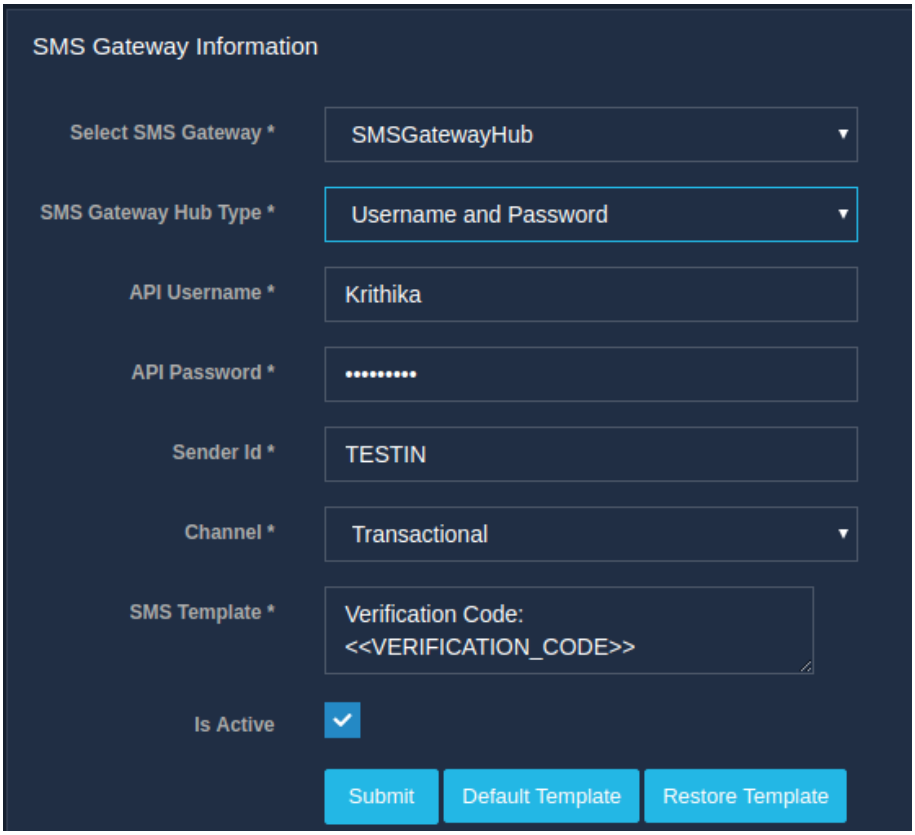


Fig

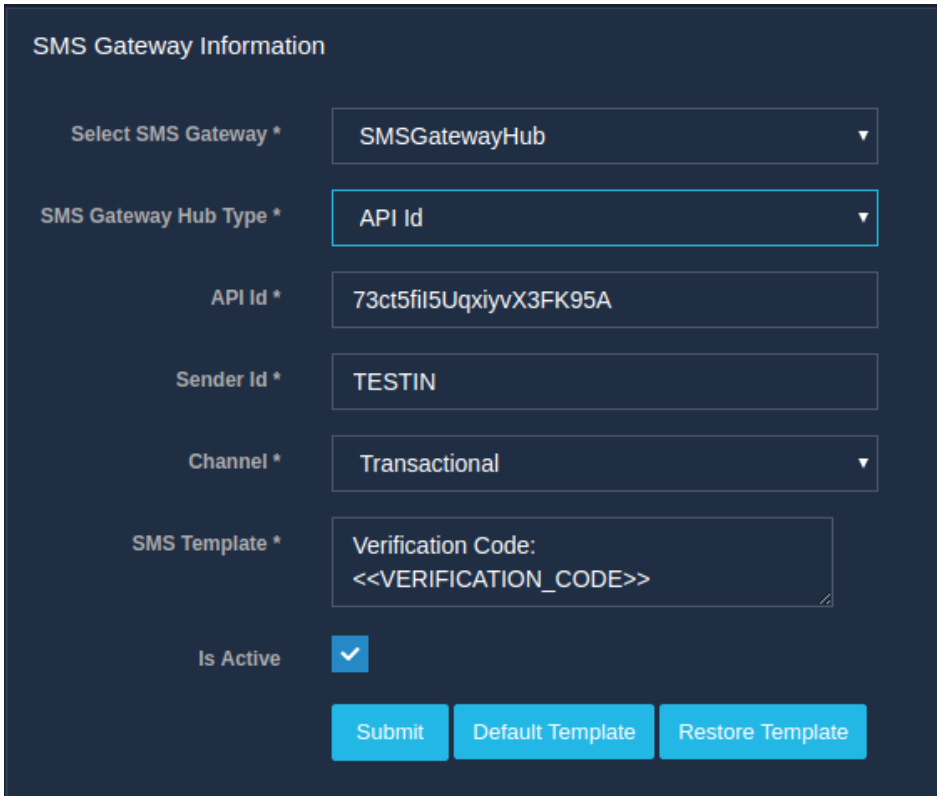
Fields	*Description*
API Username	Specify the user ID.
API Password	Specify the password.
SMS Template	Specify the content of the template. The template needs to be pre-approved from the vendor. Please get your template approved from Gupshup before uploading it.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.2 SMS Gateway Hub


SMS Gateway Information
Select SMS Gateway *
SMSGatewayHub
SMS Gateway Hub Type *
Username and Password
API Username *
Krithika
API Password *
Sender Id *
TESTIN
Channel *
Transactional
SMS Template *
Verification Code:
<<VERIFICATION_CODE>>
Is Active
Submit
Default Template
Restore Template

Fig

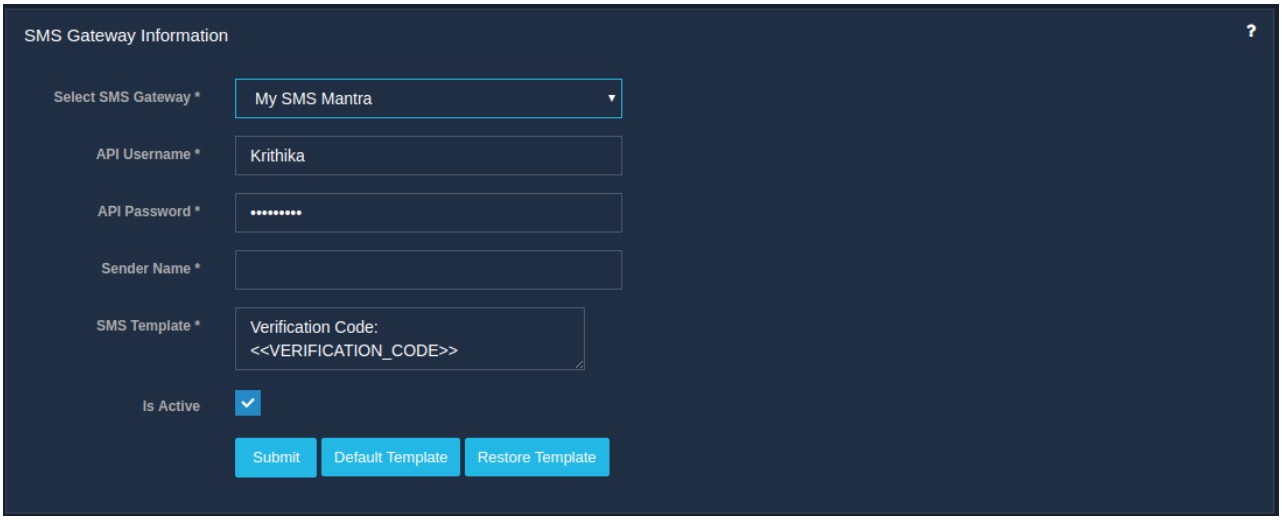


Fig

Fields	***Description***
SMS Gateway Hub Type	Select the type of gateway hub from the drop-down list.
API Username	Depending on the selected gateway hub, specify the user ID.
API Password	Specify the password.
API Id	Enter the API Id, when the selected gateway hub is API Id.
Sender Id	Enter the sender Id.
Channel	Select the channel for SMS gateway.
SMS Template	Specify the content of the template. The template may contain placeholder that will be substituted when the SMS is sent to the user.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.3 My SMS Mantra



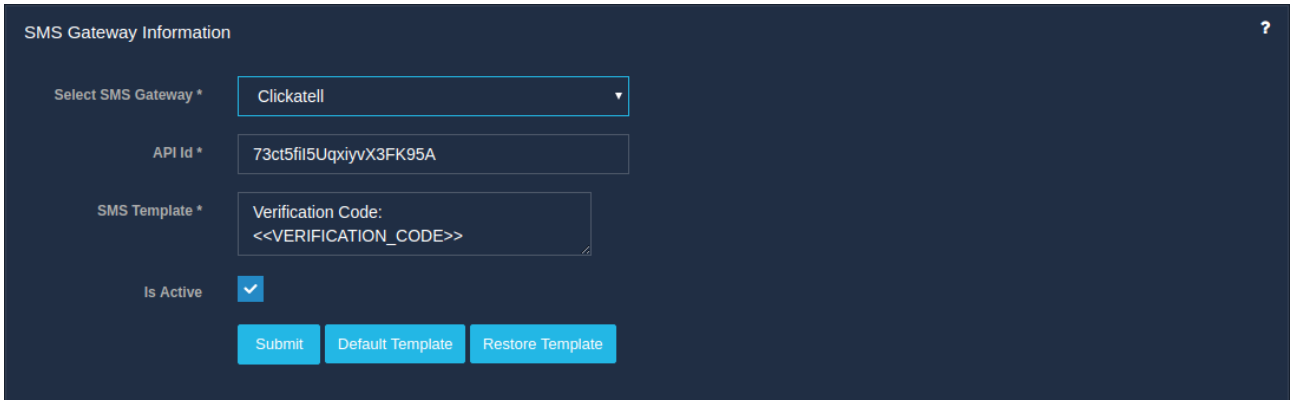
Fig

Fields	Description
API Username	Specify the user ID.
API Password	Specify the password.
Sender Name	Enter the sender's name.
SMS Template	Specify the contents of the template. The contents of the SMS will be sent to the user. If there are any placeholders, their values will be substituted before sending to the user.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.4 Clickatell

Clickatell is a global SMS gateway provider and serves many countries. Please contact Clickatell to get the SMS rates for your home country.



Fig

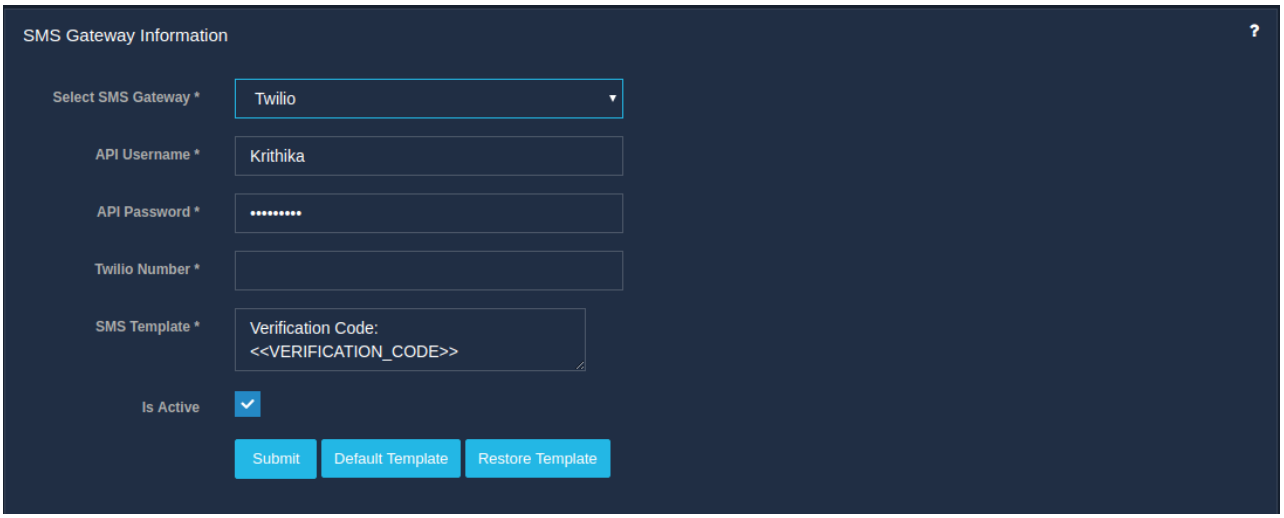
Fields	Description

API Id	Specify the API ID. The admin is supposed configure the API ID.
SMS Template	Specify the contents of the template. The admin needs to configure the template.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.5 Twilio

Twilio is another international SMS gateway. It provides SMS services to many countries. Please visit www.twilio.com to find the rates and the countries served by the SMS gateway.

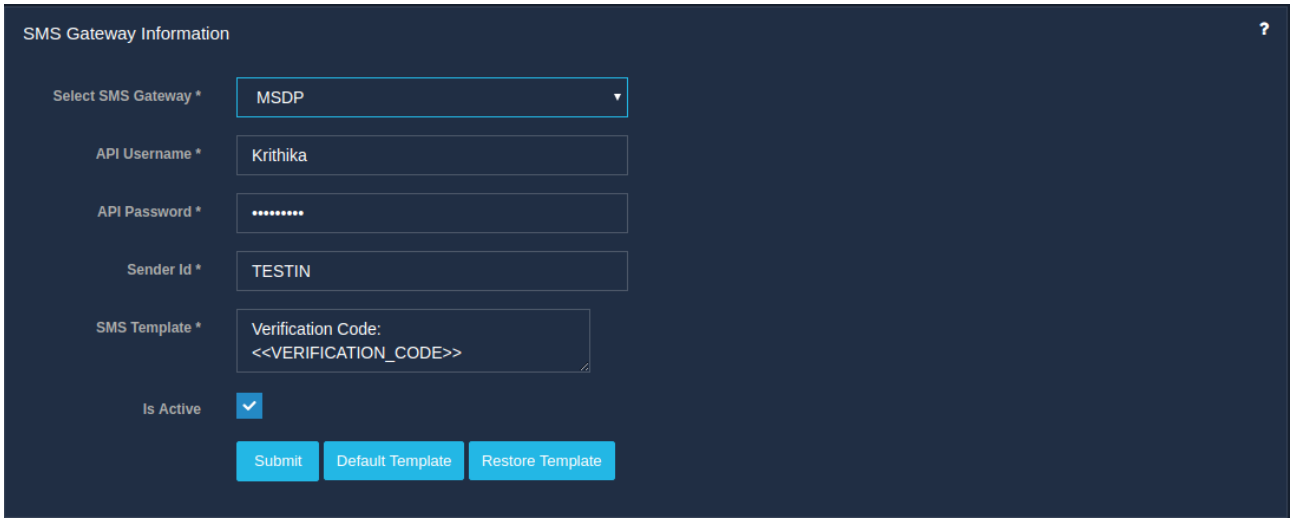


Fig

Fields	***Description***
API Username	Specify user ID.
API Password	Specify a password.
Twilio Number	Enter the Twilio number.
SMS Template	Specify the contents of the template.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.6 MSDP

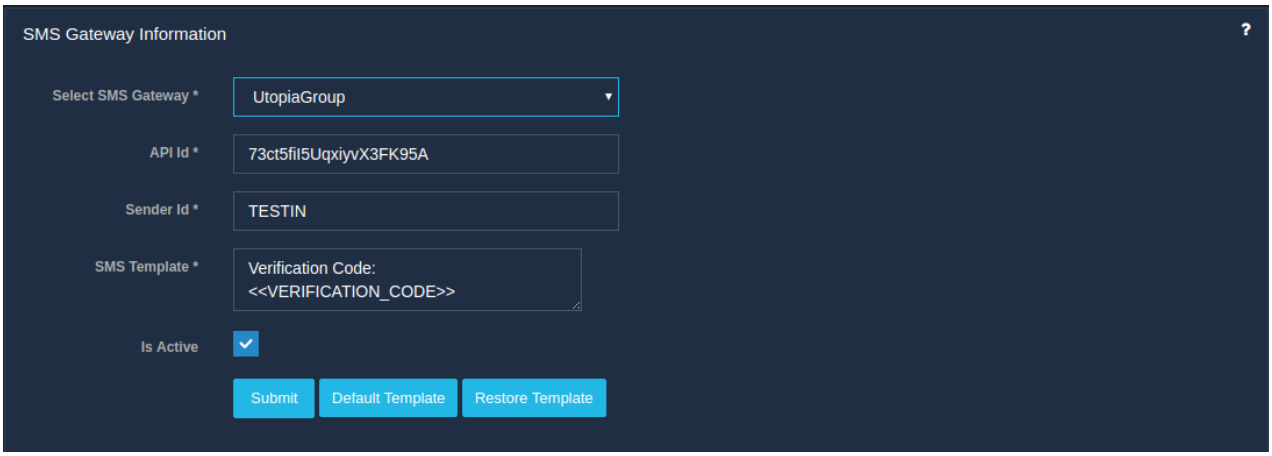


Fig

Fields	Description
API Username	Specify user ID.
API Password	Specify a password.
Sender Id	Enter the sender's ID.
SMS Template	Specify the contents of the template.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

4.6.7 Utopia Group



Fig

Fields	Description
API Id	Enter the specific API Id.
Sender Id	Enter the sender's ID.
SMS Template	Specify the content of the template.
Is Active	Tick the checkbox to enable the SMS configuration.

Table

Note:

- In all the gateways, the admin needs to configure the API Id, API Username and Password, SMS template content, Channel, and Sender Id wherever required.
- For some SMS gateway, the SMS template content needs to be vetted by the company. Please contact the respective company for the process of configuring the SMS templates.
- The SMS gateway needs to have sufficient balance for the feature to work correctly.
- **Default Template** - The user can set his or her own SMS template content. If not, a default template could be used.
- **Restore Template** – The SMS template set by the user could be retrieved by this feature.

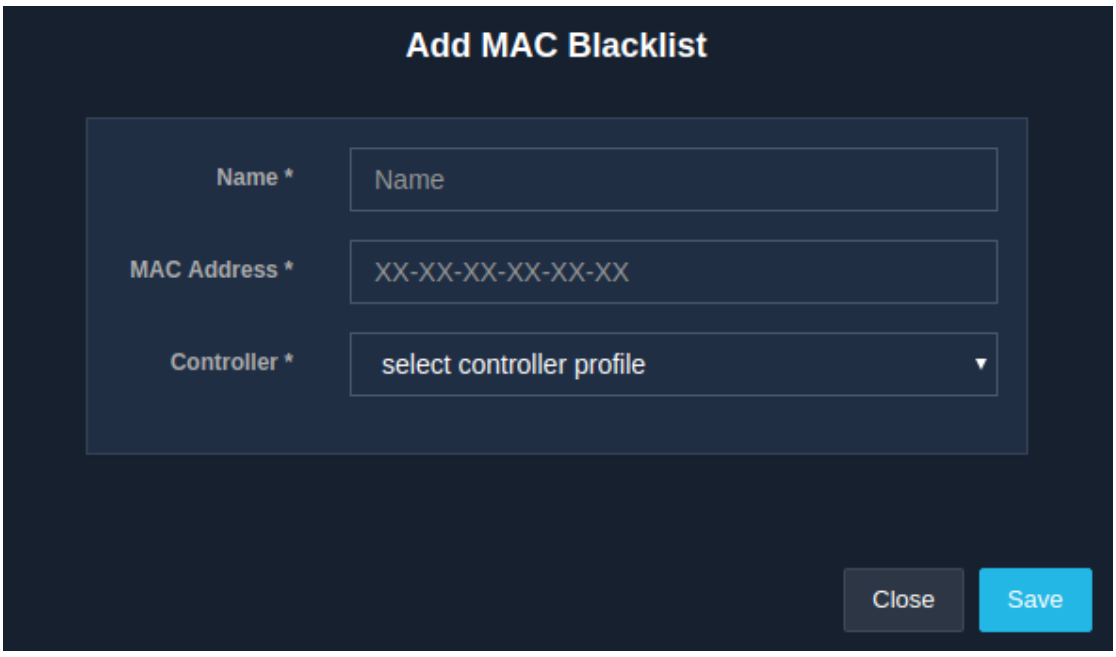
When all the information required is filled in, click on the 'Submit' button.

4.7 MAC Blacklists

Admin can block certain devices on the network. This allows admin to control who gets connected on the network. When the device is blacklisted, the user will not be allowed to join the network and use the Internet service.

4.7.1 Creation

An admin is allowed to create new MAC blocklist entries. To add new devices in the MAC blacklist, select the 'MAC Blacklists' section under the 'Authentication' module. Then click on the '**+**' icon. A window is displayed with a small form to gather the information required for adding.



Fig

Fields	*Description*
Name	Enter the name.
MAC Address	Enter a valid MAC address for blacklisting.

Controller	Select the controller profile from the drop-down menu.

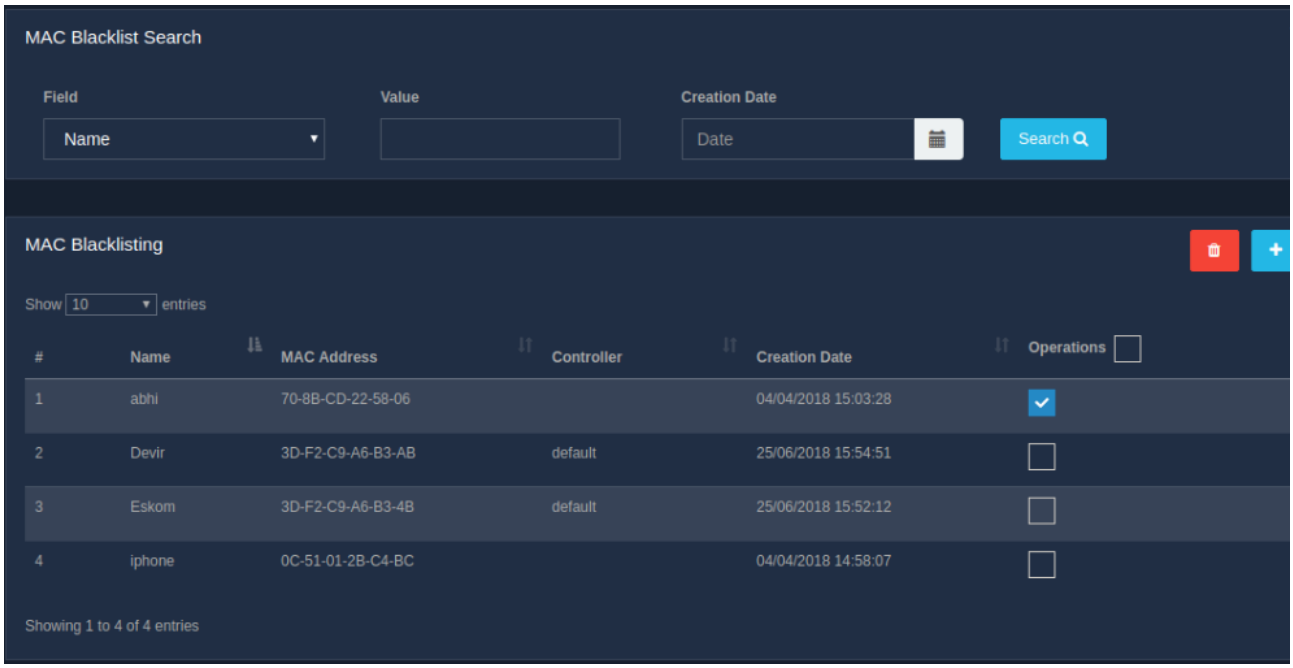
Table

Click on ‘Save’ to the add device MAC address to the list.

4.7.2 List Blacklist MAC

All the blacklisted MAC in the UniBox can be found listed in a table. The MAC addresses added in the list are not allowed to login on a given controller.

To view the list of all the blacklisted MAC, simply click on the ‘MAC Blacklists’ section present in the ‘Authentication’ module.

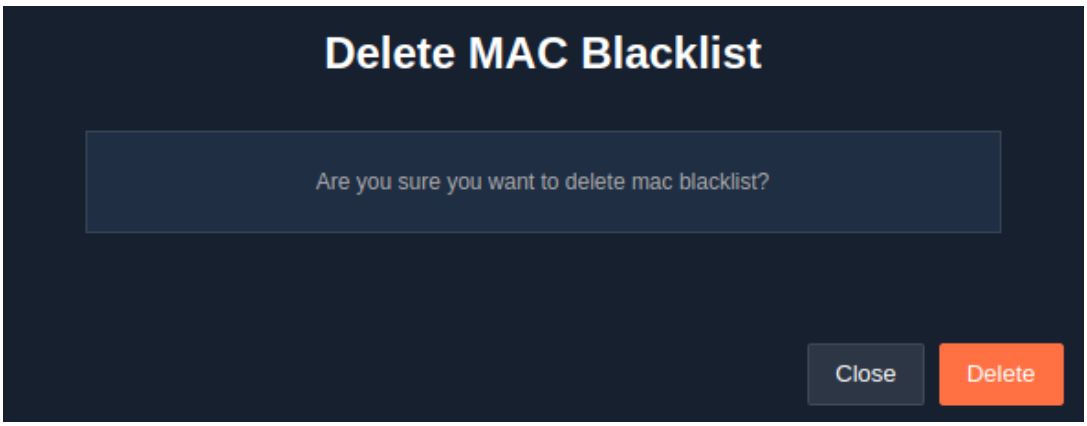


Fig

A blacklisted MAC can be also searched based on the name or MAC addresses.

4.7.3 Delete Blacklist MAC

To delete an existing blacklisted MAC entry, simply select the check-box of the respective entry and click on the **red coloured delete icon**.



Fig

To delete multiple entries at once, click on all the checkboxes of the entries that need to be deleted. Then click on the **red coloured delete icon** that appears.

4.8 External Services

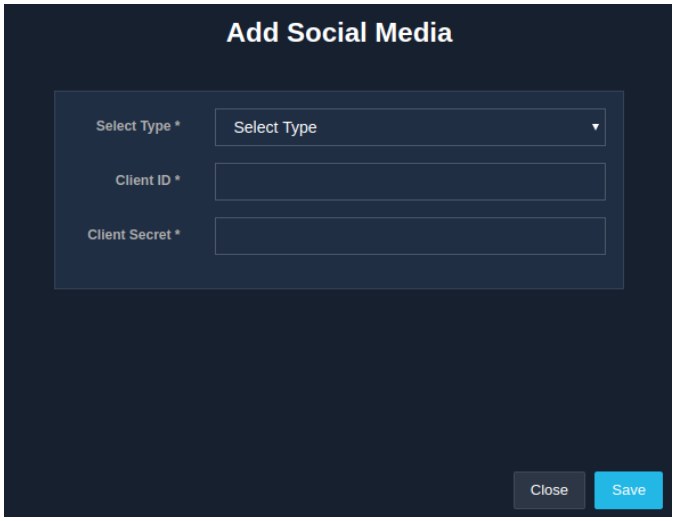
4.8.1 Social Media

Social Media section allows admin to configure the social media account credentials for enabling social media login on the captive portal.

4.8.1.1 Creation

An admin is provided with the feature to create new social media entries. The admin can specify the credentials for social media. Social media authentication might need to provide a temporary access to the user to validate against the social media servers. So, create a templogin user with username as 'templogin' and password as 'templogin123', if it is not already created.

To create new social media entries, select the 'Social Media' section in the 'External Services' sub-module, under the 'Authentication' module. Then click on the '**+**' icon where a window pops up with a form required to gather details for creating entries.



Fig

Fields	Description
Social Media Type	Select the type of social media for which the configuration will be created.
Client ID	Client ID or Oauth ID for selected social media. Please refer to the social media documentation to find how to get the Client ID from the social media settings.
Client Secret	Client secret or Oauth Secret for selected social media. Please refer to documentation for steps to get the client secret.

Table

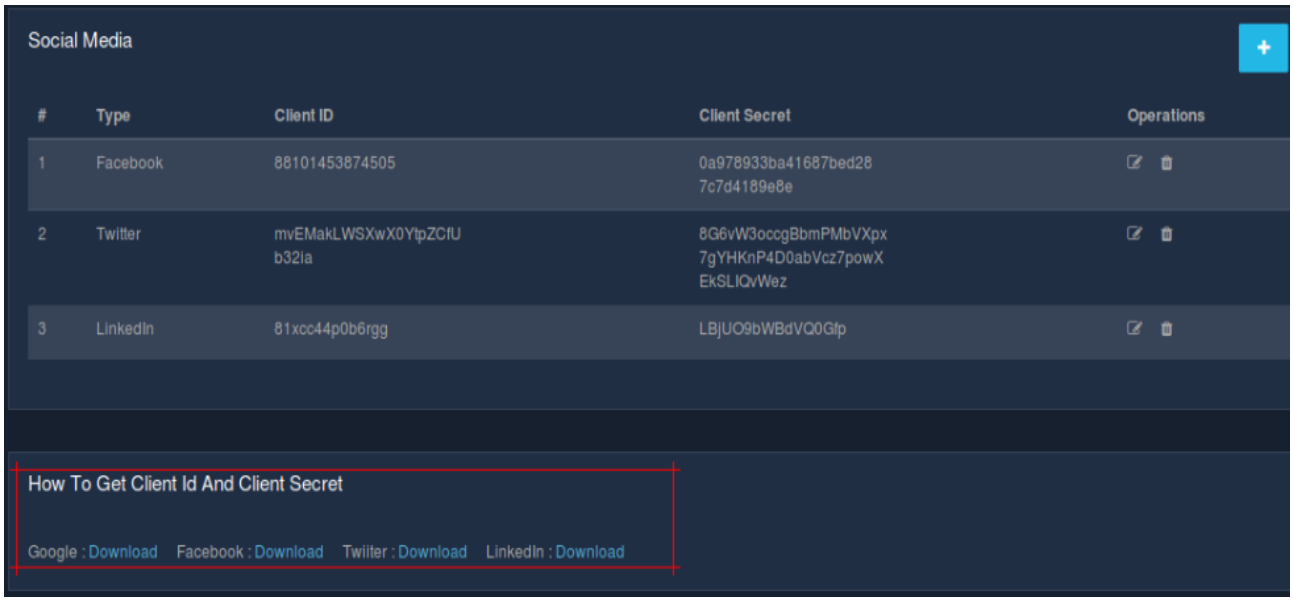
Click on the 'Save' button to save the information and add a social media entry.

Note: For a detailed information on client Id and client secret, have a look into the '**How To Get Client Id And Client Secret**' files for respective social media, present at the bottom of the listing page. Refer.

4.8.1.2 List Social Media

An admin is allowed to list the social media configurations. The list displays the client ID and client secret along with the type of the social media. The list also has a 'Operations' column, which provides the edit or delete actions.

To view the list of all the social media configurations, select the 'Social Media' section in the 'External Services' sub-module, under the 'Authentication' module.

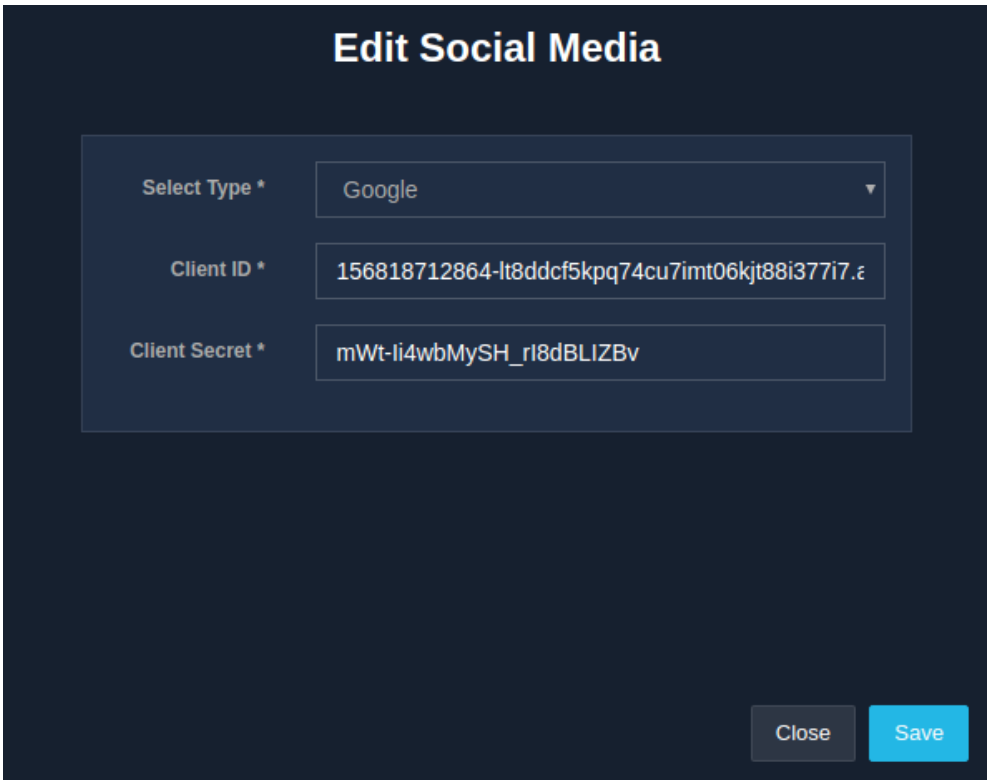


Fig

4.8.1.3 Edit Social Media

This feature allows an admin to make changes or update social media entry. The admin can specify credentials for selected social media type.

To edit a social media entry, go to the ‘Social Media’ section in the ‘External Services’ sub-module present in the ‘Authentication’ module. Then click on the edit icon present in the ‘Operations’ column. A window is displayed with a form similar to the one displayed during the creation. Refer.

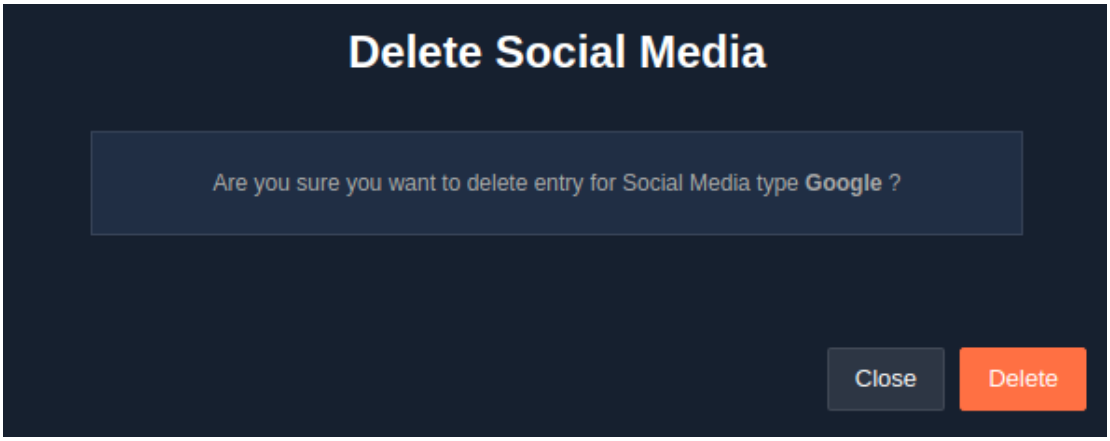


Fig

Once the required changes are made, apply the changes by clicking the ’Save’ button.

4.8.1.4 Delete Social Media

To delete a social media entry, simply click on the delete icon, in the ‘Operations’ column present in the listing table of the ‘Social Media’ section of ‘External Services’ sub-module, against the respective social media entry.



Fig

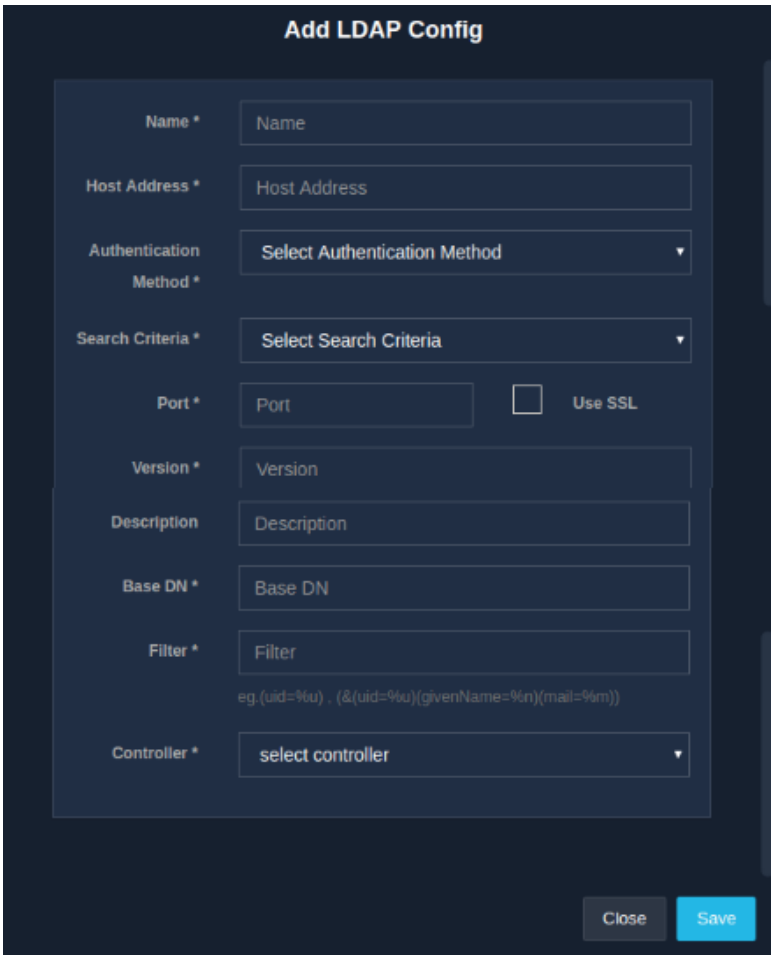
Click on the ‘Delete’ button to remove the social media entry.

4.8.2 LDAP

4.8.2.1 Add/Create LDAP

An admin is facilitated with the feature to configure and create an LDAP profile. UniBox will use the profile to establish a connection to the LDAP server to authenticate the users. The users will be authenticated with the LDAP credentials during the login process. This feature is specially useful in corporate offices, colleges and institutions that use LDAP or Active Directory for maintaining user credentials.

To create or add an LDAP profile, go to the 'LDAP' section in the 'External Services' sub-module present in the 'Authentication' module. Then click on the '**+**' icon and a window appears displaying a form to gather details required to configure an LDAP profile.



Fig

Fields	***Description***
Name	Enter the name of the LDAP profile.
Host Address	Enter the server IP address of the LDAP server
Authentication Method	Select the authentication method, whether DN (Domain Name) password or Samba NTP password, from the drop-down menu.

Search Criteria	Select the search criteria, whether anonymous or admin, from the drop-down menu.
Port	Enter the port number of LDAP server.
Version	Enter the LDAP version.
Description	Enter short description for the profile.
Base DN	Enter the base DN string.
Filter	Enter the filter string.
Controller	Select the controller profile which will access the LDAP profile.

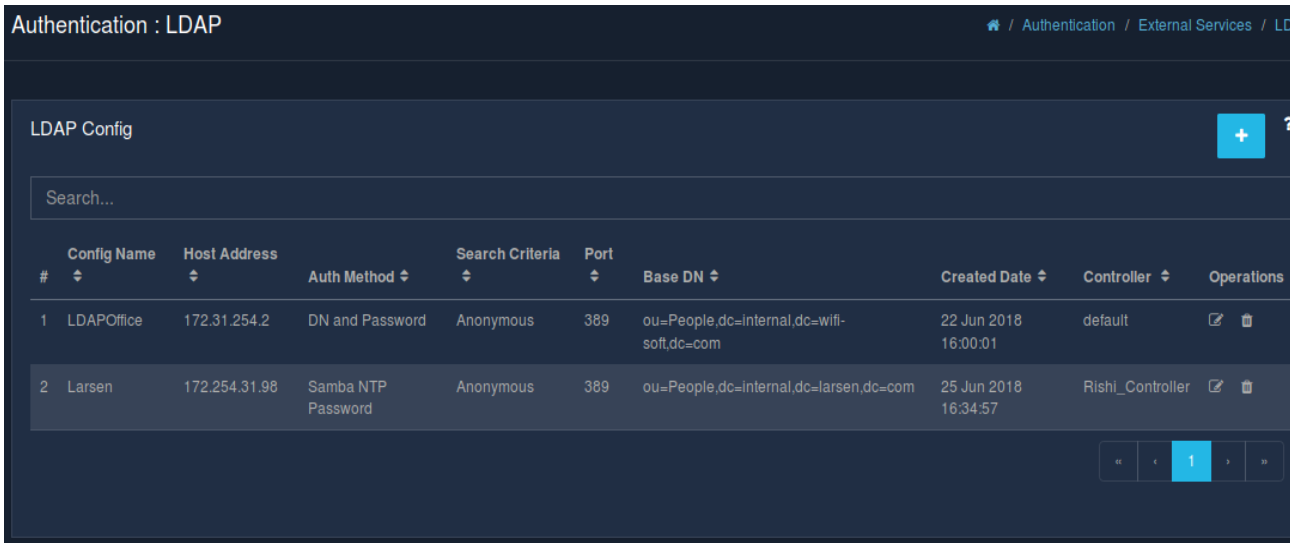
Table

Once all the configuration details are filled in, click on the 'Save' button. And there! A new LDAP profile is hence created.

4.8.2.2 List LDAP

The LDAP configurations are all listed in a tabular way which includes the config name, host address, authentication method, search criteria, port, base DN, the creation date and also the controller it belongs to. The listing table also consists of an 'Operations' column.

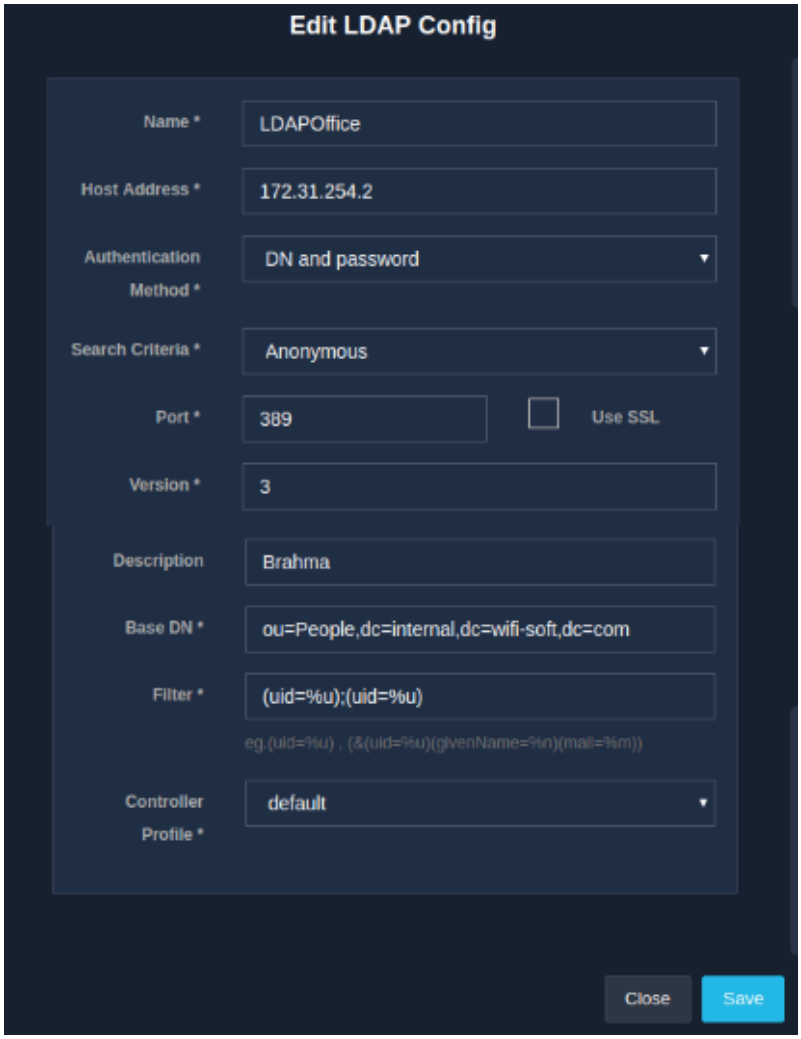
To view the list of all the LDAP configurations, select the 'LDAP' section in the 'External Services' sub-module under the 'Authentication' module.



Fig

4.8.2.3 Edit LDAP

There can be changes made to the configurations of an LDAP profile by an admin. All an admin has to do is select the 'LDAP' section in the 'External Services' sub-module present in the 'Authentication' module. Then click on the edit icon in the 'Operations' column. A window displays a form required to make changes to the configuration of an LDAP profile. Refer.

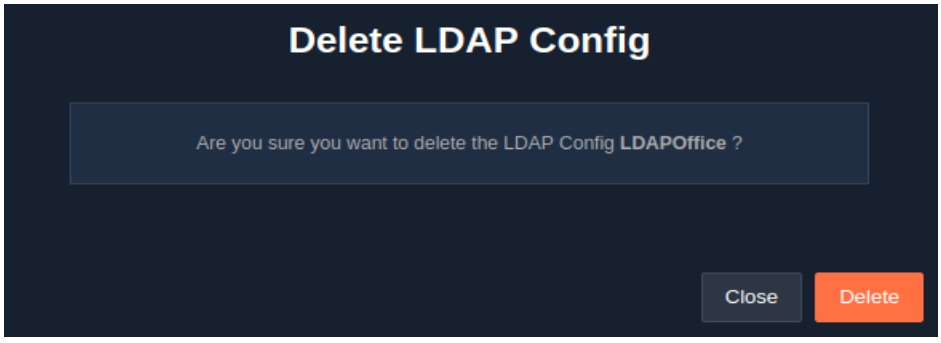


Fig

Once all the changes are made to the settings, click on the 'Save' button to apply the changes made to the LDAP profile. These changes will then be used for the subsequent logins.

4.8.2.4 Delete LDAP

Deleting an LDAP profile is simple. Click on the delete icon, present in the 'Operations' column in the 'LDAP' section which falls under the 'External Services' sub-module of 'Authentication' module. Once clicked, a window pops up to confirm the delete action.



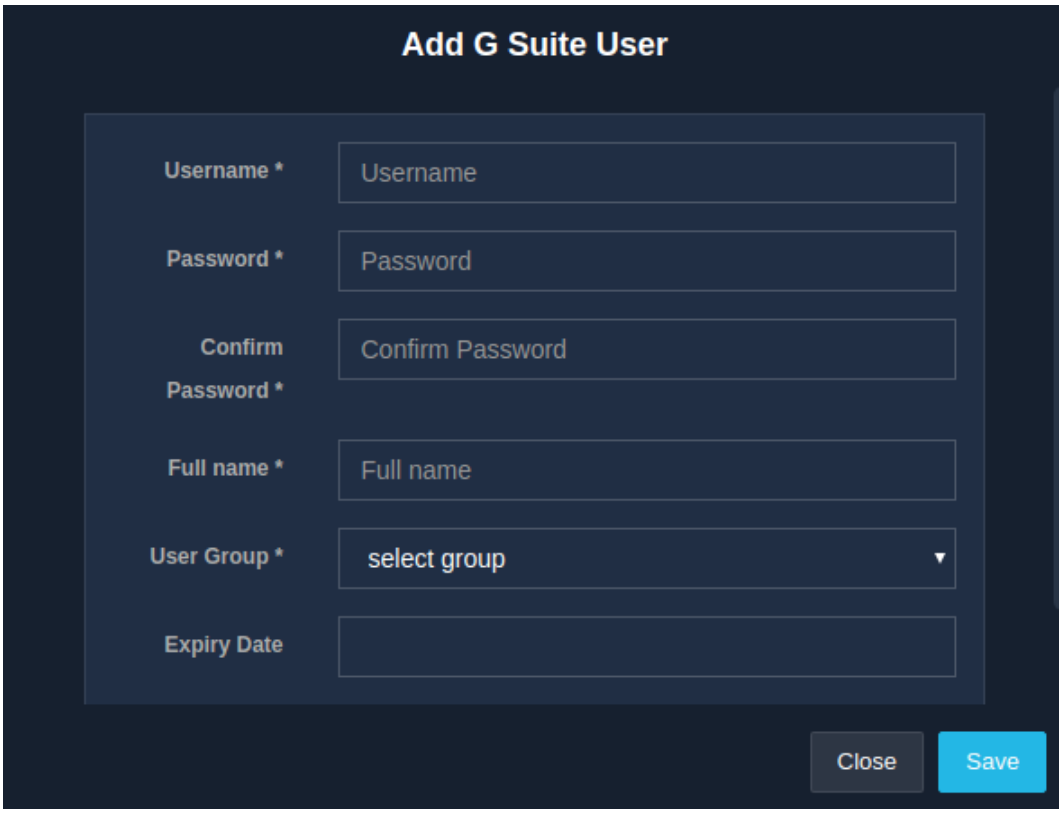
Fig

If sure, click on the ‘Delete’ button.

4.8.3 G SUITE

4.8.3.1 Create / Add GSuite

The feature to manually add a GSuite user record is made available to an admin. To create or add a new GSuite user record, go to the ‘GSuite’ section in the ‘External Services’ sub-module of the ‘Authentication’ module. Then click on the ‘**+**’ icon, a window appears with a form required to gather all the information for creating a GSuite user record.



Fields	*Description*
Username	Enter the username.
Password	Enter the password.
Confirm Password	Confirm the entered password.
Full Name	Enter the full name.
User Group	Select the user group.
Expiry Date	Use the calendar to enter the expiry date.

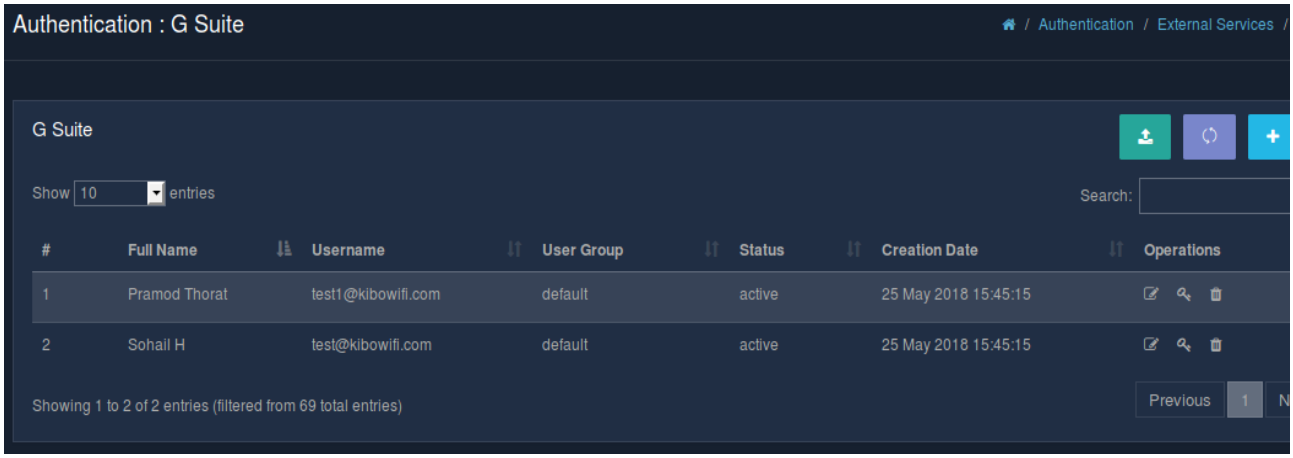
Table

Click on the ‘Save’ button to create a new record.

4.8.3.2 List GSuite

A list of all the GSuite users is displayed to an admin. The list contains all the user records that were imported from the GSuite database. The list displays the name of the user, username, group name, status, and creation date. It also contains an 'Operations' column.

To view the list of GSuite users, click on the 'GSuite' section of the 'External Services' sub-module under the 'Authentication' module.

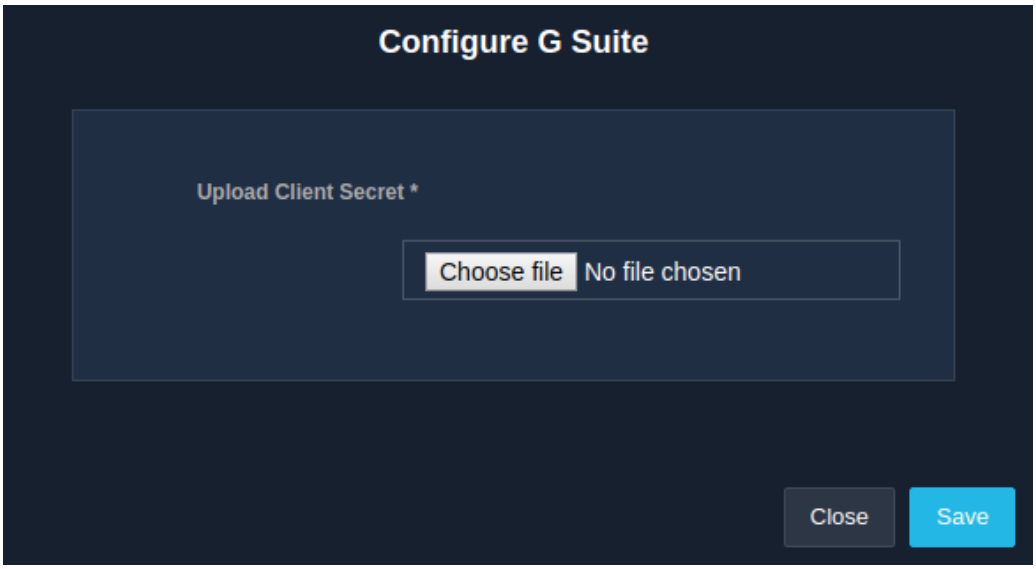


Fig

4.8.3.3 Configure GSuite

This feature enables an admin to upload the client secret key obtained from the Google Suite admin panel. Once the key is uploaded, GSuite is ready to import the users from Google.

To configure GSuite, select the 'External Services' sub-module under the 'Authentication' module. Then, select the 'GSuite' section and click on the configure icon. A window is displayed asking to upload client secret.



Fig

Choose the file and upload it, and then click on 'Save'.

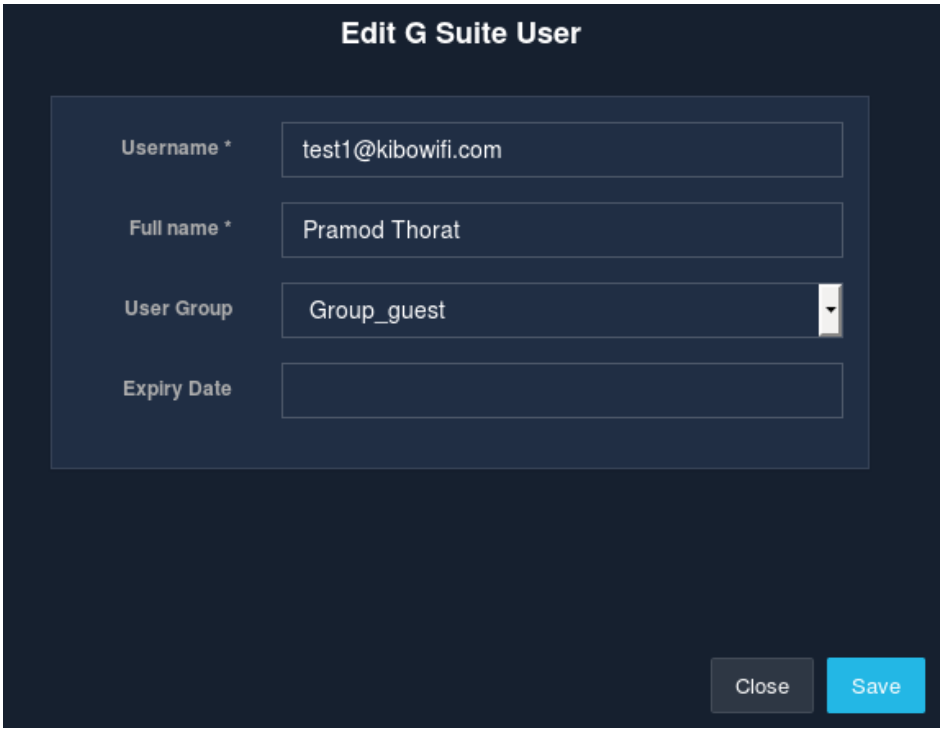
4.8.3.4 Sync GSuite

An admin is provided the facility to sync the UniBox database with GSuite. While syncing, the admin is redirected to the Google page for validation using the client secret key that was uploaded in GSuite configuration.

To sync the database with GSuite, click on the sync icon in the 'GSuite' section of the 'External Services' sub-module. If the login is successful, UniBox will sync the user records and will import the users in the local database.

4.8.3.5 Edit GSuite

Changes to an already existing user information can be made by an admin. To edit a user record, click on the edit icon present in the 'Operations' column of the 'GSuite' section. A form is displayed to make the required changes.



Fig

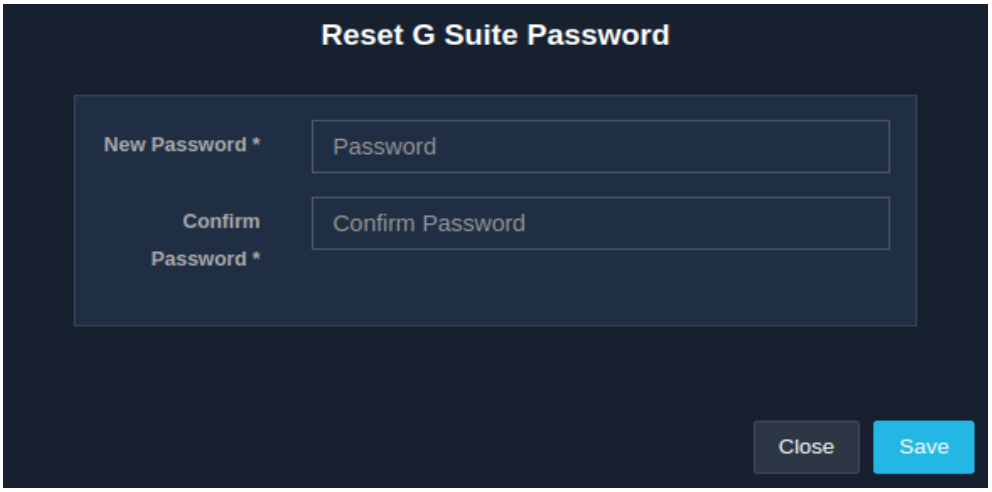
Fields	*Description*
Username	Enter the Username.
Full Name	Enter the Password.
User Group	Select the user group from the drop-down menu.
Expiry Date	Use the calendar to set the expiry date.

Table

Once the required changes are made, click on the 'Save' button.

4.8.3.6 Reset Password

A GSuite user's password can be changed and reset by an admin. To reset password, click on the reset password icon present in the 'Operations' column of the 'GSuite' section. A window is displayed where the existing password and the new password are to be entered.

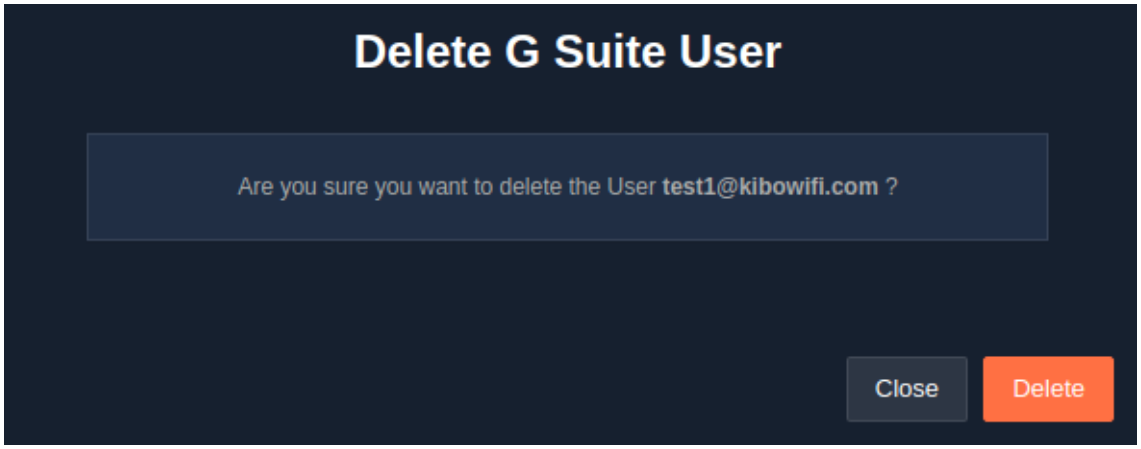


Fig

When the existing and new passwords are entered, click on the 'Save' button.

4.8.3.7 Delete GSuite

To delete a GSuite user record, all an admin has to do is to click on the delete icon present in the 'Operations' column of the 'GSuite' section. A confirmation message pops up to confirm the delete action.



Fig

Click on the 'Delete' button to remove a GSuite user record.

5. CONTROL

5.1 Policies

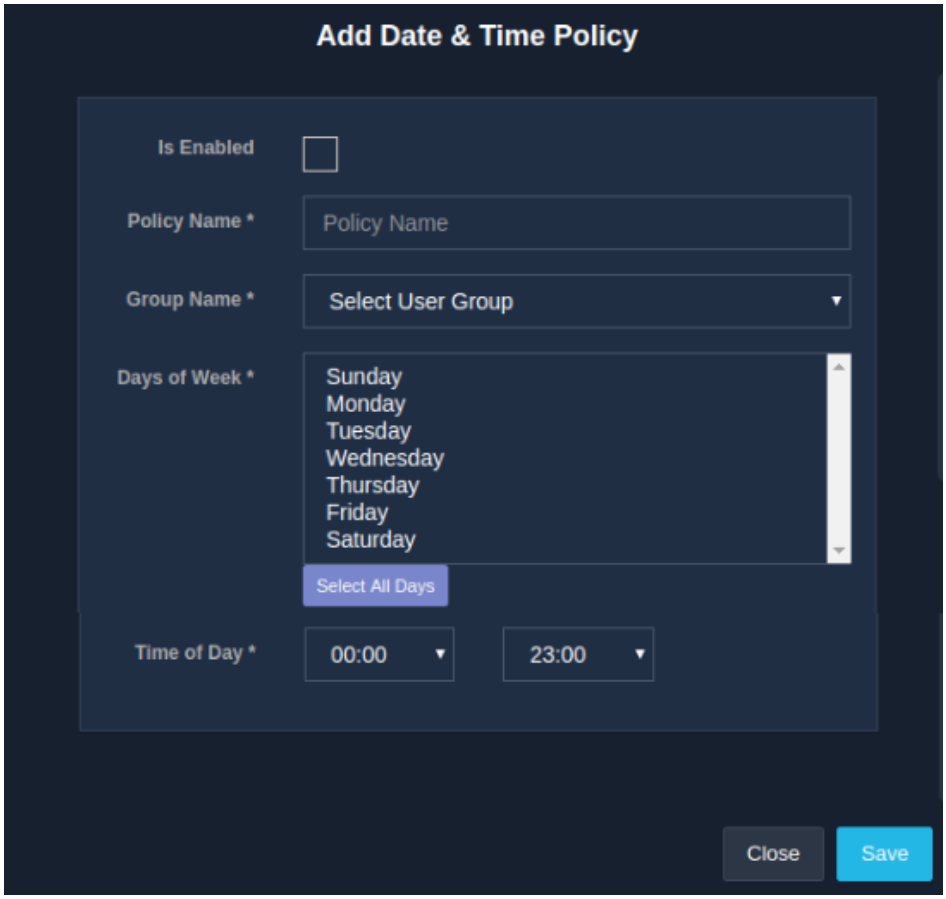
5.1.1 Date & Time

The date and time policy decides the specific date and time period when a set of users will be allowed access to the Internet.

5.1.1.1 Creation

An admin is allowed to define new date and time policy for a given user group. UniBox will grant access to the internet based on the date and time rules defined under this policy. The policy needs to be defined for a specific user group. The policy will be enforced for all users assigned to the group.

To add new date and time policy, select the 'Control' module followed by the 'Policies' sub-module. Then select the 'Date & Time' section and finally click on the '**+**' icon. A window is displayed with a form to gather information required for creating a policy.



Fig

Fields	*Description*
Is Enabled	Ticking the check-box enables the addition of the date and time policy.
Policy Name	Name of the policy.

Group Name	Select the user group on which the policy will apply.
Days of Week	Select the days of the week when user will be granted access to the internet. The 'Select All Days' option can be selected to grant a user access on all days.
Time of Day	Select the hours of the day when the user will be granted access to the internet.

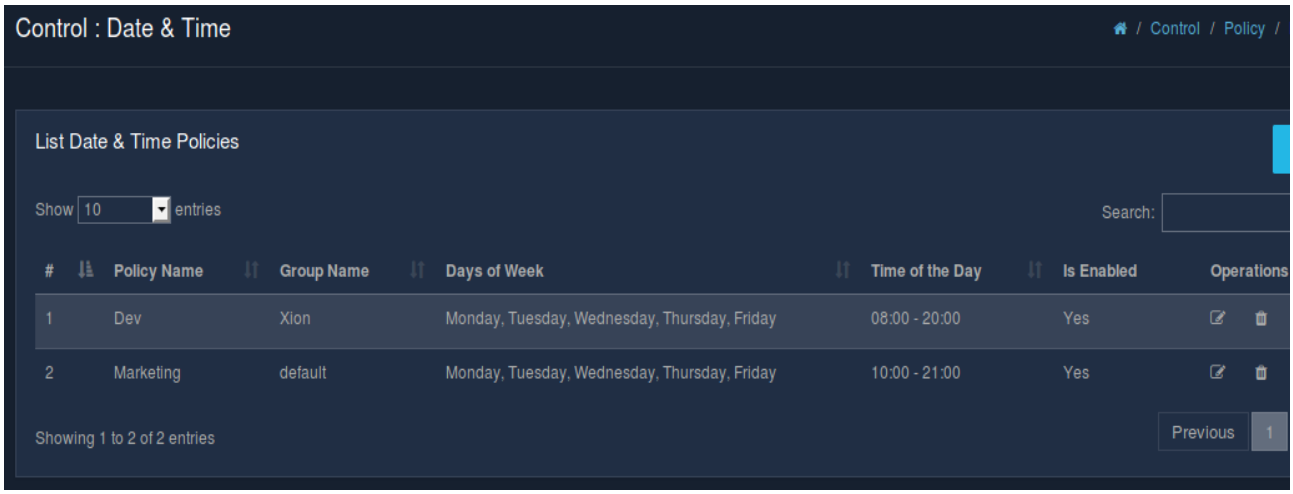
Table

Once the requirements are filled in, click on the 'Save' button to apply the settings.

5.1.1.2 List Date & Time Policy

The date and time policies defined in the UniBox are displayed in the listing table. The list allows an admin to view which policy has been assigned to which user group, whether it is enabled or not, for how many days and how long. The list also includes an 'Operations' column giving options to edit and delete.

To view the list of policies, select the 'Date & Time' section in the 'Policies' sub-module under the 'Control' module.

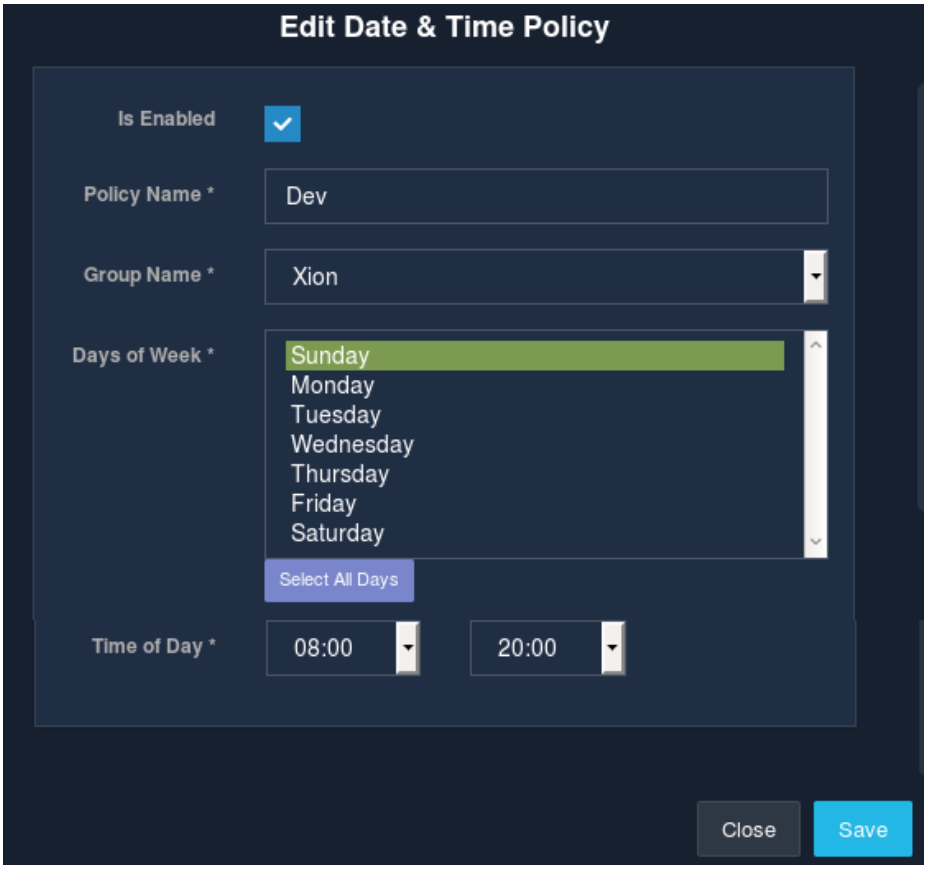


Fig

5.1.1.3 Edit Date & Time Policy

This option allows an admin to make changes to date and time policy for a given user group. Once the changes are applied, UniBox will grant access to internet based on the date and time rules defined under the edited policy.

To edit an existing date and time policy, go to the 'Control' module followed by 'Policies' sub-module and then select the 'Date & Time' section. Now, click on the edit icon present in the 'Operations' column. A modal form appears required to make the necessary changes to the policy for a given user group. Refer.



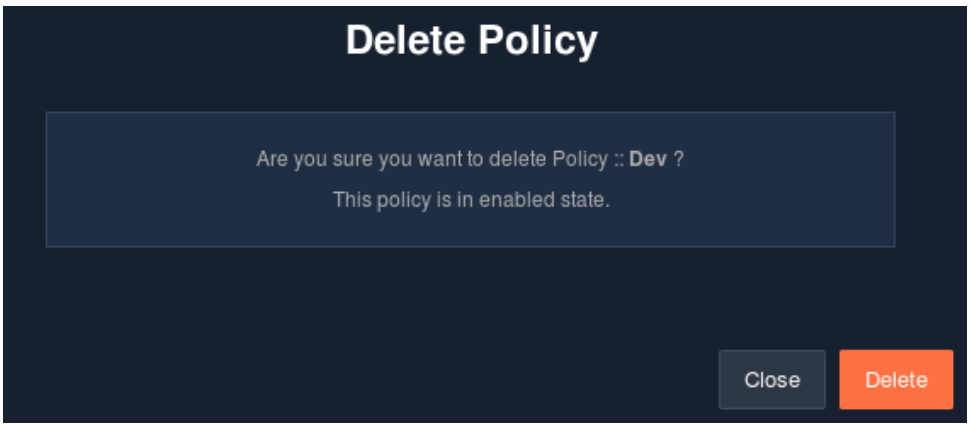
Fig

Click on the 'Save' button to apply the changes made.

5.1.1.4 Delete Date & Time Policy

This option allows an admin to delete an existing date and time policy. Though, the policy restrictions will remain on the current users until they log off.

To delete a date & time policy, click on the delete icon in the 'Operations' column of the 'Date & Time' section in the 'Policies' sub-module under the 'Control' module. Once clicked, a window pops up to confirm the delete action.



Fig

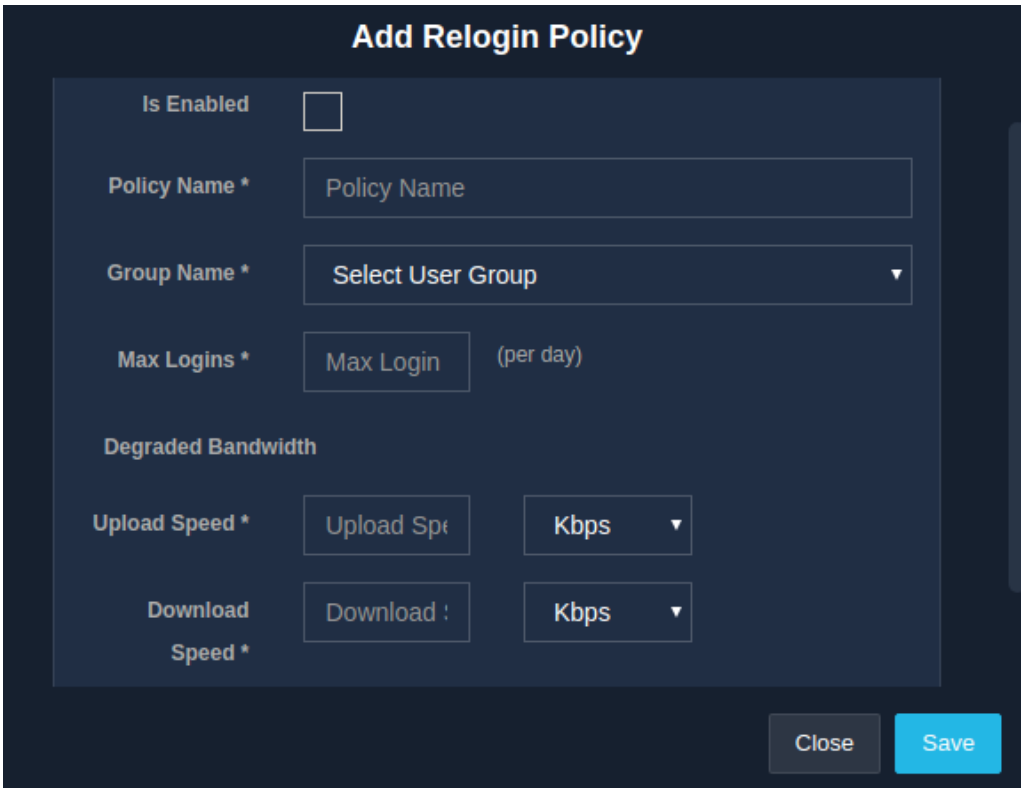
Click on the ‘Delete’ button to discard the policy.

5.1.2 Relogin

5.1.2.1 Creation

An admin is facilitated with the feature to create or add a new relogin policy for a given user group. The relogin policy will control the bandwidth allocation to the users when they login multiple times on a given day. The admin can define maximum logins, defining the maximum number of sessions that users can use before the policy is enforced. For example, if the maximum session count is 1, then the reduced bandwidth policy will be applied to all the subsequent logins on a given day.

To add a new relogin policy for a given group of users, go to the ‘Control’ module, followed by the ‘Policies’ sub-module and then select the ‘Relogin’ section. Then click on the ‘**+**’ icon, a modal form is displayed where all the information required for adding a policy is to be entered.



Fig

Fields	*Description*
Is Enabled	Ticking the check-box enables the addition of policy.
Policy Name	Name of the policy.
Group Name	Select the user group on which the policy will be applied.
Max Logins	Enter the number of maximum logins per day after which the policy will be enforced.
Upload Speed	Enter the reduced upload bandwidth once the maximum session limit is reached.

Download Speed	Enter the reduced download bandwidth once the maximum session limit is reached.

Table

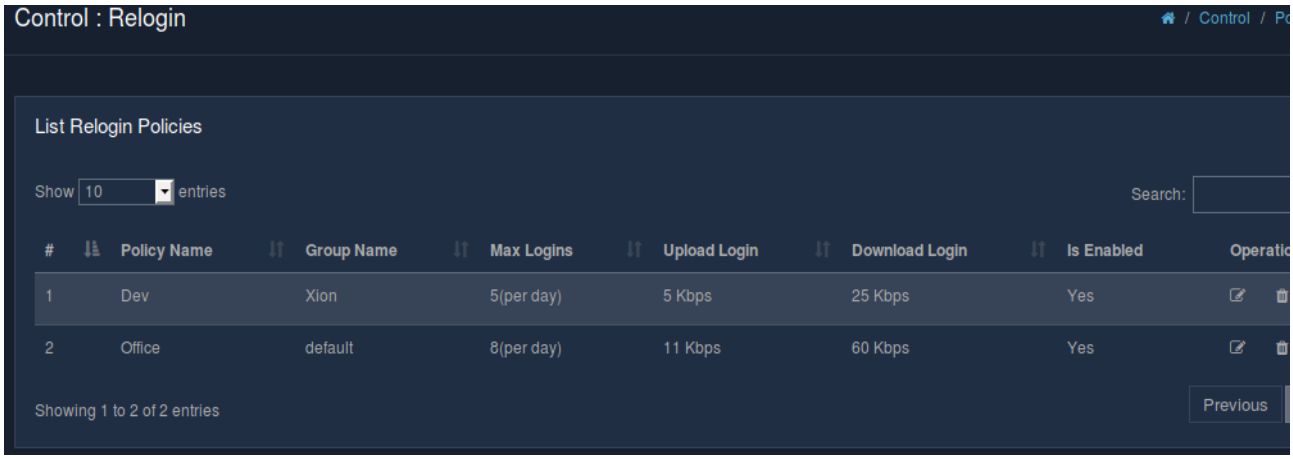
Note: The upload and download rate needs to be less than the available rate, for the restrictions to be enforced.

Fill in the modal form and then click on the ‘Save’ button.

5.1.2.2 List Relogin Policy

An admin can view a list of all the relogin policies defined in UniBox. The list allows the admin to see a user’s access restrictions, which are based on the maximum number of times the user logins in a given day.

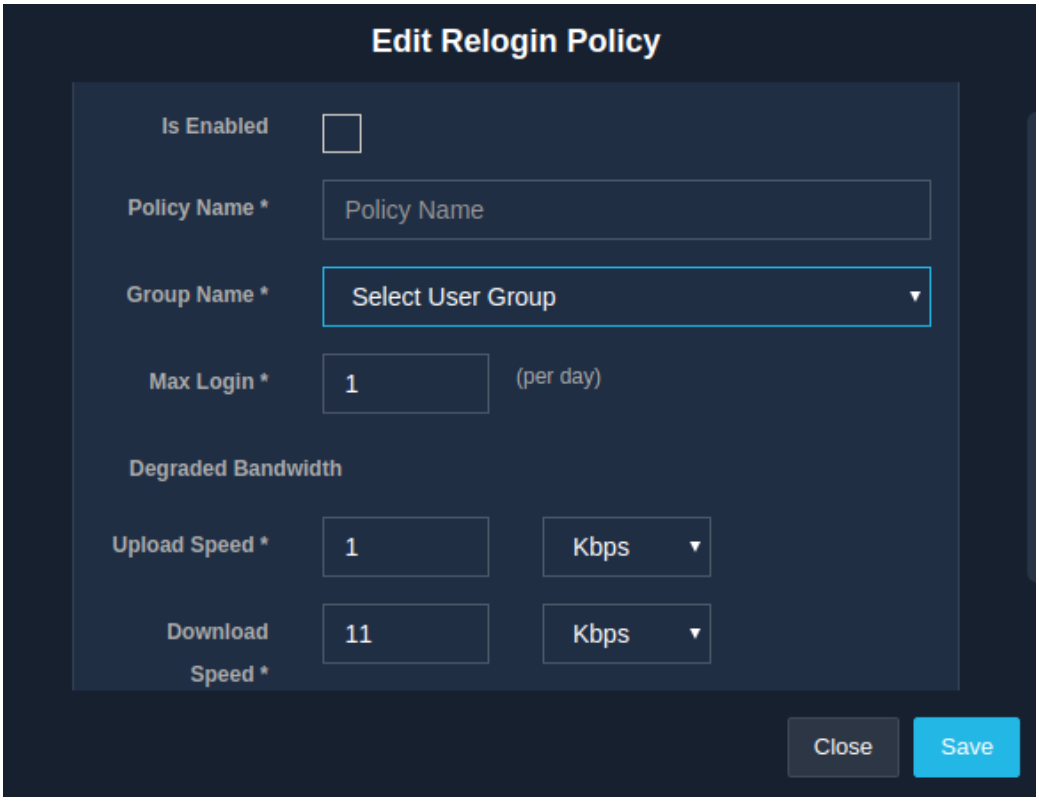
To view the list of all the defined policies, click on the ‘Relogin’ section in the ‘Policies’ sub-module which falls under the ‘Control’ module.



Fig

5.1.2.3 Edit Relogin Policy

An admin is provided with the option to make changes to an existing relogin policy of a given user group. To edit a relogin policy, select the ‘Policies’ sub-module under the ‘Control’ module and then select the ‘Relogin’ section. The list of all the relogin policies will be displayed, the listing table also contains an ‘Operations’ column wherein the options to edit and delete are available. Click on the edit icon, a modal form is displayed that gathers all the required changes to be made. Refer.

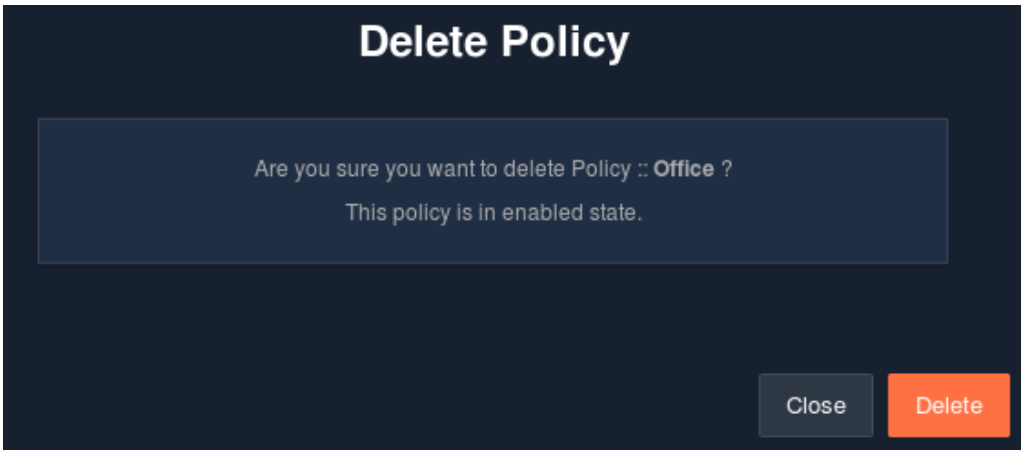


Fig

Click on the 'Save' button to save and apply all the changes made to the policies.

5.1.2.4 Delete Relogin Policy

The option to delete an existing relogin policy is provided to an admin. The policy restrictions will remain on the current users until the users log off. To delete any existing policy, the 'Operations' column in the 'Relogin' section provides the delete option. Click on the delete icon and a window appears with a message to confirm the delete action.



Fig

If sure, click on the 'Delete' button.

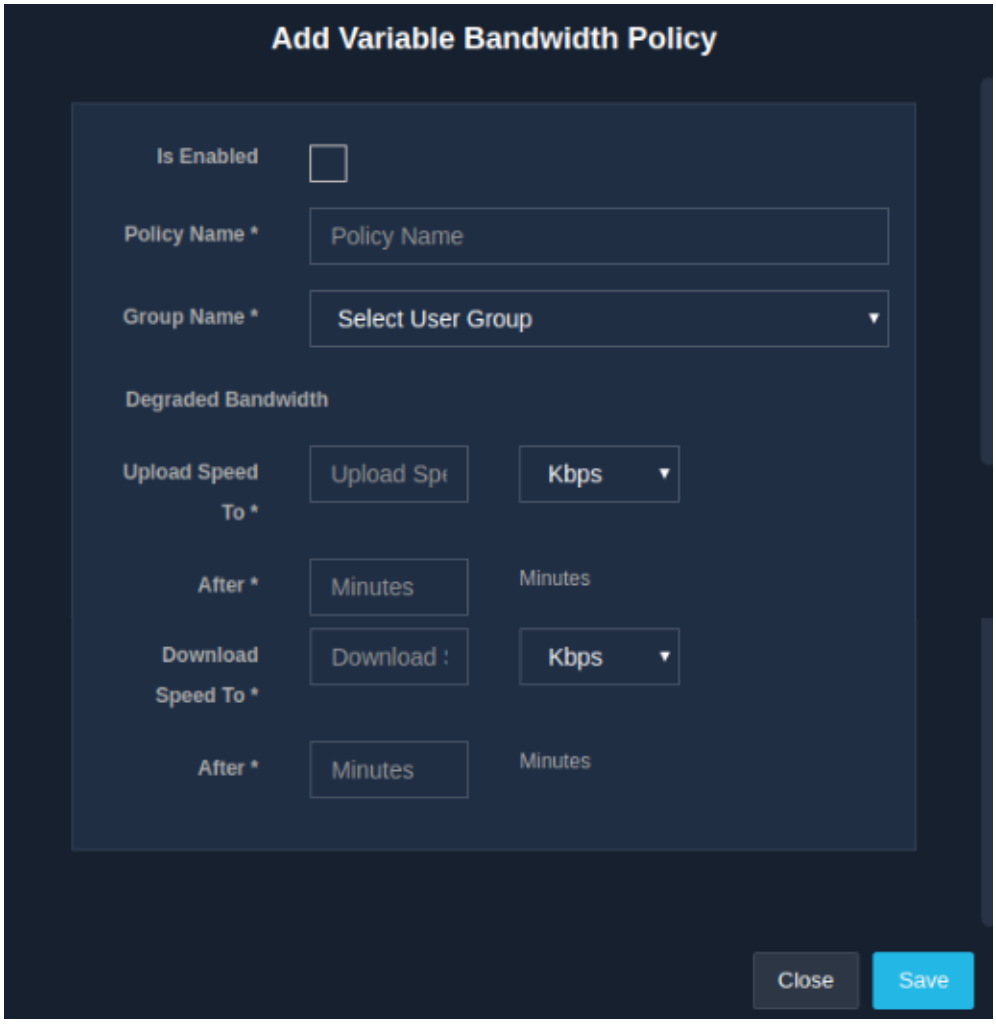
5.1.3 Variable Bandwidth

5.1.3.1 Creation

The feature to create a variable bandwidth gives an admin the option to downgrade the bandwidth rate, either upload or download, for current users that have been online for longer than the given time period.

This policy allows the admin to enforce a fair usage policy based on the online time, which means the users who are online for a longer period of time will automatically get reduced bandwidth. This policy is applied in real-time i.e. it affects the users who are currently online.

To create a variable bandwidth policy, go to the 'Control' module followed by the 'Policies' sub-module. Then select the 'Variable Bandwidth' section and click on the '+' icon. A modal form is displayed that requires all the necessary details to create a policy.



Fig

+Fields	*Description*
Is Enabled	Ticking the checkbox enables the addition of policy.
Policy Name	Name of the policy.
Group	Select the user group on which the policy will be applied.

Upload Bandwidth	Enter the upload bandwidth rate that will be applied to users in a group after a certain time period.
Download Bandwidth	Enter the download bandwidth rate that will be applied to users in a group after a certain time period.
After (mins)	Enter the time period after which the policy will be in effect.

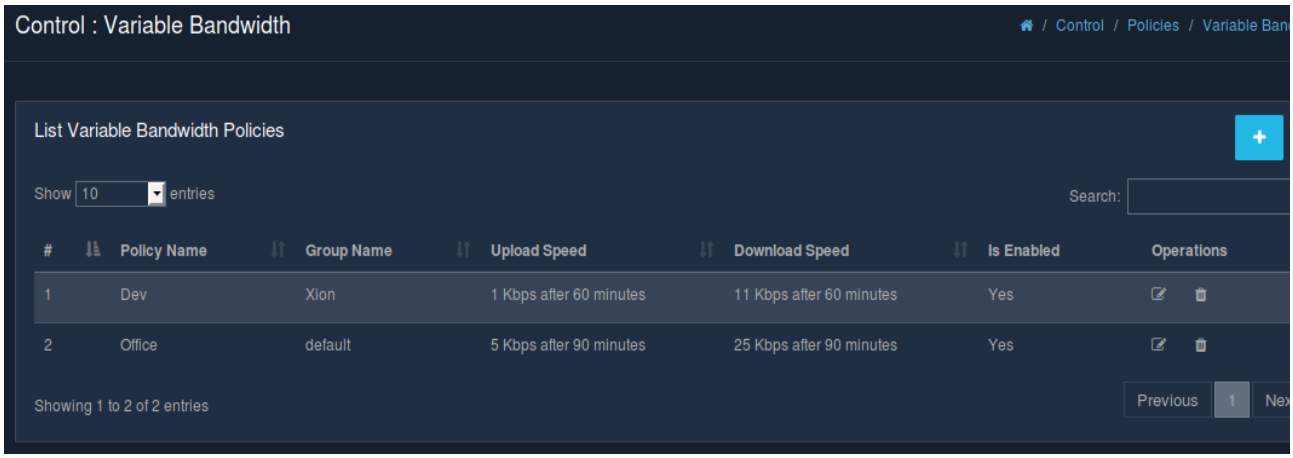
Table

When all the required details are entered, click on the 'Save' button.

5.1.3.2 List Variable Bandwidth Policy

An admin is allowed to view all the variable bandwidth policies defined in the UniBox. The list displays the group name, the upload and download speed, whether it is enabled or not, along with the policy name. The list also includes an 'Operations' column, which provides the options to edit and delete policies.

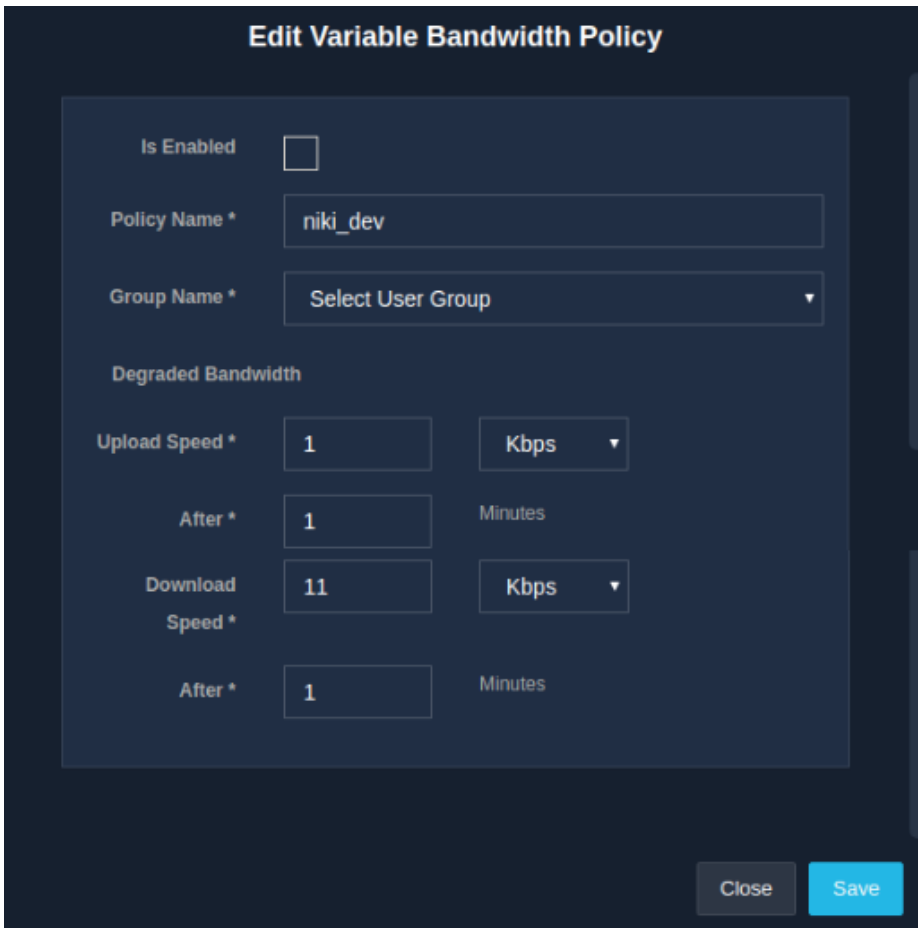
To view the list of all the defined policies, go to the 'Control' module followed by the 'Policies' sub-module. Then select the 'Variable Bandwidth' section.



Fig

5.1.3.3 Edit Variable Bandwidth Policy

This feature allows an admin the option to edit and make changes to the existing variable bandwidth policies. To edit the policies, click on the edit icon present in the 'Operations' column of the 'Variable Bandwidth' section which falls under the 'Policies' sub-module. A modal form appears that is required to make the necessary changes. Refer.



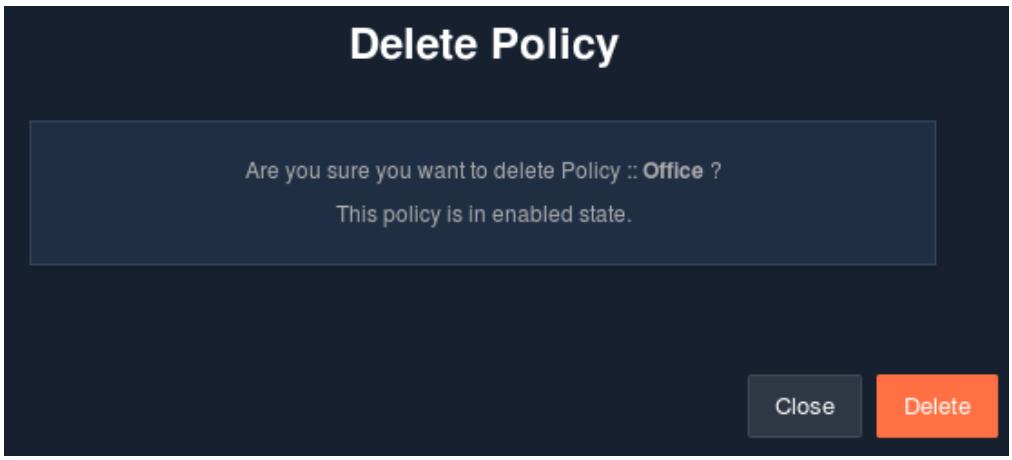
Fig

Click on the 'Save' button to apply the changes made.

5.1.3.4 Delete Variable Bandwidth Policy

This option allows an admin to delete an existing variable bandwidth policy. The policy restrictions will remain enforced on the current users until the users log off.

To delete the policies, click on the delete icon present in the 'Operations' column in the 'Variable Bandwidth' section under the 'Policies' sub-module. A message window appears asking to confirm the delete action.



Fig

Click on the ‘Delete’ button to delete a policy.

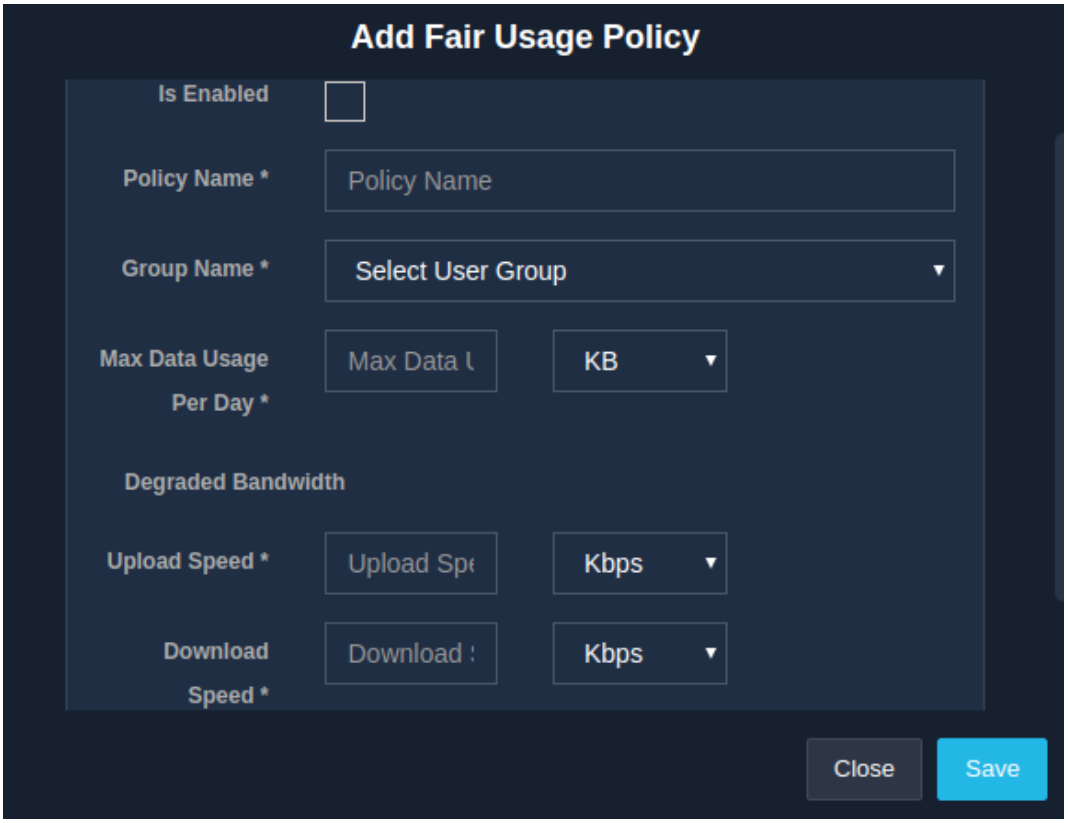
5.1.4 Fair Usage

Fair Usage policy allows admin to ensure fair usage of bandwidth on the network. This policy will automatically reduce the speed of the users who are abusing the network resources. The policy applies to real-time users and gets enforced on the users when they are online. The policy will penalize the users who use more than the allotted bandwidth.

5.1.4.1 Creation

This feature allows an admin to create policies to degrade the bandwidth rate for users of a given group who have exceeded the data usage limit. This policy would allow an admin to find users who use an extensive amount of data transfer, in turn causing traffic congestion on the network. This policy is applied in real-time based on the data usage of online users.

To create a fair usage policy, select the ‘Fair Usage’ section in the ‘Policies’ sub-module under the ‘Control’ module. Then click on the ‘**+**’ icon where a window appears displaying a form to collect information required to create the policy.



Fig

Fields	*Description*
Is Enabled	Ticking the check-box enables the addition of policies.
Policy Name	Name of the policy.
Group	Select the user group where the policy will be applied.
Maximum Data Usage	Maximum data usage limit (upload + download data) allowed to a user of a group for a given day. This is the

	amount of data that the user can consume at the assigned rate. After this limit is reached, the fair usage policy will take effect.
Upload Speed	Enter the upload bandwidth rate that will be applied to users in a group after the data usage limit exceeds.
Download Speed	Enter the download bandwidth rate that will be applied to users in a group after the data usage limit exceeds.

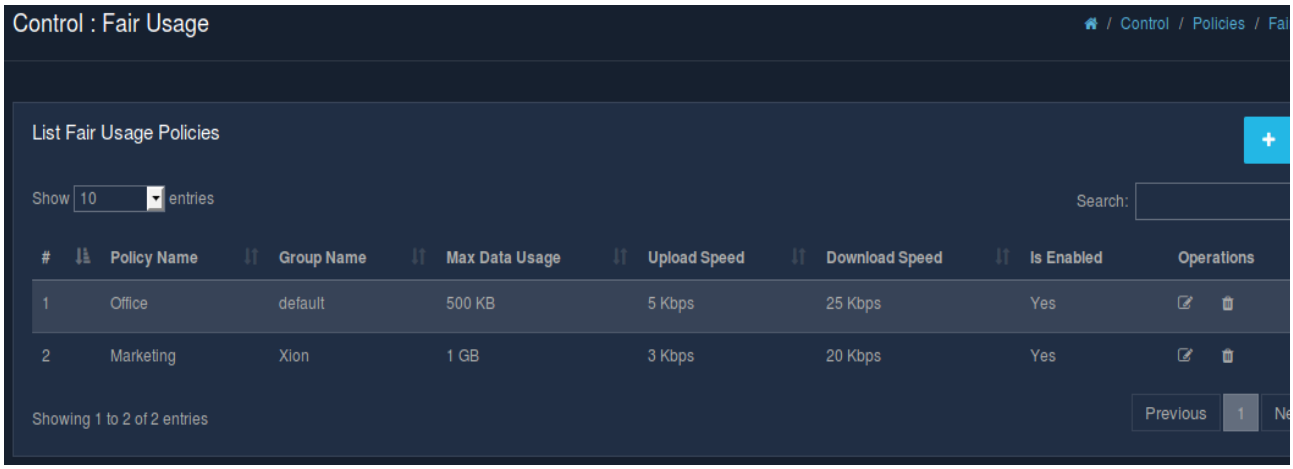
Table

Once the form is filled with all the required details, click the 'Save' button.

5.1.4.2 List Fair Usage Policy

An admin can view all the fair usage policies defined in the UniBox. The fair usage policy is a run-time policy i.e., the restrictions are applied to a user's session while the session is still in progress. This, in a way, helps the admin to curtail the bandwidth usage of heavy internet users, thus enforcing a fair usage policy on the network.

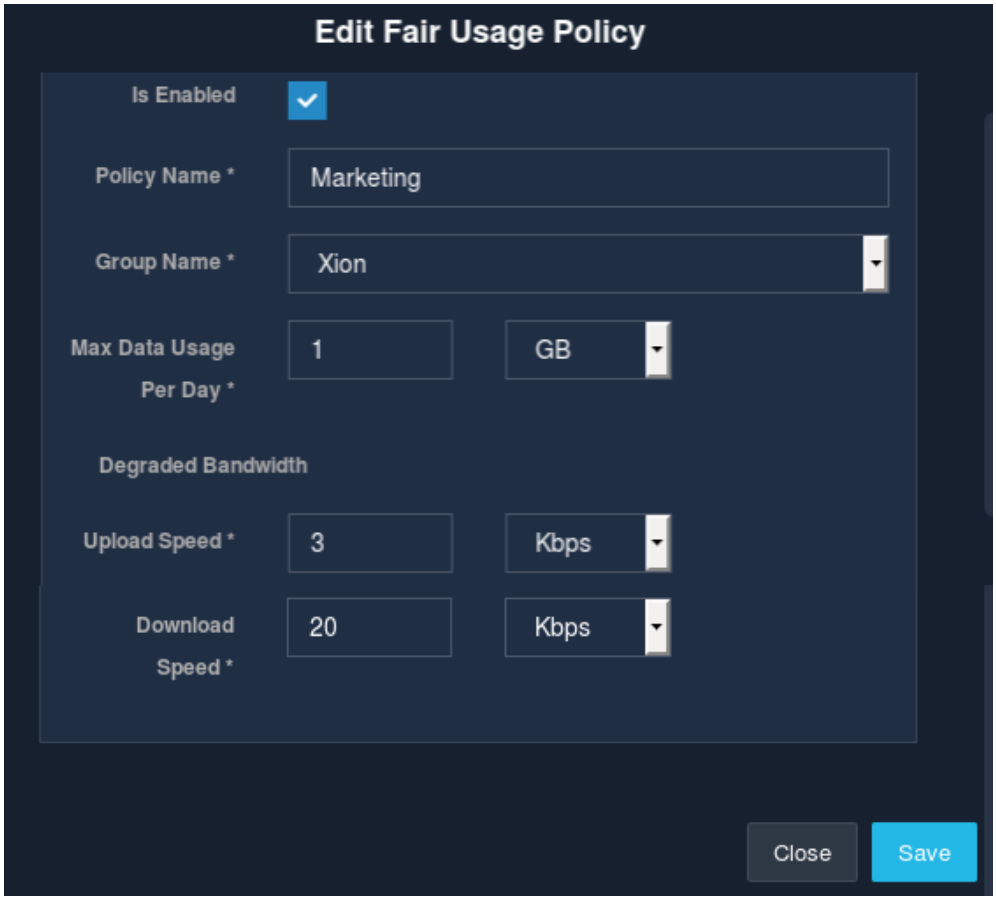
To see the list of the defined policies, select the 'Fair Usage' section in the 'Policies' sub-module under the 'Control' module. The list displays the policy name along with the group name, max data used, upload/download speed, whether enabled or not and also the 'Operations' column.



Fig

5.1.4.3 Edit Fair Usage Policy

An admin is provided the feature to edit and make changes to the already existing policies. To edit the existing policies, click on the edit icon in the 'Operations' column present in the 'Fair Usage' section in the 'Policies' sub-module under the 'Control' module. On clicking, a window appears displaying a form required to make changes to an existing policy.

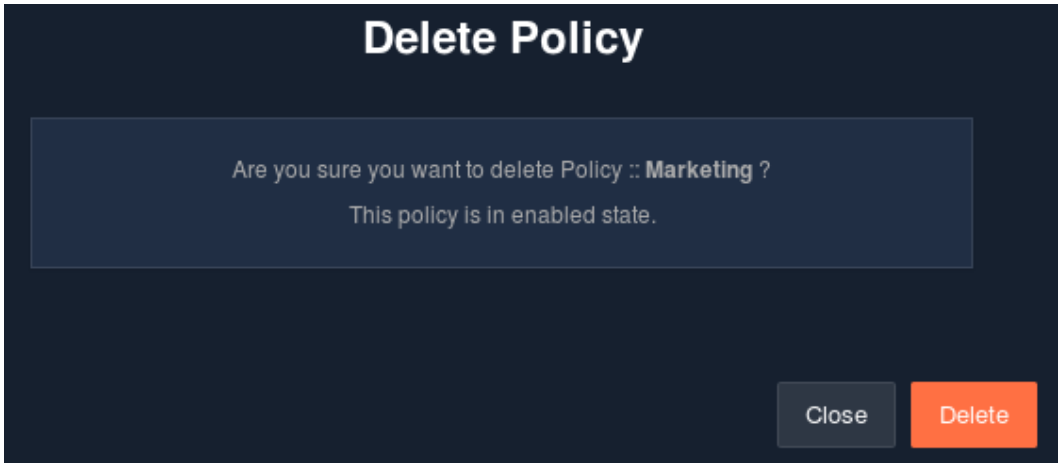


Fig

Once the necessary changes are made to the policy, click on the 'Save' button.

5.1.4.4 Delete Fair Usage Policy

Deleting a fair usage policy is fairly simple. Click on the delete icon in the 'Operations' column present in the 'Fair Usage' section under the 'Policies' sub-module. A message window appears to confirm the delete action.



Fig

Click on the 'Delete' button to surely delete it.

5.2 Content Filter

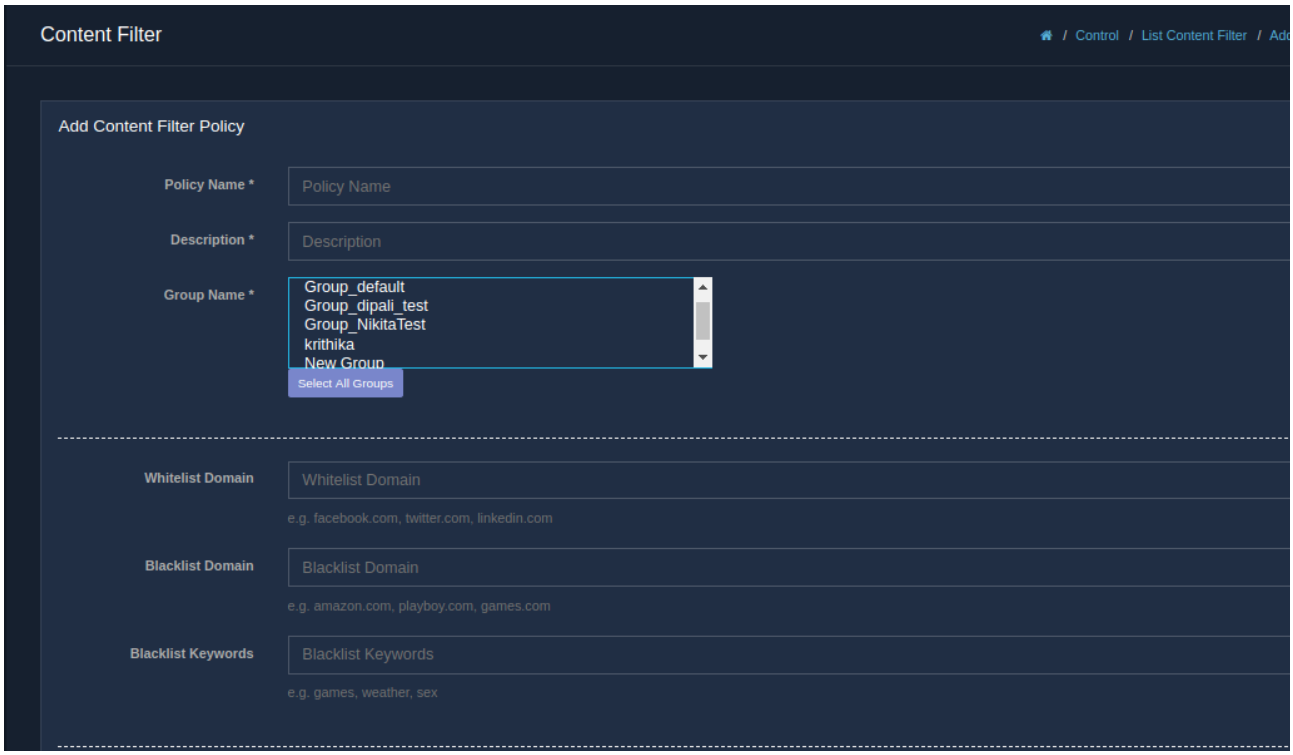
Content filtering is web filtering service offered by UniBox. It allows admin to enforce rules for filtering certain category of URLs from the users. The URLs are clubbed into different categories so the admin doesn't need to keep track of the whole database. Once the rules are applied, all the URLs listed in the given domain will be filtered.

In addition, the admin can also add or remove the domains from the categories.

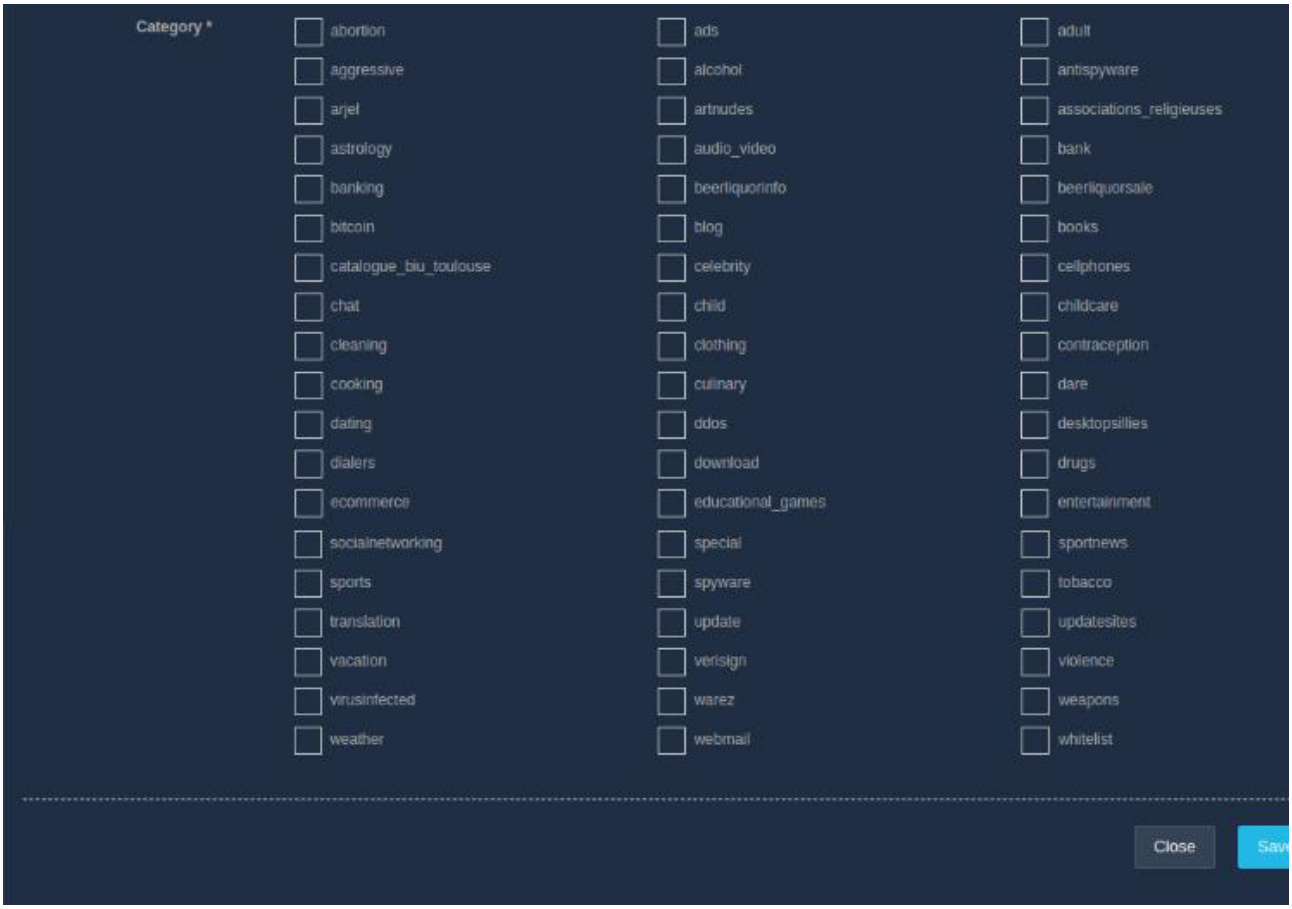
5.2.1 Creation

An admin can create a new group based on content filter policy. This allows the admin to define the domains that should be blocked by the content filtering service. UniBox maintains a database of domains or URLs that belong to each category. When the user tries to access the domain, UniBox checks if the domain is in the blocked list and will block the user access. The user is redirected to a blocked page.

To create a new group, go to the 'Control' module followed by the 'Content Filter' section. Then, click '**+**' icon where a page displays a form required to collect the information necessary to create a group.



Fig



Fig

Fields	***Description***
Policy Name	A unique name for the group policy.
Description	Give a brief description about the policy.
Group Name	Select the user group to which the policy will apply. All the user under the given group will be affected by this policy.
Whitelist Domain	Domain names of the Whitelist URL. Enter comma separated multiple domain names which need to be allowed access. Whitelisting will allow admin to specify exceptions to the given list of URLs. Domain name like facebook.com
Blacklist Domain	Domain name of the Blacklist URL. Enter comma separated multiple domain names which need to be blocked. Blacklisted domains will be filtered even if they don't belong to the category.
Blacklist Keywords	Enter the list of keywords that will be blocked. UniBox will check for the keyword in the domain name and will block the website if the keyword exists in the domain name.

Category	Select the domains from the list that should be filtered. All websites that fall under these domains will be automatically blocked by the filter.

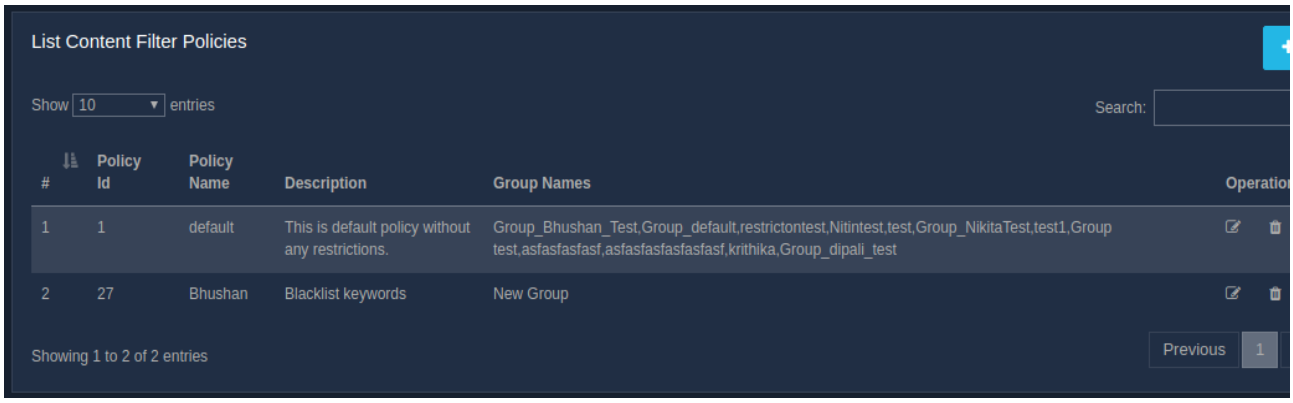
Table

Click on the ‘Save’ button to create new policy and apply the settings.

5.2.2 List Content Filter Policy

The list of all the content filter policies defined in the UniBox is displayed to an admin. The policies are listed in a table with policy name, policy id and description and group names. The policy will apply to all the groups defined in the rule.

To view the list, go to the ‘Content Filter’ section under the ‘Control’ module. Here, all the filtering policies are displayed.



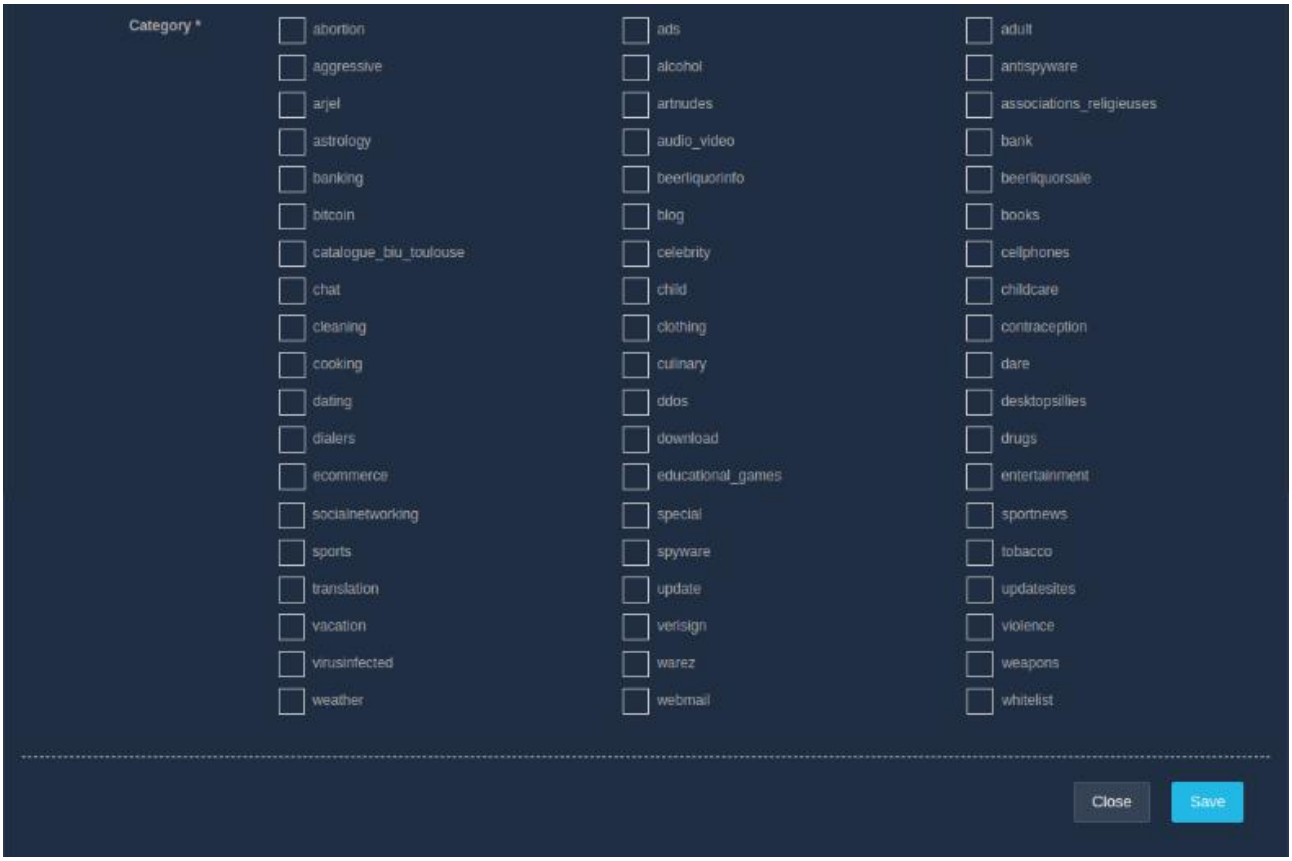
Fig

5.2.3 Edit Content Filter Policy

This facilitates an admin with the option to make changes to the content filter policies of user groups. To edit the existing policies, click on the edit icon in the ‘Operations’ column present in the ‘Content Filter’ section of the ‘Control’ module. A page displays a form which is required to make the changes to the policy.


Edit Content Filter Policy
Policy Name *
default
Description *
This is default policy without any restrictions.
Group Name *
asfasfasfasf
asfasfasfasfasf
Group test
Group_Bhushan_Test
Group_default
Select All Groups
Whitelist Domain
Whitelist Domain
e.g. facebook.com, twitter.com, linkedin.com
Blacklist Domain
Blacklist Domain
e.g. amazon.com, playboy.com, games.com
Blacklist Keywords
fb
e.g. games, weather, sex

Fig

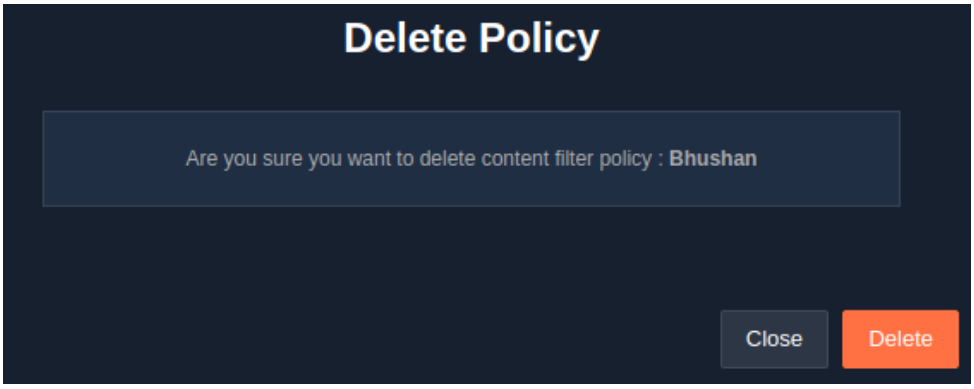

Category *
abortion
ads
adult
aggressive
alcohol
antispyware
arjel
artnudes
associations_religieuses
astrology
audio_video
bank
banking
beerliquorinfo
beerliquorsale
bitcoin
blog
books
catalogue_biu_toulouse
celebrity
cellphones
chat
child
childcare
cleaning
clothing
contraception
cooking
culinary
dare
dating
ddos
desktopsillies
dialers
download
drugs
ecommerce
educational_games
entertainment
socialnetworking
special
sportnews
sports
spyware
tobacco
translation
update
updatesites
vacation
verisign
violence
virusinfected
warez
weapons
weather
webmail
whitelist
Close
Save

Fig

When the required changes are made, click on the ‘Save’ button to update and apply the edited policy.

5.2.4 Delete Content Filter Policy

To delete a content filter policy, all an admin has to do is to click on the delete icon in the ‘Operations’ column present in the ‘Content Filter’ section of the ’Control’ module. A message window appears to confirm the delete action.



Fig

Click on the ‘Delete’ button to surely delete the policy.

6. Billing

This section allows admin to configure various billing related settings in Unibox. UniBox provides a complete set of billing features such as credit card clearing, prepaid vouchers, PMS integration and more.

6.1 Plans

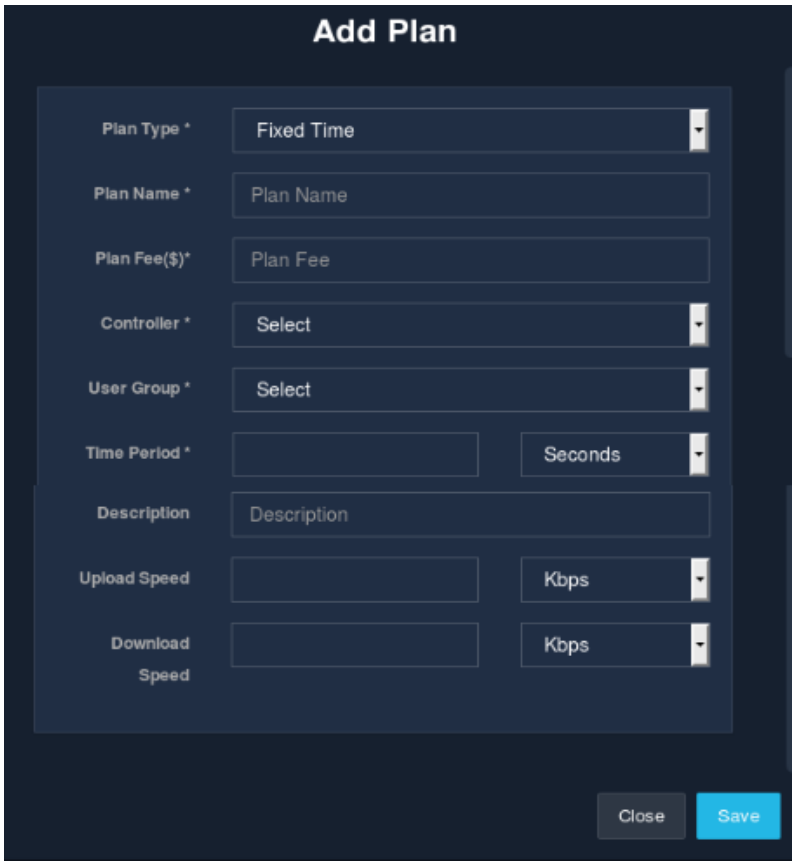
Unibox allows administrators to create a new billing plan. A billing plan defines how much the user pays for using the Internet service. This page displays the list of all billing plans defined in the system. Each plan is displayed in a tabular format with name of plan, plan fee, Type of plan, plan creation date. There are 3 types of plan:

- **Fixed Time:** This plan has a fixed time duration. The plan expires once the time period is reached irrespective of whether the user used the service.
- **Time Usage:** This plan has time usage limit. The plan expires once the given time is used up or the validity period is reached.
- **Bandwidth Usage:** This plan has bandwidth usage limit. The plan expires once the given bandwidth is used up or the validity period is reached.

6.1.1 Creation

Click on the '**+**' icon to create or add a new plan in the Unibox. A modal form will be displayed that collects the information required to create a new plan.

The fields marked with asterisk (*****) are mandatory.



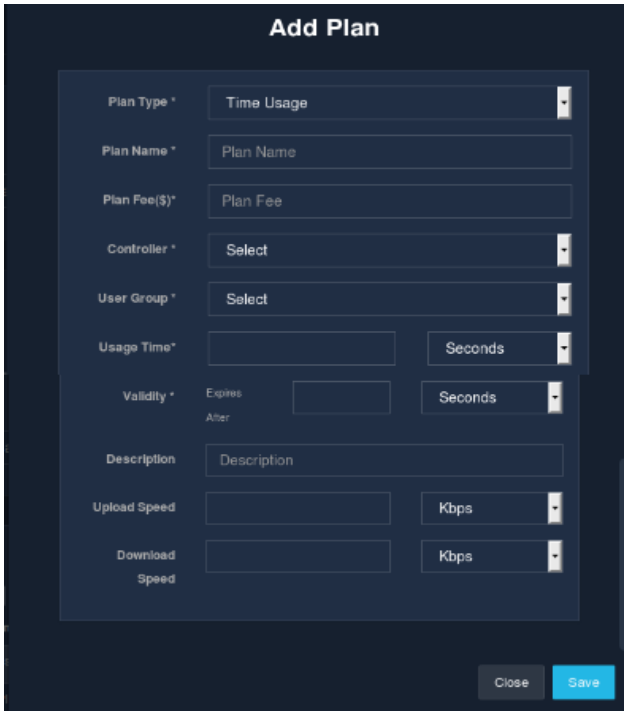
Fig

Fixed Time:

Fields	*Description*
Plan Type	Select Fixed Time from the **Plan Type** drop down menu.
Plan Name	Enter a unique name of the plan in the **Plan Name** field.
Plan Fee (USD)	Enter the fees in the **Plan Fee** field. (numbers only). The amount specified will be in the currency configured in UniBox profile.
Controller	Select the controller profile on which the given plan will be active.
User Group	Select a user group for the plan. Users signing up for this plan will be automatically signed to the user group.
Time Period	Enter the time in the **Time Period** field. Select the time duration in seconds, minutes, hours and days from the drop down menu
Description	Enter a short description of the plan in the **Description** field.
Upload Speed	Enter the upload speed to apply to the users who sign up with the given plan.
Download Speed	Enter the upload speed to apply to users who sign up with the given plan.

Table

Time Usage:



Fig

Fields	***Description***
Plan Type	Select Time Usage from the **Plan Type** drop down menu
Plan Name	Enter the name of the plan.
Plan Fee	Enter the fees in the **Plan Fee** field. (numbers only). The currency will be same as the one configured in the profile section.
Controller	Select the controller profile in which the plan will be active.
User Group	Select a user group for the plan. Users signing up for this plan will be automatically signed to the user group.
Usage Time	Enter the time in the **Usage Time** field. Select the time duration in seconds, minutes, hours and days from the drop down menu.
Validity	Enter the time of validity of the plan in the **Validity** field. Select the time duration in seconds, minutes, hours and days from the drop down menu.
Description	Enter a short description of the plan in the **Description** field.
Upload Speed	Enter the upload speed to apply to users who select this plan.
Download Speed	Enter the download speed to apply to the users who select this plan.

Table

Fig

Bandwidth Usage:

Fields	***Description***
Plan Type	Select Bandwidth Usage from the **Plan Type** drop down menu.
Plan Name	Enter the name of the plan
Plan Fee	Enter the fees in the **Plan Fee** field. (numbers only). The currency will be one that is configured in the profile section.
Controller	Select the controller profile in which the plan will be active.
User Group	Select a user group for the plan. Users signing up for this plan will be automatically signed to the user group.
Bandwidth Limit	Enter the bandwidth limit in the **Bandwidth Limit** field. Select the bandwidth limit in KB,MB,GB from the drop down menu.

Validity	Enter the time of validity of the plan in the **Validity** field. Select the bandwidth limit in KB,MB,GB from the drop down menu.
Description	Enter a short description of the plan in the **Description** field.
Upload Speed	Enter the upload speed to apply to users who select the plan.
Download Speed	Enter the download speed to apply to users who select this plan.

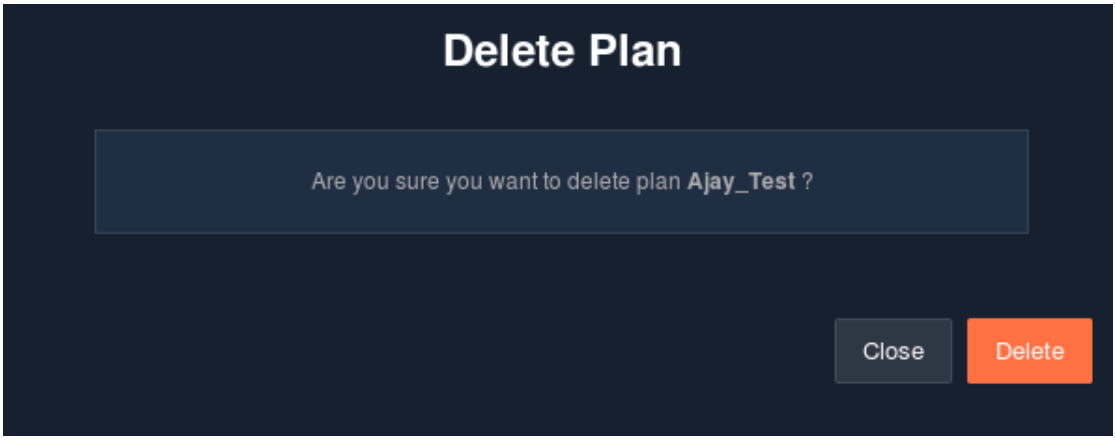
Table

Click on 'Save'. A new plan is added in the Unibox!

6.1.2 Delete Plan

This section allows administrators to delete an existing billing plan only if it is not associated with active users and portals. The administrator should then remove the plan from the portal page to which it is associated. If the plan is used on the paid portal, then the portal needs to be edited and saved again for the changes to take effect.

Click on the 'delete' icon, in the 'Operations' column, to delete an existing plan. Once clicked, a message asking for the confirmation of the delete operation pops up.



Fig

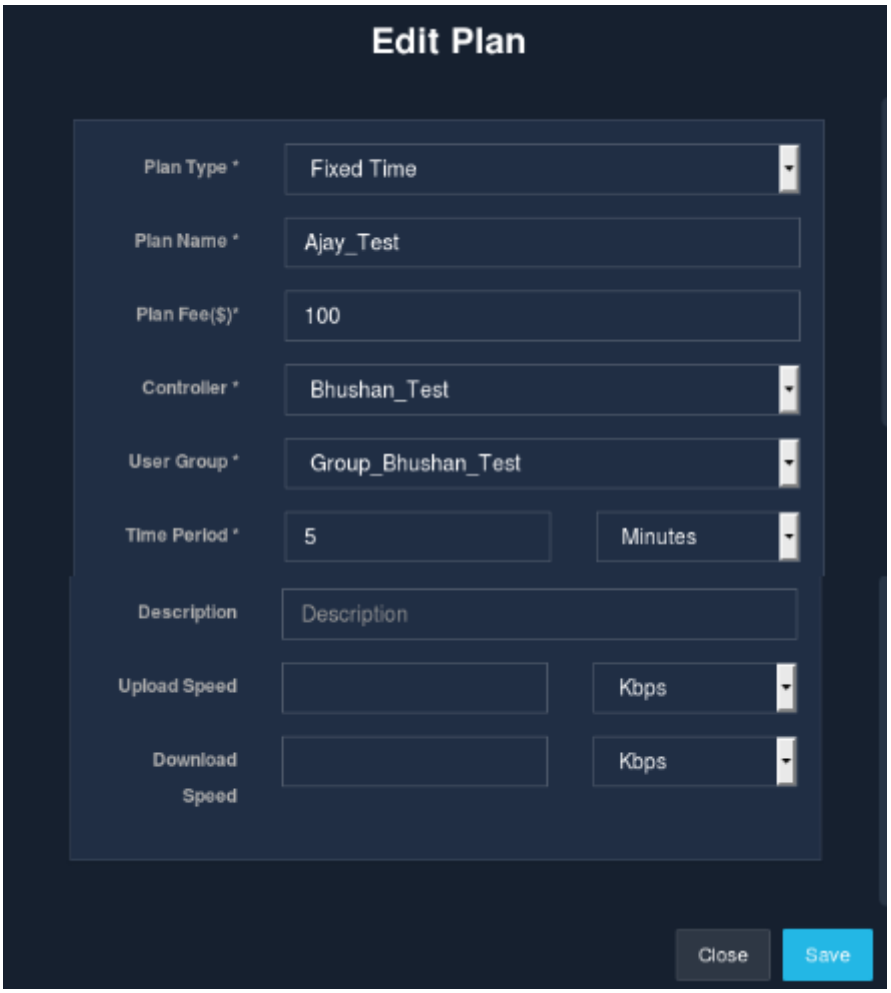
If you are sure, go ahead and click on the 'Delete' button.

6.1.3 Edit Plan

This page allows an administrator to change an existing plan information. Please note that any changes to the plan information will affect only the new users who sign-up after the changes are made. If the administrator has designed portal pages using the plan information, then he needs to recreate/update the portal page for the plan changes to take effect.

Like plan fee, the validity period changes will affect only new users. Existing users will still retain the old validity interval.

The 'Operations' column in the list allows an admin to make changes to a plan. To edit an existing plan, click on the edit icon. A modal dialog is displayed which then captures all the updated information. The changes made will be applied only when the changes are saved. Click on 'Save'.

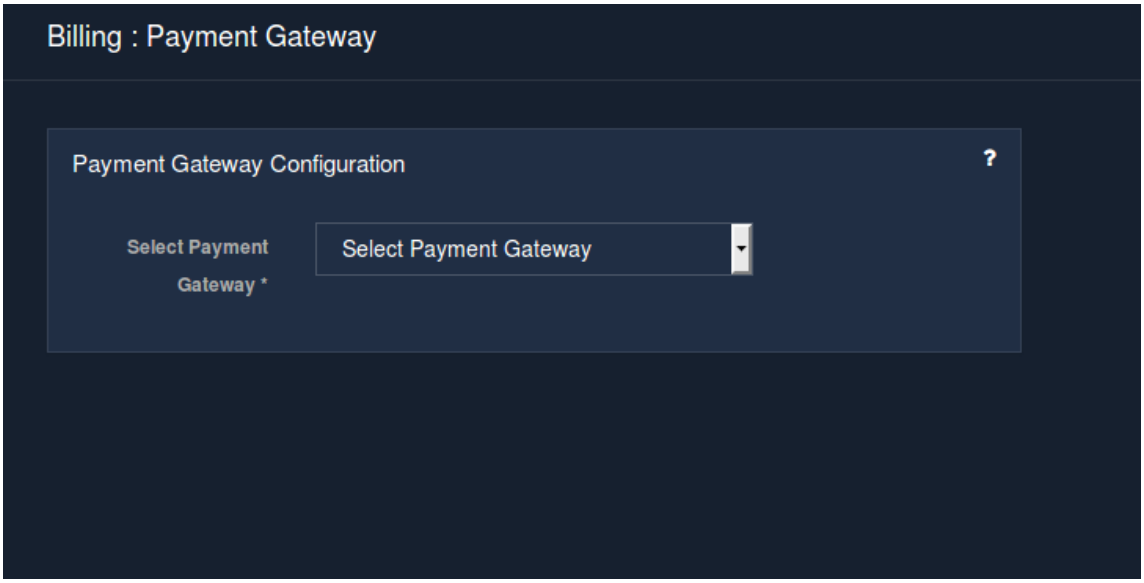

Edit Plan
Plan Type *
Fixed Time
Plan Name *
Ajay_Test
Plan Fee($)*
100
Controller *
Bhushan_Test
User Group *
Group_Bhushan_Test
Time Period *
5
Minutes
Description
Description
Upload Speed
Kbps
Download Speed
Kbps
Close
Save

Fig

6.2 Payment Gateway

Payment Gateway allows the administrator to define the payment gateway information for charging the customers using credit cards. The payment gateway is a third party service that provide credit card validation and clearing services. The payment gateway accepts the credit card details of the users and process the payment on them.

Click Payment Gateway (below Billing Configuration), Billing Payment Gateway page appears.

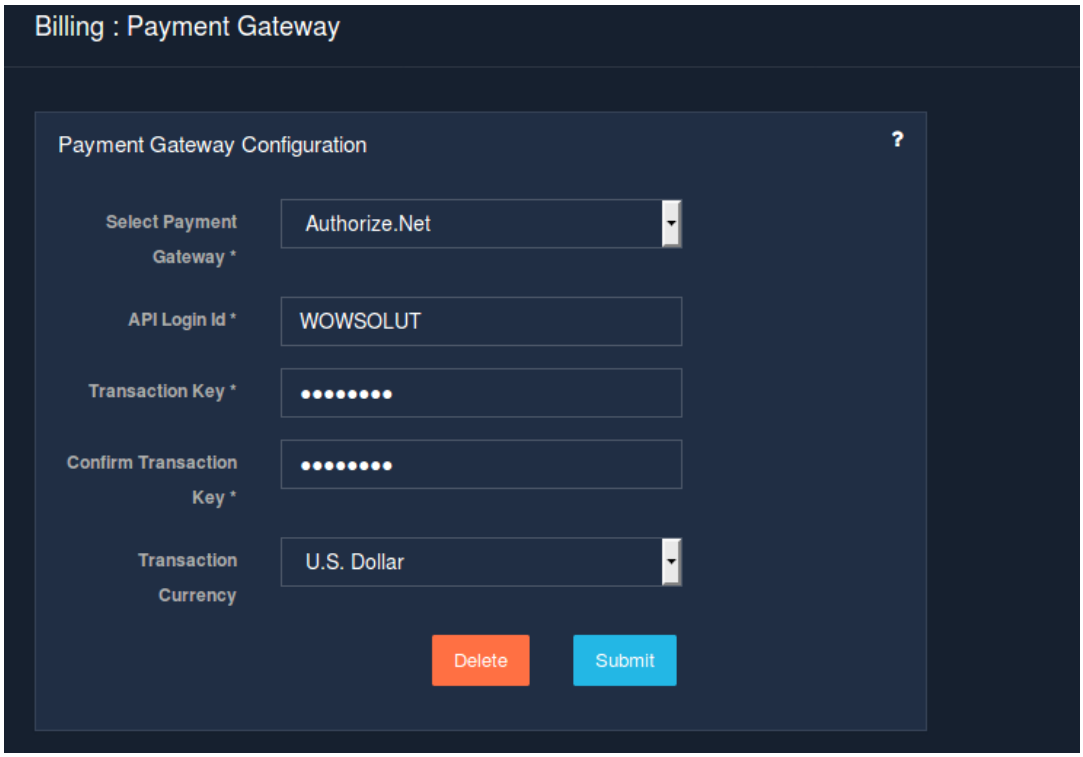


Fig

Currently, there are 4 types of payment gateways supported in UniBox:

- Authorize.Net
- PayPal.Std
- Instamojo
- PayUmoney

Authorize.Net

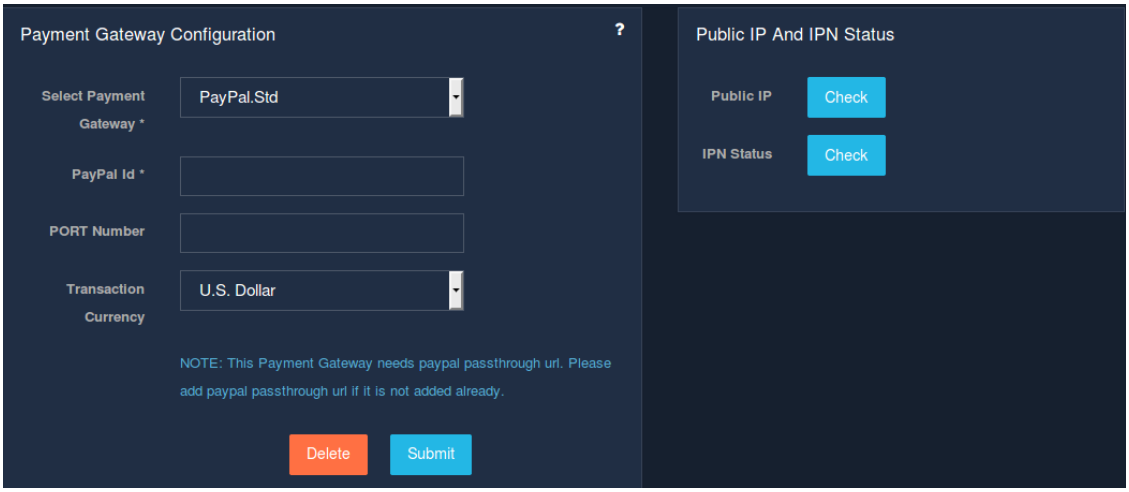


Fig

Fields	***Description***
Select Payment Gateway	Select **Authorize.Net** from the Select Payment Gateway drop down menu.
API Login Id	Specify the API Login ID.
Transaction Key	Specify the Transaction key.
Confirm Transaction Key	Confirm the Transaction key by specifying the same transaction key as above.
Transaction Currency	Specify transaction currency. If not selected, default will be U.S. Dollar.

Table

PayPal.Std:



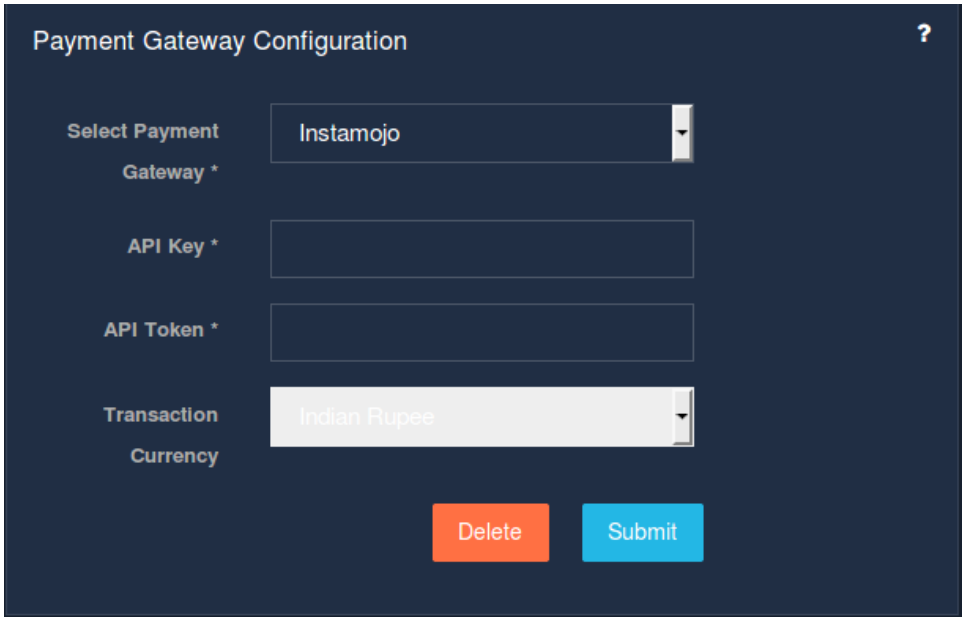
Fig

Fields	***Description***
Select Payment Gateway	Select **PayPal.Std** from the Select Payment Gateway drop down menu.
PayPal Id	Enter the PayPal id (email address) in the **PayPal ID** field.
PORT Number	Enter the PORT Number.
Transaction Currency	Select the transaction currency from the **Transaction Currency** drop down menu. The default currency is USA dollars.

Table

All the fields are mandatory, except for the port number and transaction currency.

Instamojo:

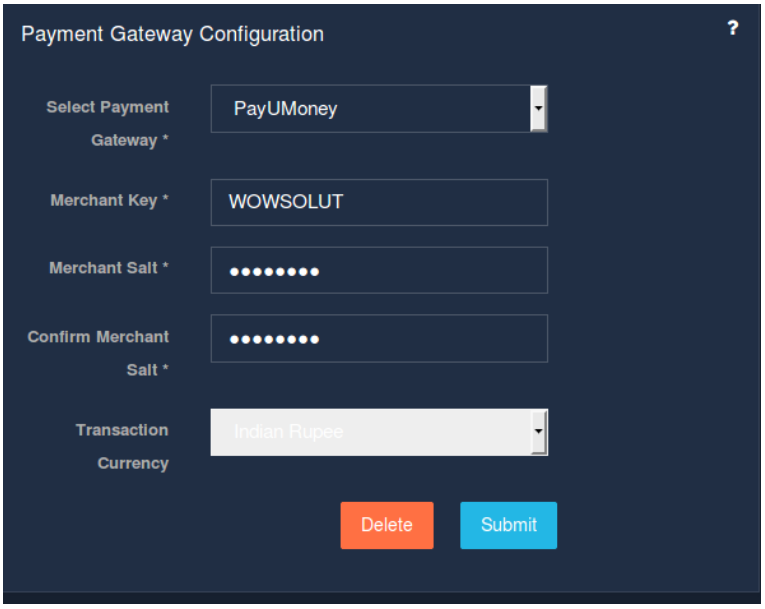


Fig

Fields	Description
API Key	Enter the API key.
API Token	Enter the API token.
Transaction Currency	Select the currency for transaction

Table

PayUMoney:



Fig

Fields	Description
Merchant Key	Enter the merchant key.
Merchant Salt	Enter the merchant salt.

Confirm Merchant Salt	Confirm the Merchant Salt by Specify the above Merchant Salt.
Transaction Currency	Select the transaction currency from the drop-down list

Table

Click on the 'Submit' button to save the payment configuration. If you want to delete the configuration, click on the 'Delete' button.

This page allows administrators to define the payment gateway. The admin will have to contact the respective company to get the payment gateway parameters. UniBox will only serve as an intermediary for processing the payments.

NOTE: UniBox doesn't save any credit card or other sensitive information. All the information is passed to the payment gateway for processing the payment. Since UniBox doesn't save any card information and processes all the transactions over 256-bit SSL certificate, it is PCI-DSS compliant.

NOTE: For Instamojo and PayUMoney Payement Gateway you need templogin user. Please create a templogin user with username as 'templogin' and password as 'templogin123' if it is not created already.

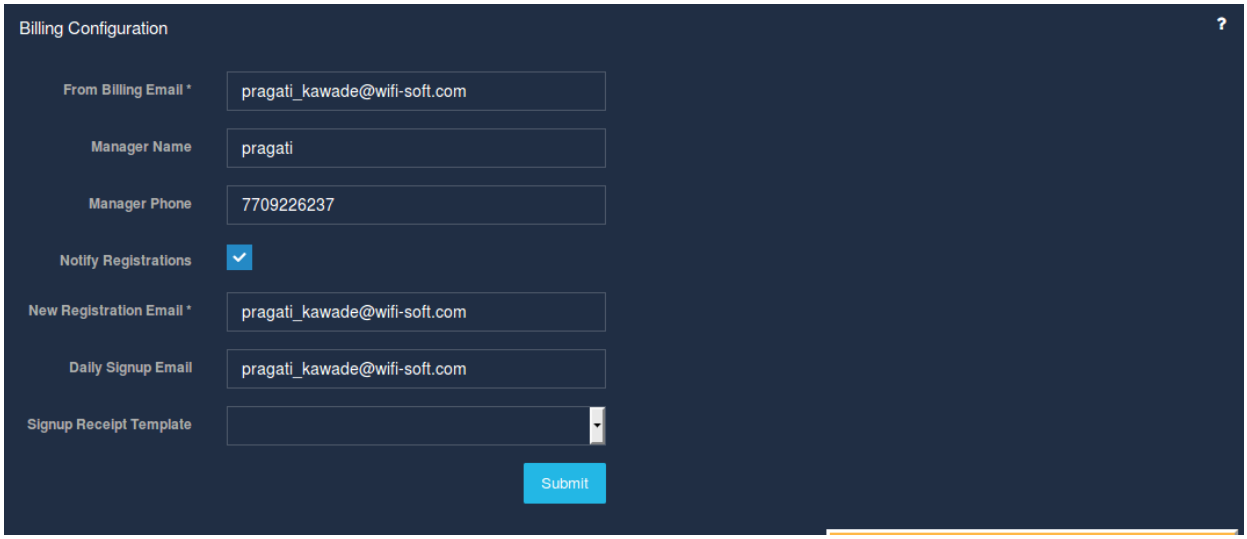
6.3 Billing Configuration

This page allows administrators to setup configuration for billing module. If the Notify Registration option is checked, then the given email addresses will receive an email notification when a new user signs up.

Fields	*Description*
From Billing Email	Enter a valid email address in **From Billing Email** field in which newly registered user will receive emails.
Manager Name	Enter the name in the **Manager Name** field.
Manager Phone	Enter phone number in the **Manager Phone** field.
Notify Registrations	Select the **Notify Registrations** check box to enable **New Registrations Emails** field. Enable this field to send registration notifications.
New Registration Email	Enter an email address which will receive the registration confirmation email in the **New Registration Emails** field. The email addresses will be notified of the new registrations
Daily Signup Emails	Enter an email address which will receive summary email of daily registrations in the **Daily Signup Emails** field. The email addresses will receive daily email from UniBox with the new signups.
Signup Receipt Template	Select an email template from the **Signup Receipt Template** drop down menu for sending new registrations/Signup emails.

Table

Mandatory field : From Billing Email, New Registration Email.



Fig

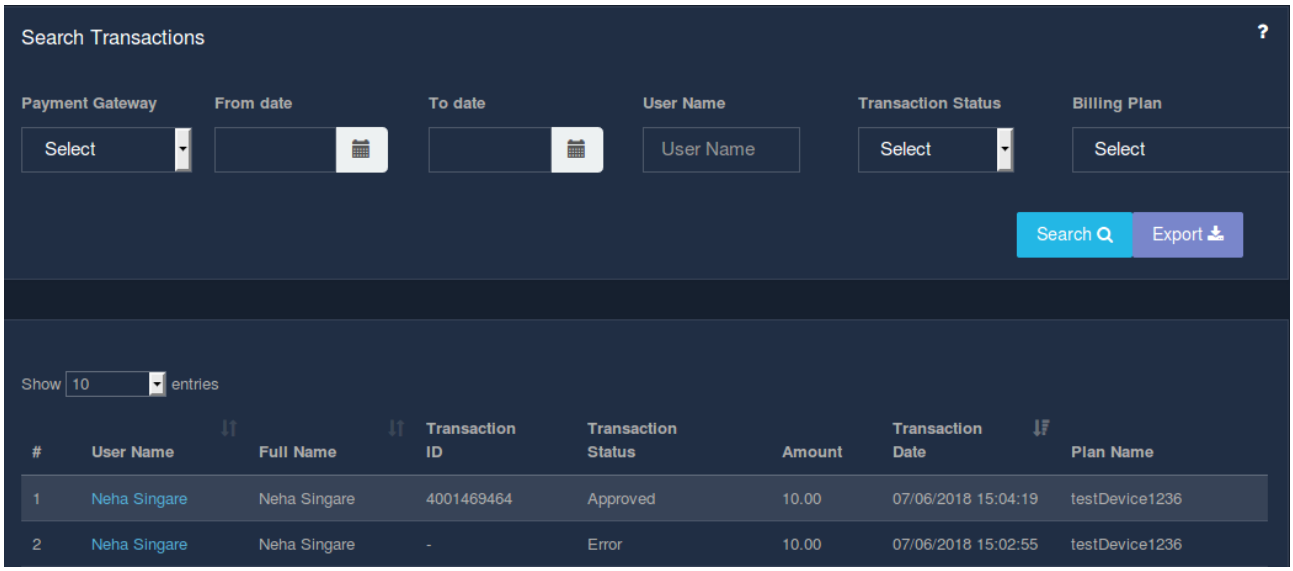
Click on the 'Submit' button to save the above entered details.

6.4 Transactions

6.4.1 List Transactions

This section displays all the billing (online payment) transactions in reverse chronological order. The transactions are logged whenever the user attempts to sign up for the paid service online. Unibox logs all (successful and failed) attempts.

Each entry displays the full name of the user, Username, Transaction ID, the status of the transaction, amount and the date of the transaction. The administrator can search for the given transaction using the search options.



Fig

6.4.2 Export:

This page allows an administrator to export the transaction records for the given time interval. The transactions are exported in Excel (CSV) format. Each row in the csv file contains the name of the user, transaction ID, amount, date of the transaction, status of the transaction and Plan of the User.

In order to export a file, click on the 'Export' button provided.

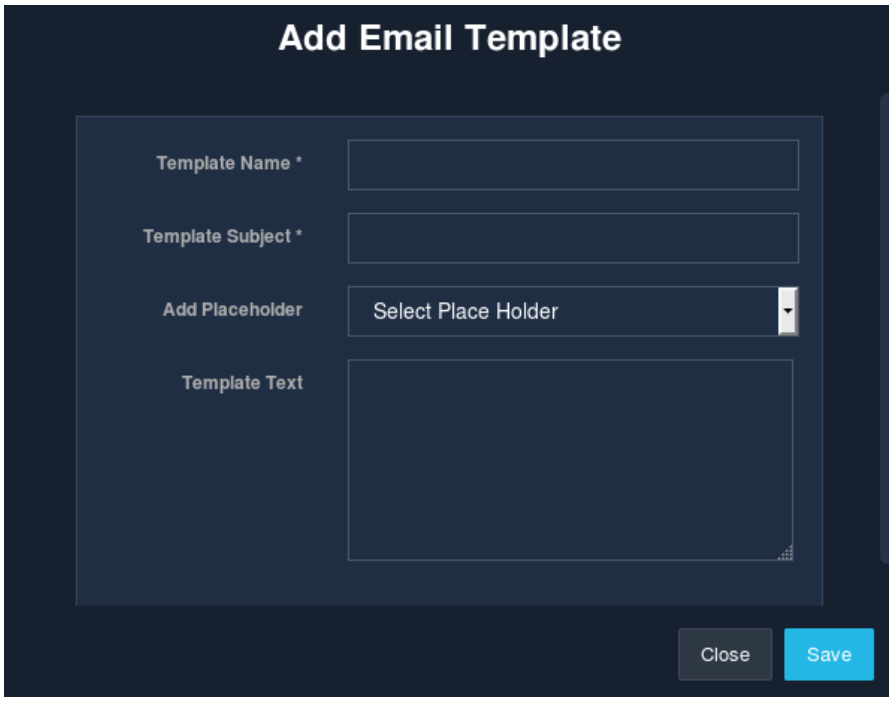
A csv file gets downloaded than.

6.5 Email Template

Unibox allows administrator to define a new email template. An email template will be used to send canned emails to the users who sign up or renew the service.

Predefined placeholders can be inserted in the template text to customize the email. Unibox will automatically insert the customer information in the placeholder while sending the email.

6.5.1 Creation



Fig

Fields	*Description*
Template Name	Enter the name of the email template in the **Template Name** field.
Template Subject	Enter the subject of the email in the **Template Subject** field.
Place Holder	Select the placeholder to insert in the email text from the **Place Holder** drop down menu. Place holders will be replaced with the actual values when the email is sent.

Template Text	Enter the email message in the **Template Text** field.

Table

Once the form is filled, click on the ‘Save’ button and a new email template would be created.

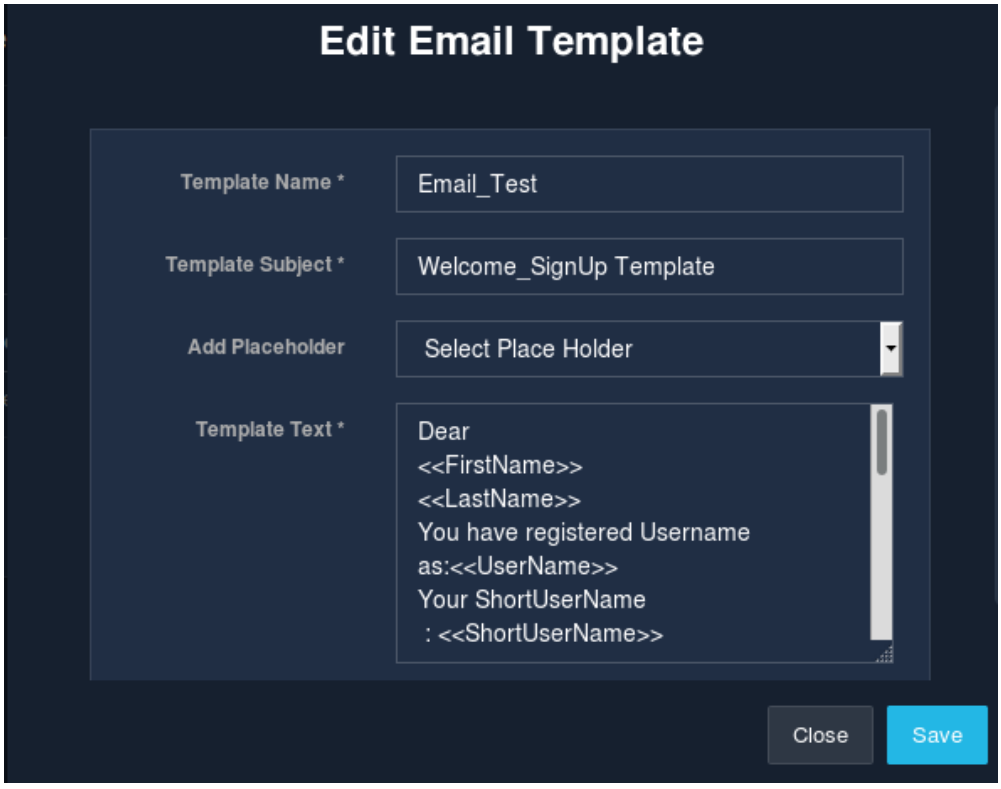
6.5.2 List Email Template

This section displays the list of email templates defined in Unibox. Placeholders are special strings that are replaced with the actual value before the email is composed. For example <<>> placeholder will be replaced with the first name of the user.

6.5.3 Edit Email Template

This section allows an administrator to edit an existing email template.

The ‘Operations’ column in the list allows an admin to make changes to an email template. To edit an existing email template, click on the edit icon. A modal dialog is displayed which then captures all the updated information. The changes made will be applied only when the changes are saved. Click on ’Save’.

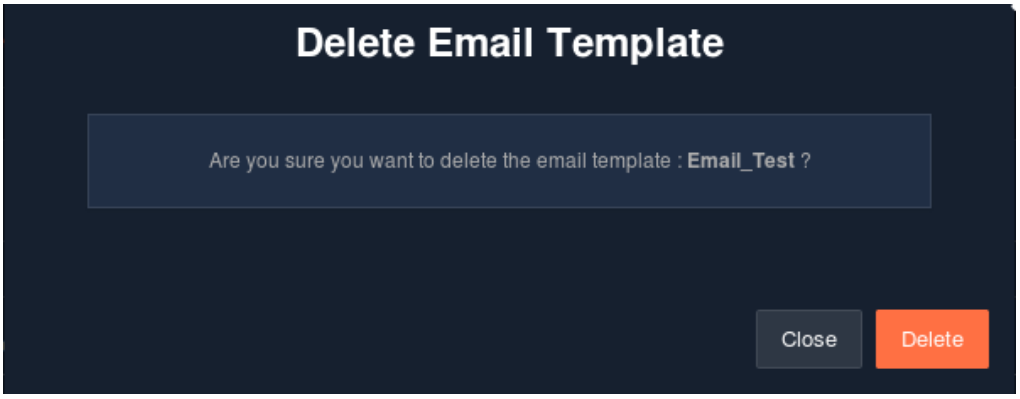


Fig

6.5.4 Delete Email Template

This page allows an administrator to delete an existing email template. If the template is in use, the administrator needs to configure Unibox to use another template.

Click on the ‘delete’ icon, in the ‘Operations’ column, to delete an existing email template. Once clicked, a message asking for the confirmation of the delete operation pops up.



Fig

If you are sure, go ahead and click on the ‘Delete’ button.

6.6 Vouchers

Vouchers are special codes created for user authentication when username is not used. They are created in batches and distributed by a person to the end users. The end users are prompted to enter them on the captive portal. It may be possible that the vouchers may be clubbed together with other fields to enable more secure authentication.

The voucher section is sub-divided into two parts:

- Batches
- Design

6.6.1 Batches

Unibox allows the administrator to create new voucher batch of voucher codes. A batch can have 1 or more prepaid codes.

When you select a group for voucher batch, group constraints like control policy assigned to the group, if any, will also get applied to all voucher users under that batch.

The administrator can create two types of voucher codes -

- Time Based: Each code has time usage restrictions.
- Bandwidth Based: Each code has bandwidth quota restrictions.

For time-based codes, the administrator can specify them as fixed (continuous use) time or time (non-continuous use) usage. For bandwidth the administrator can assign a quota to each code and specify number of days within which the user must use the quota once activated.

All codes are activated when they are used for the first time.

In addition, the administrator can also assign upload/download rate limits, session limits and client limits for each code. The rate limits control the browsing speed for the users. The session limit controls how many times the user can login with the same code and the client limit control number of devices the user can use with the same code.

6.6.1.1 Creation

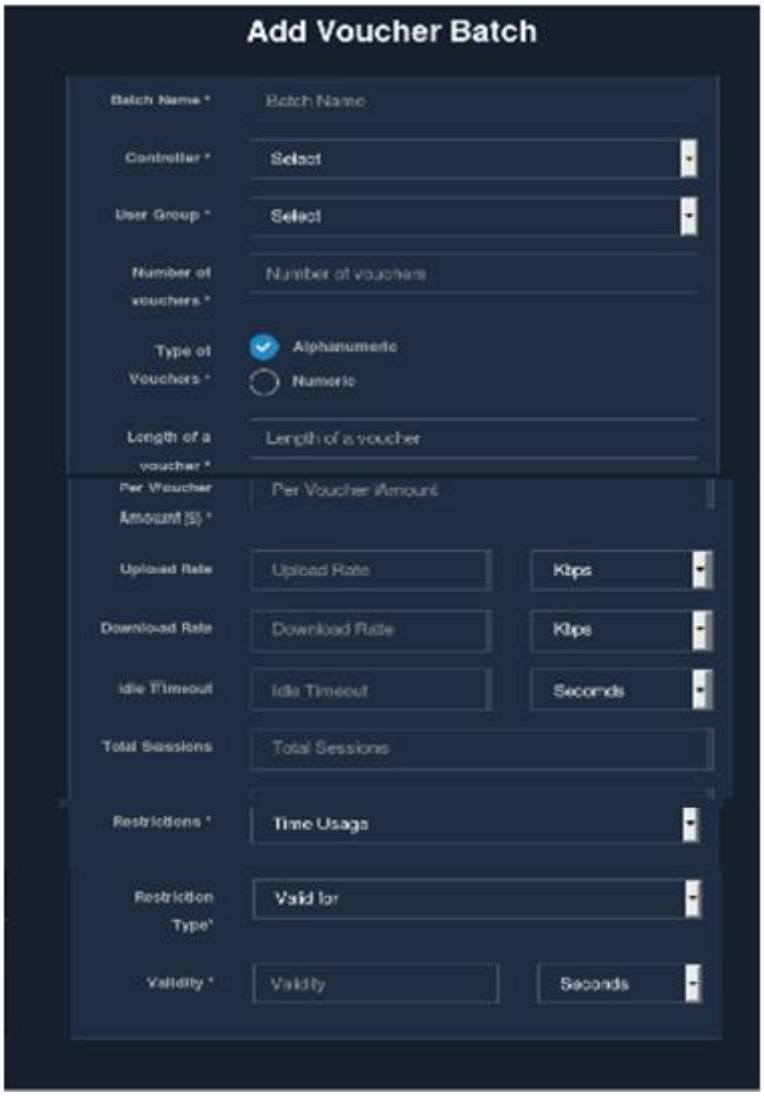
Fields	*Description*
Batch Name	Enter the **Name** of the voucher batch.
Controller	Select the **Controller** profile for the voucher batch.
User Group	Select the group for the batch from the **User Group** drop down menu. All vouchers will be assigned to the user group.
Number of Vouchers	Enter the number of codes to create in the voucher batch
Type of Vouchers	Select the **Type of Vouchers** (Alphanumeric/Numeric).
Length of a voucher	Enter the **Length of a voucher code.**
Per Voucher Amount	Enter the **Price** of each voucher code in the batch.
Upload Rate	Enter the maximum upload speed for the voucher code.

Download Rate	Enter the maximum download speed for the voucher codes in the **Download Speed** field.
Idle Timeout	Enter the time in **Idle Timeout field**. User sessions will be closed if it is idle for the given time
Total Sessions	Enter the maximum number of sessions allowed for the code in the **Sessions** field.
Max Device Limit	Enter the maximum number of devices who can use the code in the **Clients** field.
Restrictions	Select the Restriction type (Time Usage or Bandwidth Usage).

Table

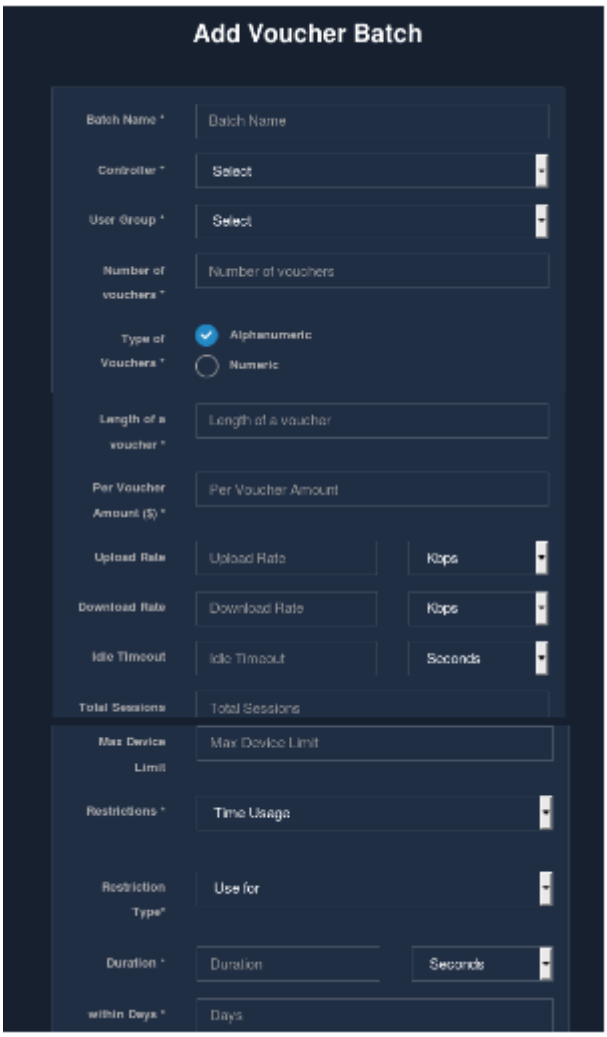
Based on the Restriction selected, the following fields would appear.

If the restriction selected is Time Usage and the restriction type is 'Valid for', then it looks something like this:



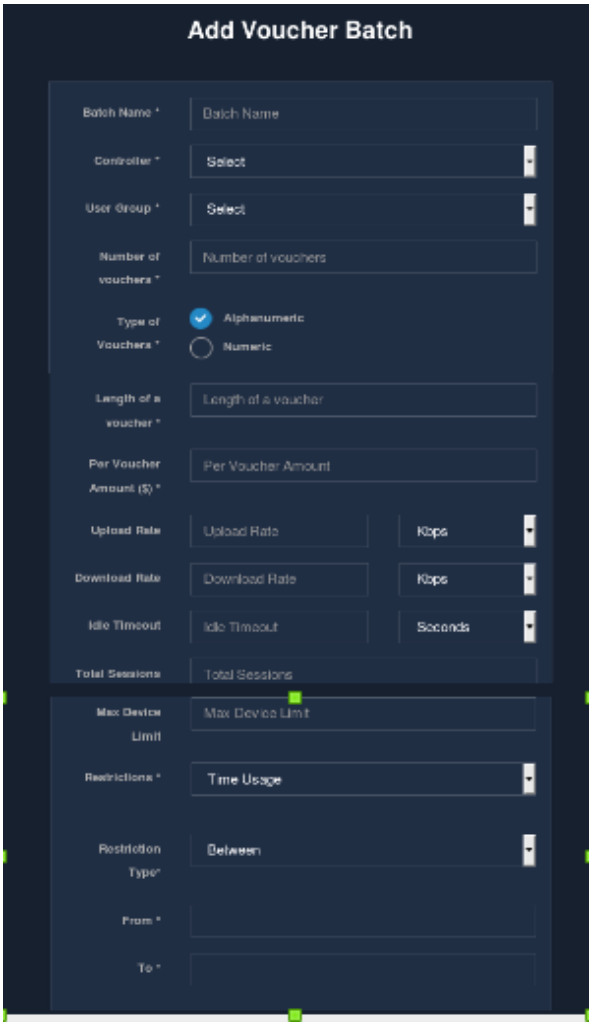
Fig

If the restriction selected is Time Usage and the restriction type is ‘Use for’ , then it looks something like this:


Add Voucher Batch
Batch Name *
Batch Name
Controller *
Select
User Group *
Select
Number of vouchers *
Number of vouchers
Type of Vouchers *
Alphanumeric
Numeric
Length of a voucher *
Length of a voucher
Per Voucher Amount ($) *
Per Voucher Amount
Upload Rate
Upload Rate
Kbps
Download Rate
Download Rate
Kbps
Idle Timeout
Idle Timeout
Seconds
Total Sessions
Total Sessions
Max Device Limit
Max Device Limit
Restrictions *
Time Usage
Restriction Type*
Use for
Duration *
Duration
Seconds
within Days *
Days

Fig

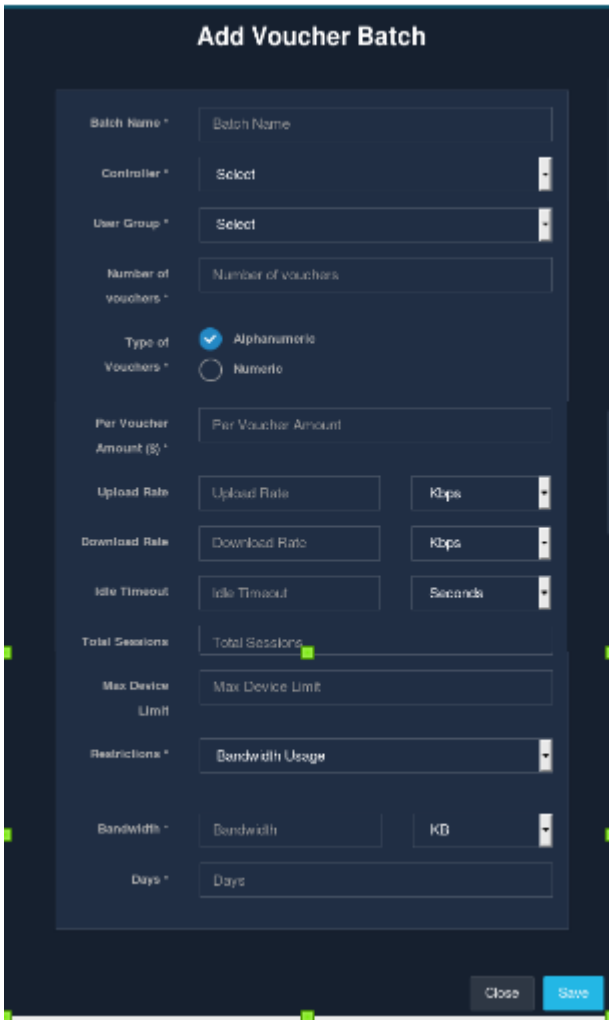
If the restriction selected is Time Usage and the restriction type is ‘Between’ , then it looks something like this:



Fig

Fields	***Description***
Valid for	Enter time duration for which the code is valid in the **Validity** field. Select the validity limit in seconds, minutes, hours and days.
Use For	Enter the total time for which the code can be used in the **Use for** field.
Between	Enter dates between which the codes are valid.

Table



Fig

If the restriction selected is Bandwidth Usage then following fields would appear:

Fields	***Description***
Bandwidth	Enter the **Bandwidth** limit for each voucher batch. Select the bandwidth limit in KB, MB and GB.
Days	Select the **Number of Days the restrictions will be valid.**

Table

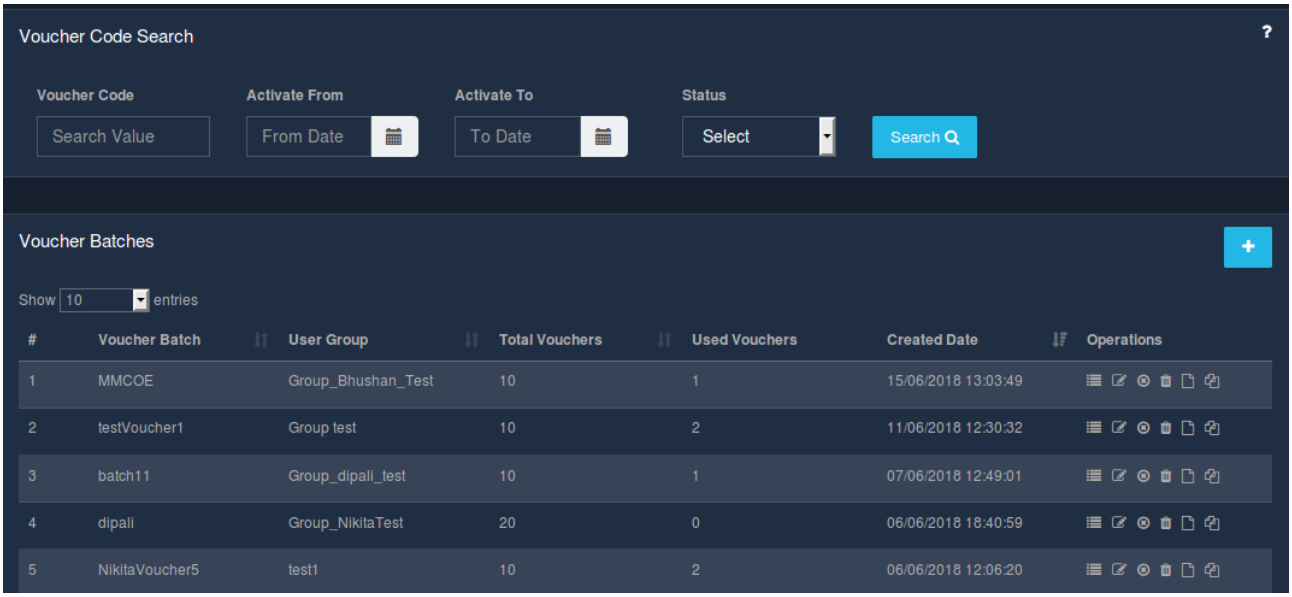
Click on the 'Save' button to save the voucher related data.

6.6.1.2 List Voucher Batches

This page displays the list of voucher batches defined in UniBox. Each batch is identified using a batch name. The tabular format displays the total number of voucher codes and the used Voucher Codes in each batch, a user group for the batch along with various operations.

It also allows you to search for particular codes by providing various search parameters like Voucher Code, Activate From date , Activate To Date or Status. Click on the 'Search' button once you have provided the desired search criteria and you will be displayed with the list of desired Voucher Batch Codes.

The list can be sorted in ascending or descending order using the icon on each column header.



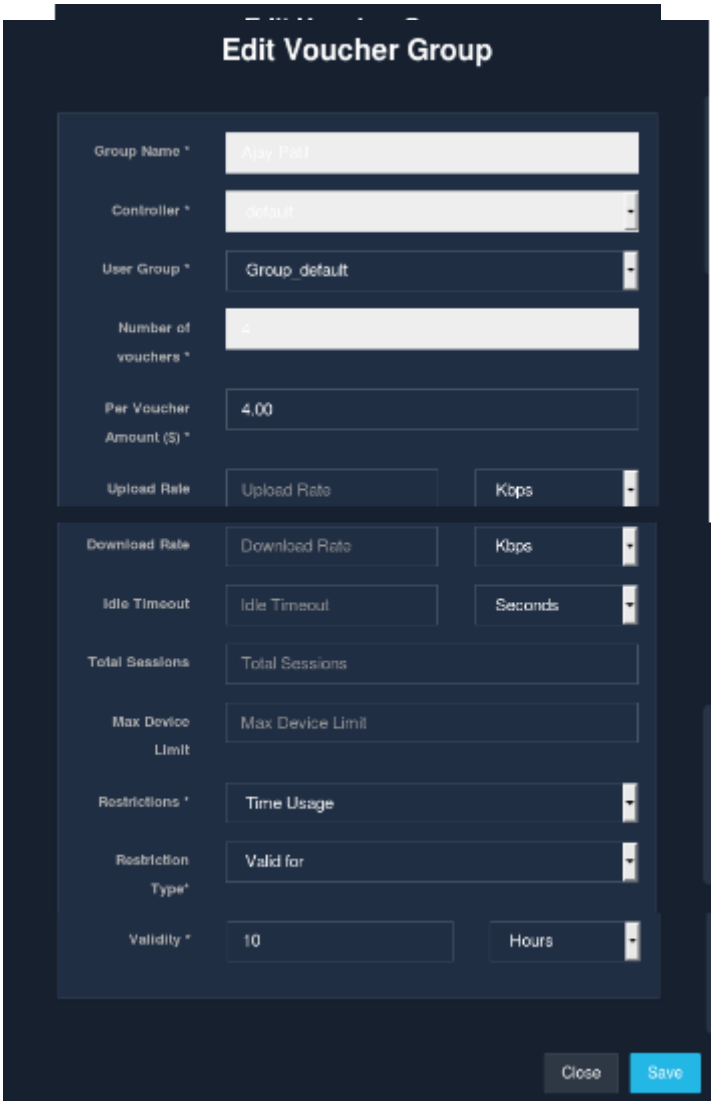
Fig

6.6.1.3 Edit Voucher Batch

This page allows the administrator to edit an existing voucher batch.

The admin can change the parameter like the name of the batch, user group, amount per voucher and the time and data restrictions. The other parameters can also be changed. The changes to the restrictions will apply to the vouchers which are unused.

In addition, the administrator can also change upload/download rate limits, session limits and client limits for each code. The option to edit a voucher's batch information can be found in the 'Operations' column. When the edit icon in the 'Operations' column is clicked, a modal is displayed which captures all the information. You cannot edit/change the group name, controller profile, number of vouchers, the restrictions implied and the restriction type. Once the changes are made, click on 'Save' to save the changes made.



Fig

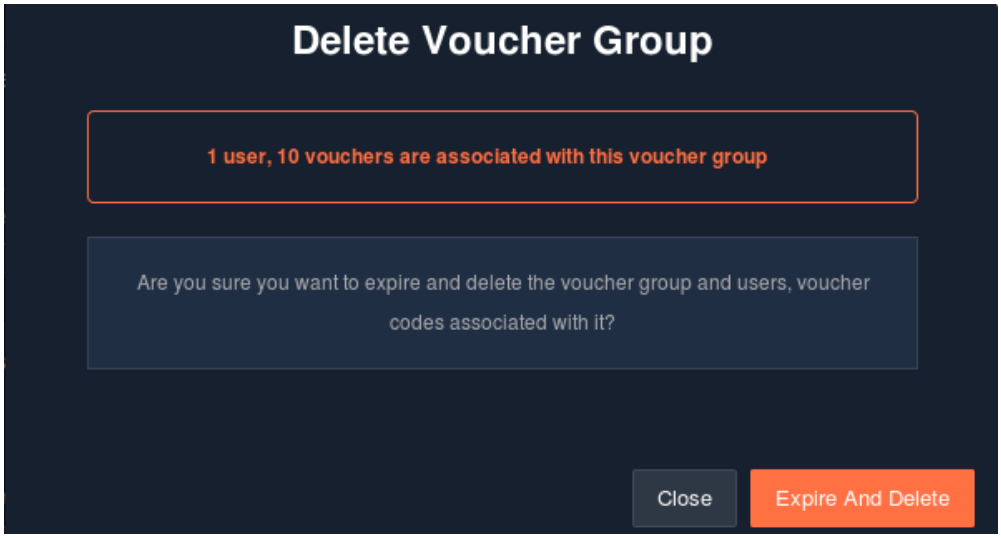
6.6.1.4 Delete Voucher Batch

For deleting the voucher button click on the delete button.

This section will allow admin to delete an existing voucher batch provided it is expired. **If the batch has voucher codes that are in use or have been used, then the batch can't be deleted.** It gives links to download batch report/record before deleting batch.

Deleting the batch will delete all the voucher codes defined in the batch.

To delete the voucher batch, click on the ‘Delete’ button in the ‘Operations’ section. A confirmation message pops up to confirm the delete action. Once sure, click on the ‘Delete’ button.



Fig

6.6.1.5 Export Voucher Batch

This section allows an administrator to export the batch of Voucher Codes for printing or distribution. All voucher codes in the batch (used, new or active) are included in the exported list.

The batch can be exported in two formats - Excel (CSV) or PDF.
In CSV format, the codes and batch information like time duration, bandwidth restrictions, etc, are exported as comma-separated values. The file can be imported into Excel for viewing or printing. The file can be easily emailed to other people for distribution.

In PDF format, each code is printed in business card format. Each code will have the company logo, name along with the code details. Administrator can customize the look for each code using the voucher defaults section.
The exported file is in print-ready format i.e. it can be easily printed on a A4 sized paper and each code can be cut for distribution.

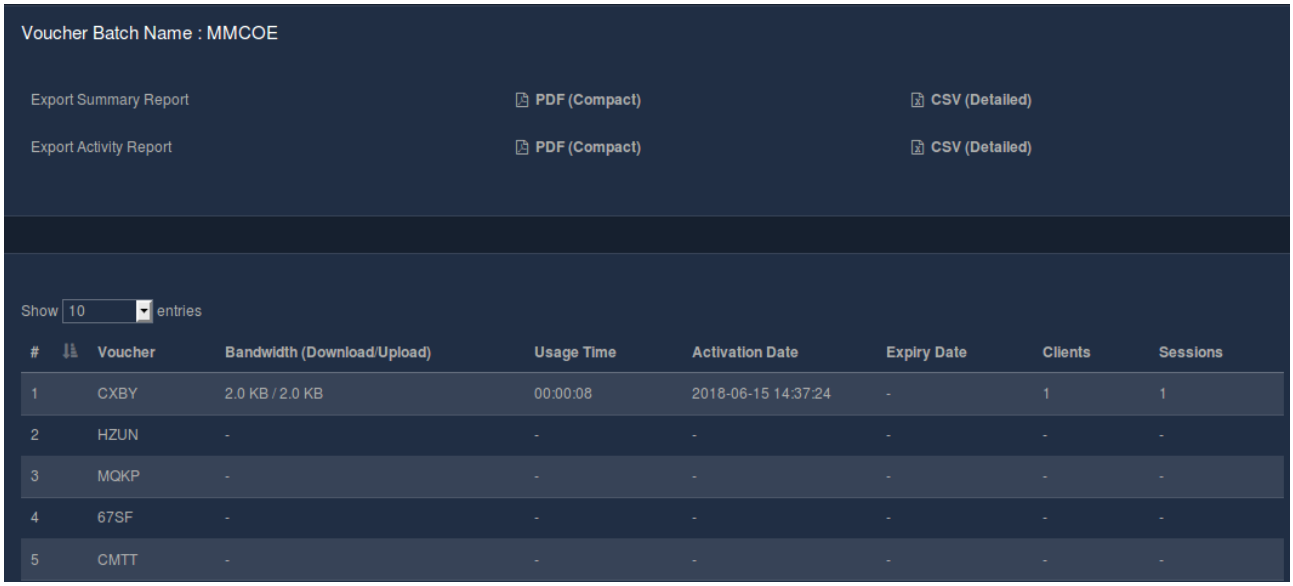
To export the voucher batch, click on the 'Export Voucher Group' button in the 'Operations' section. It than prompts you to select the required file type (csv or pdf).

Fig

6.6.1.6 Export Voucher Batch Report

This section allows an administrator to export individual voucher code report for accounting/auditing purpose. The code report is exported in PDF as well as CSV format.

To export the individual voucher batch, click on the 'Export Voucher Group Report' button in the 'Operations' section. It then allows you to choose between the two reports (Activity Report and Summary Report).



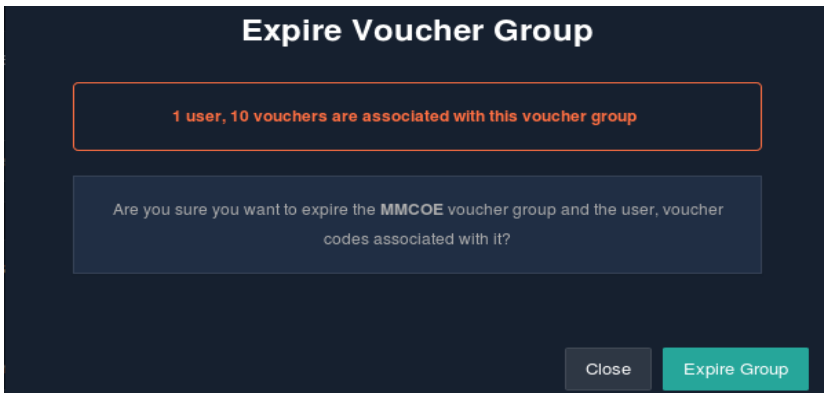
Fig

6.6.1.7 Expire Voucher Batch

It allows administrator to expire voucher batch. Before expiring voucher batch it will ask for confirmation and gives two options yes and no. If user clicks on 'Yes', then it expires batch and when clicks on 'No' it comes back to expire voucher batch page.

Expiring the batch will Expire all the voucher codes defined in the batch.

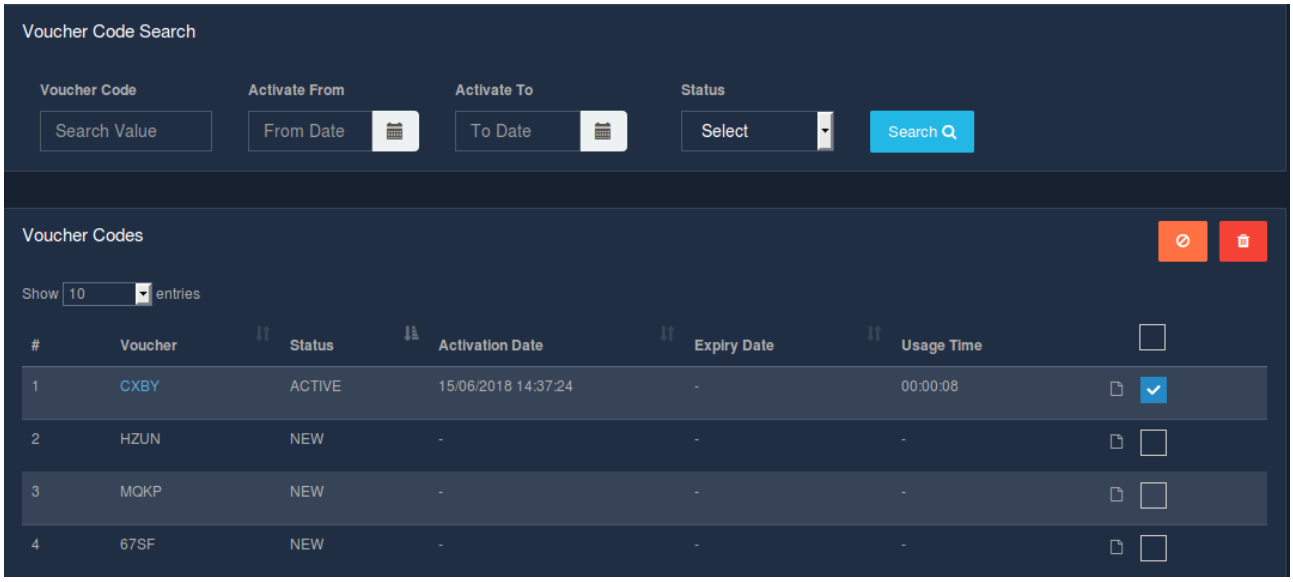
To expire the voucher batch, click on the 'Expire' button in the 'Operations' section. It than prompts you a confirmation message. As this option would expire both the batch as well as the voucher codes associated with it. Once sure, click on the 'Expire' button.



Fig

6.6.1.8 View the vouchers created

On the list voucher batch page, you can click on the first icon to view the list of codes created under this batch. This page displays all the details related to the voucher batch. It will display a tabular representation of the voucher, status, activation date, expiry date and time-usage. Click on the 'Vouchers' button in the 'Operations' section to view the voucher details. The Checking the checkbox corresponding to each entry enables you to either delete or expire the prepaid voucher.



Fig

6.6.2 Customize Voucher Design

Unibox allows an administrator to customize the look of the voucher card. The customization will be applied to each card printed from UNIBOX. The card can be printed in a PDF file.

This page allows an administrator to customize the look-and-feel of the voucher card. The voucher card is generated for each voucher code in the batch when the whole batch is exported in PDF format. The admin can upload the logo and background for the card. Each card will get the logo and background image.

The PDF cards will be laid out on an A4 size paper and each paper will hold 10 cards.

Fields	***Description***
Header	Enter a text for card header in the **Header** field. For example: Welcome to WiFi Hotspot
Footer	Enter a text for card header in the **Footer** field. E.g. WiFi provided by XYZ
Logo	Click **Browse**, and search and select an image for the card logo. Or click **Use Default** check box for the default logo.(Image should be in JPG or PNG format). Please make sure that you upload a transparent logo if you use a darker background.
Background	Click **Browse**, and search and select an image for the background. Or click **Use Default** check box for the default background. (Image should be in JPG or PNG format).

Table

Fig

If you don't want a customize voucher template, select the default option for logo and the background. This will then apply the default values for the logo and the background.

Click on the 'Submit' button to save the changes made to the voucher design.

6.7 PMS

PMS stands for Property Management System. This system is usually installed in hotels, resorts and other hospitality venues for managing the guest payment and services in the property. Since WiFi service is one of the important amenities in the hotel, it is important to interface the WiFi system with the PMS for centralized billing and verification of the guests.

Unibox interfaces with multiple PMS systems. You need to have the PMS module enabled to use this feature.

6.7.1 PMS Configuration

Unibox allows an administrator to setup PMS configuration. This configuration will establish communication of PMS Server with Unibox, and help processing sign up and login requests from Unibox portal. Click on the Enable Configuration checkbox to enable PMS configuration.

Select the type of PMS from the PMS Type drop down menu.

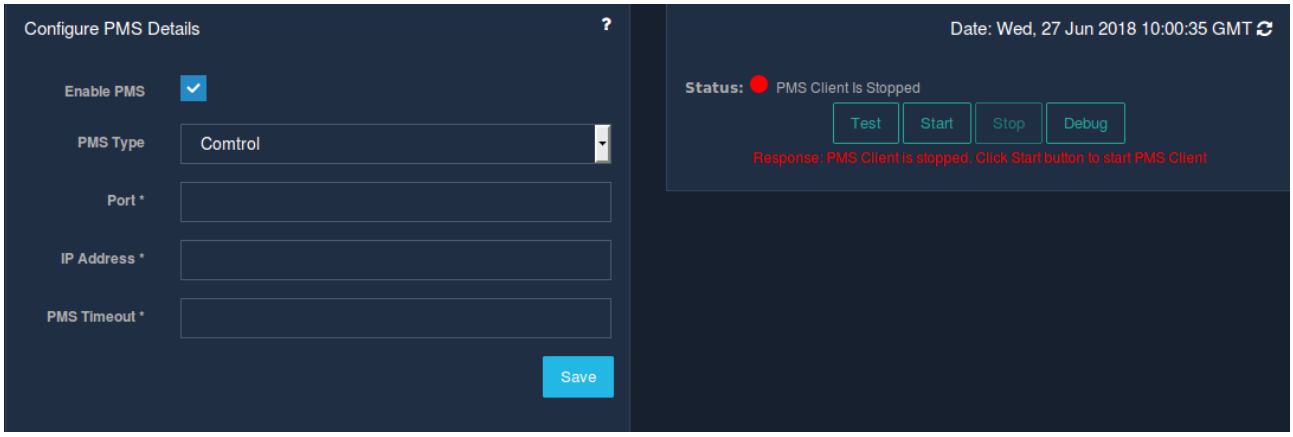
The options are:

- Comtrol
- Hotelier
- Hotsoft
- IDS Fortune
- IDS Fortune Serial
- Micros*
- WinHMS

- Lucid
- Virtual

***Need special certification.**

Comtrol:

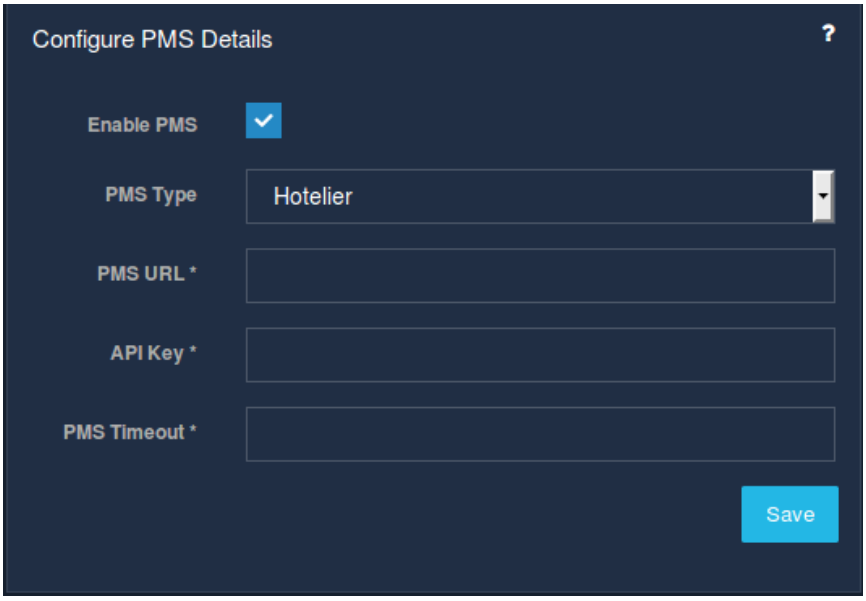


Fig

Fields	***Description***
PMS Type	Select **Comtrol** option from the **PMS Type** drop down menu.
IP Address	Enter the IP Address of the PMS server in the **IP Address** filed.
Port	Enter the port of PMS server in the **Port** field.
PMS Timeout	Enter the PMS timeout in seconds. (Recommended is 5 seconds)
Test PMS Connectivity	Click the **Check PMS** button in front of **Check PMS Connectivity** to check the PMS connectivity.

Table

Hotelier:

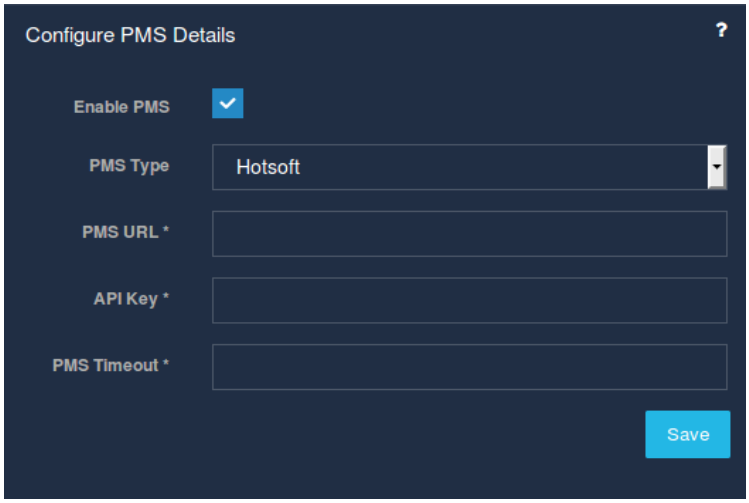


Fig

Fields	***Description***
PMS Type	Select **Hotelier** option from the **PMS Type** drop down menu.
PMS Url	Enter the PMS Url in the PMS Url field.
API Key	Enter the API key for the PMS in the **API Key** field.
PMS Timeout	Enter the PMS timeout in seconds in the **PMS Timeout** field. (Recommended is 5 seconds)

Table

Hotsoft:

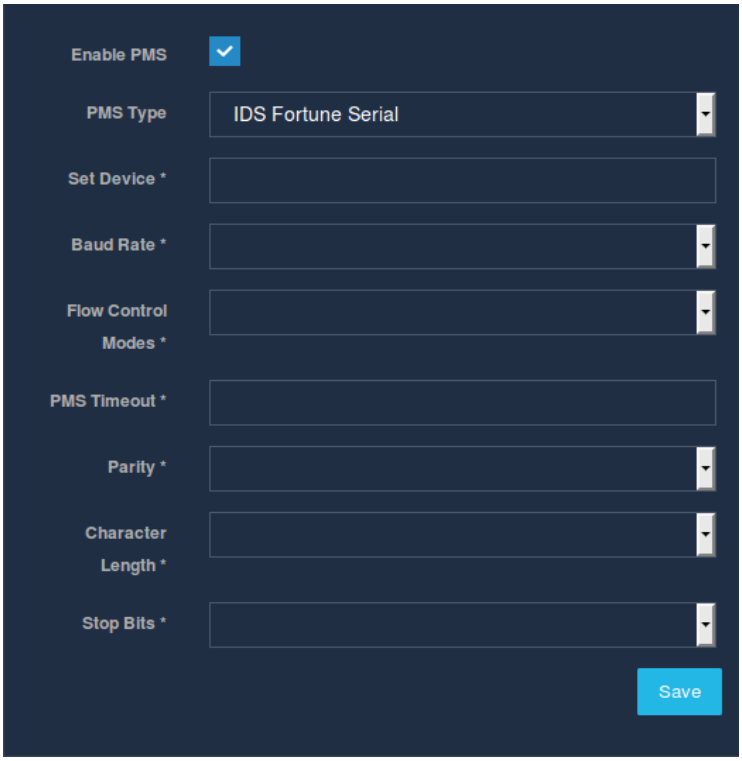


Fig

Fields	***Description***
PMS Type	Select the Hotsoft PMS type from the drop-down list.
PMS Url	Enter the PMS Url in the PMS Url field.
API Key	Enter the API key for the PMS in the **API Key** field.
PMS Timeout	Enter the PMS timeout in seconds in the **PMS Timeout** field. (Recommended is 5 seconds)

Table

IDS Fortune Serial:

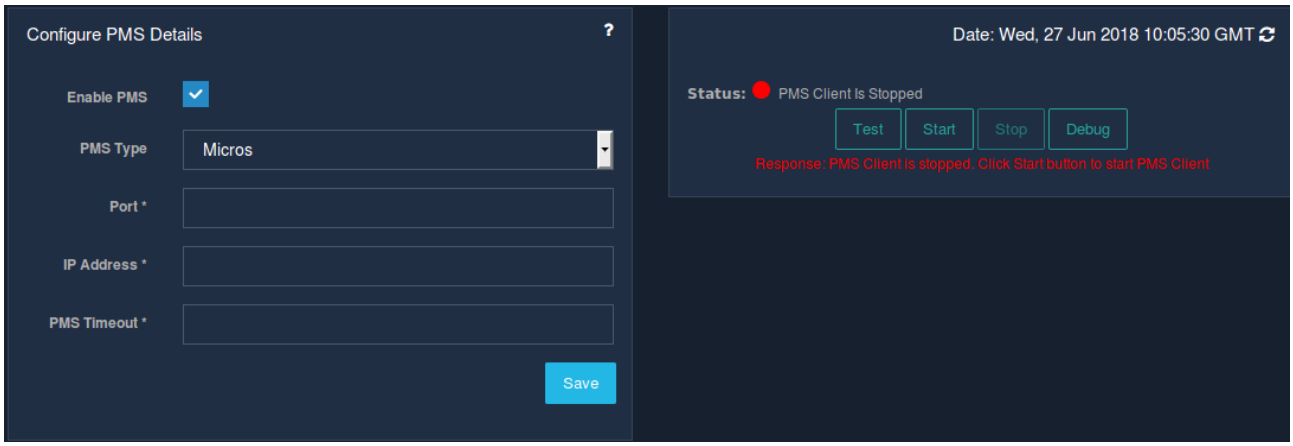


Fig

Fields	***Description***
PMS Type	Select **IDS Fortune Serial** option from the **PMS Type** drop down menu.
Set Device	Enter the device set for the PMS server in the **Set Device** field.
Baud Rate	Select the Baud rate for PMS server from the **Baud Rate** drop down menu.
Parity	Select the parity of the PMS server from the **Parity** drop down menu.
Character Length	Select the character length for PMS Server from the **Character Length** drop down menu.
Stop Bits	Select the stop bits for PMS server from the Stop Bits drop down menu.
Flow Control Modes	Select the flow control modes for PMS server from the **Flow Control Modes** drop down menu.
PMS Timeout	Enter the PMS timeout in seconds in the PMS Timeout Field. (Recommended is 5 seconds)

Table

Micros:

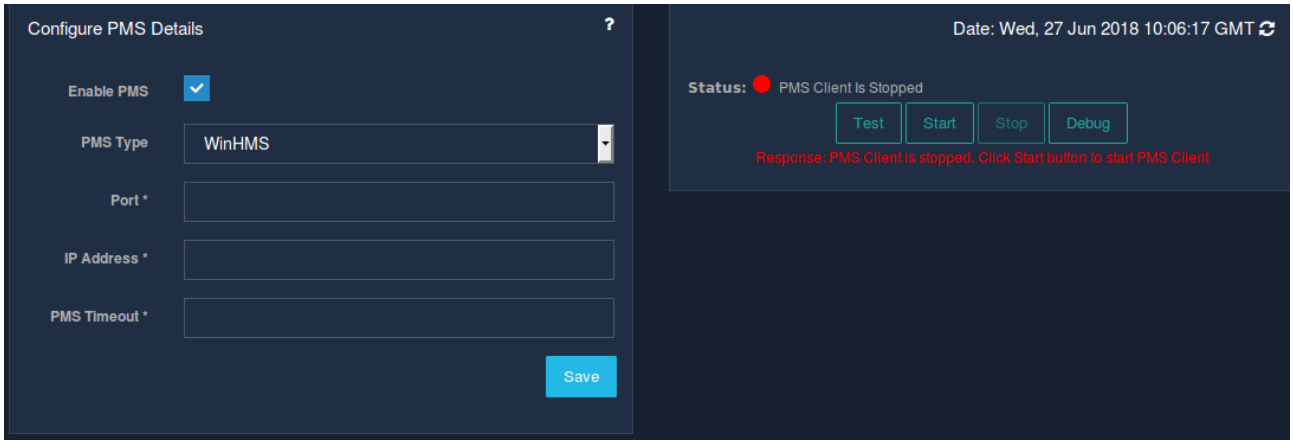


Fig

Fields	***Description***
PMS Type	Select **Micros** option from the **PMS Type** drop down menu.
IP Address	Enter the IP Address of the PMS server in the **IP Address** filed.
Port	Enter the port of PMS server in the **Port** field.
PMS Timeout	Enter the PMS timeout in seconds. (Recommended is 5 seconds)
Test PMS Connectivity	Click the **Check PMS** button in front of **Check PMS Connectivity** to check the PMS connectivity.

Table

WinHMS:

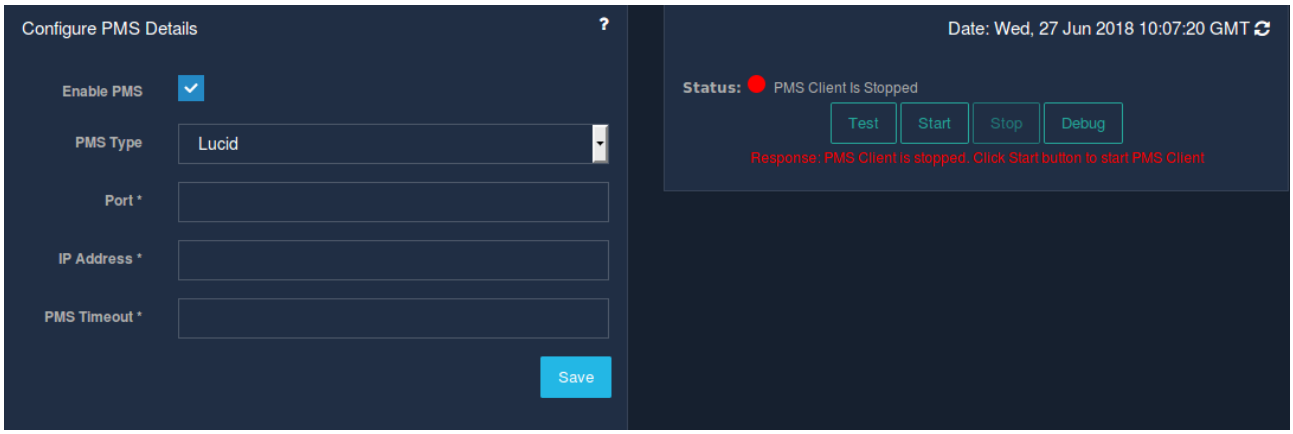


Fig

Fields	***Description***
PMS Type	Select **WinHMS** option from the **PMS Type** drop down menu.
IP Address	Enter the IP Address of the PMS server in the **IP Address** filed.
Port	Enter the port of PMS server in the **Port** field.
PMS Timeout	Enter the PMS timeout in seconds. (Recommended is 5 seconds)
Test PMS Connectivity	Click the **Check PMS** button in front of **Check PMS Connectivity** to check the PMS connectivity.

Table

Lucid:



Fig

Fields	***Description***

PMS Type	Select **Lucid** option from the **PMS Type** drop down menu.
IP Address	Enter the IP Address of the PMS server in the **IP Address** field.
Port	Enter the port of PMS server in the **Port** field.
PMS Timeout	Enter the PMS timeout in seconds. (Recommended is 5 seconds)
Test PMS Connectivity	Click the **Check PMS** button in front of **Check PMS Connectivity** to check the PMS connectivity.

Table

Click on the 'Save' button to save the PMS configuration.

6.7.2 PMS Guests

This page displays the list of all PMS guests downloaded from the PMS server as well as those defined in the system manually. UniBox communicates with the PMS system and downloads the list of current guests so they can be validated locally. Each guest is displayed in a tabular format with its name, room number, guest number, arrival date, departure date and username linked. The username is linked when guest logs in or authenticate using standard PMS portal using client machine. Guest will need to enter his room number and last name combination in portal while login process.

6.7.2.1 Creation

Select the subsection named 'Guest' from the 'PMS' section in the 'Billing' module present in the sidebar. Click on the '**+**' icon to create or add a new pms guest. A modal will be displayed that collects the information required to create a new pms guest.

Fields	*Description*
Guest Number	An unique guest number for the guest. You dont have to enter this value since it is auto-generated.
Guest Name	Enter the name for the guest.
Room Number	Enter the room number for the guest.
Arrival Date	Enter the arrival date for the guest from the calendar provided.
Departure Date	Enter the departure date for the guest from the calendar provided.

Table

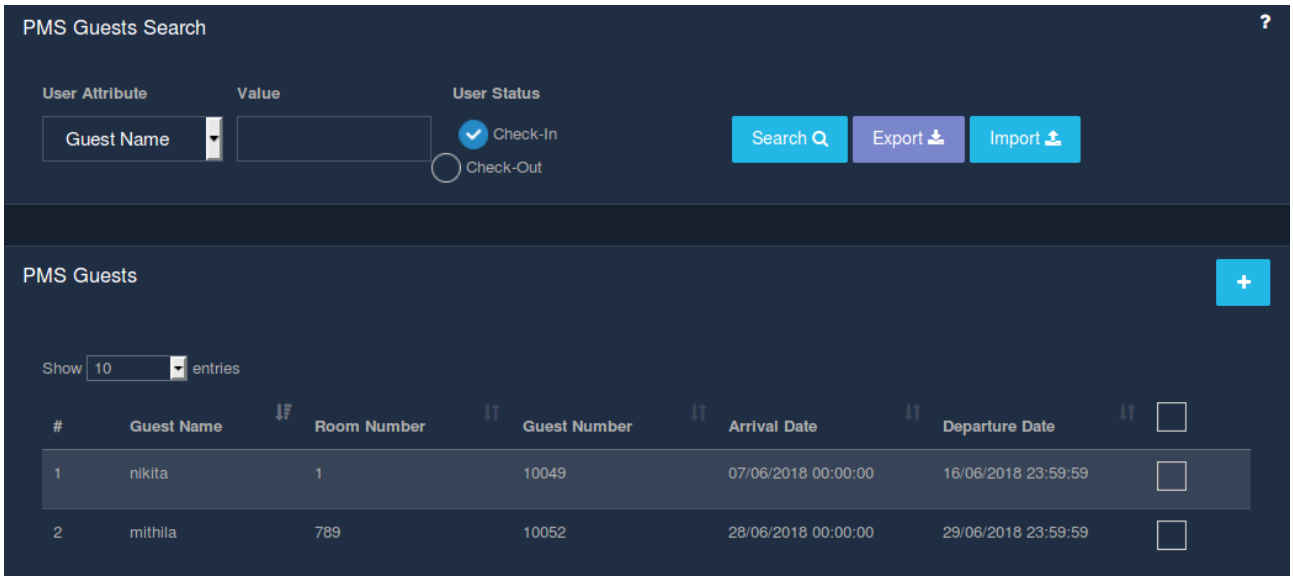
Click 'Save' and a new pms guest will be created.

6.7.2.2 List PMS Guests

Each guest is displayed in a tabular format with its name, room number, guest number, arrival date, departure date and username linked.

To search for given guest records, enter the search criteria and click the 'Search' button.

The list can be sorted in ascending or descending order using the icon on each column header.



Fig

6.7.2.3 Delete PMS Guest

This section allows the administrator to delete the existing PMS guest from Unibox.

To delete a specific PMS guest, check in the checkbox provided besides the guest details and then click on the delete option. A message pops up to confirm the delete operation. If sure, click on ‘Delete’ button.

Fig

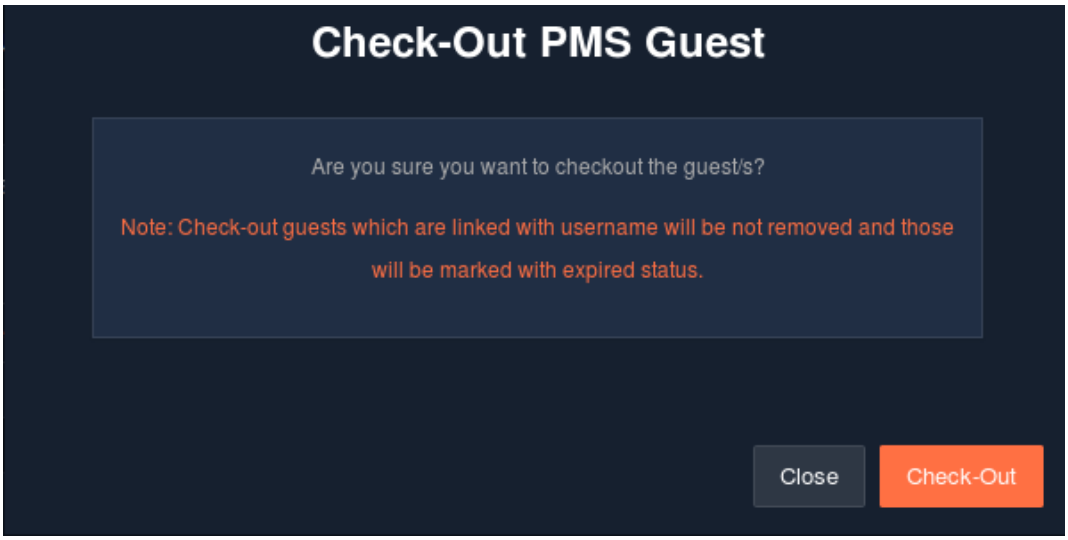
6.7.2.4 Check-Out PMS Guest

This section allows the administrator to perform the check-out operation the guest.

It basically removes the existing pms guest from the pms guest list.

In order to perform the check-out operation, check on the checkbox provided besides the guest details and then click on the check-out button. A message pops up to confirm the check-out operation.

If sure, click on ‘check-out’ button.



Fig

6.7.2.5 Export PMS Guest

This section allows an administrator to export the PMS guest information. All check-in or check-out guest information is included in the exported list.

The guest information can be exported in one format - Excel (CSV).

In CSV format, the guest information like guest name, room number, guest number, arrival date, departure date is exported as comma-separated values. The file can be imported into Excel for viewing or printing. The file can be easily emailed to other people for distribution.

Click on the ‘Export’ button to export the PMS guest list.

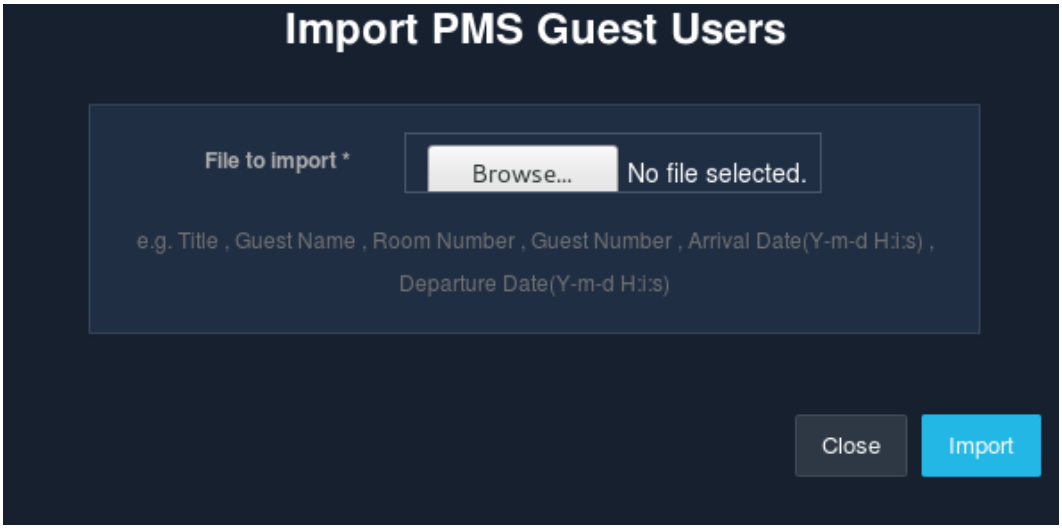
6.7.2.6 Import PMS Guest

This section imports PMS guests from the provided CSV file. Existing guests will get updated while importing all guests.

The csv file should be of the following format:

- Guest Name
- Room Number
- Guest Number
- Arrival Date
- Departure Date

In order to import a file, click on the ‘Import’ button. Then choose the file you wish to import.



Fig

6.7.3 Transactions

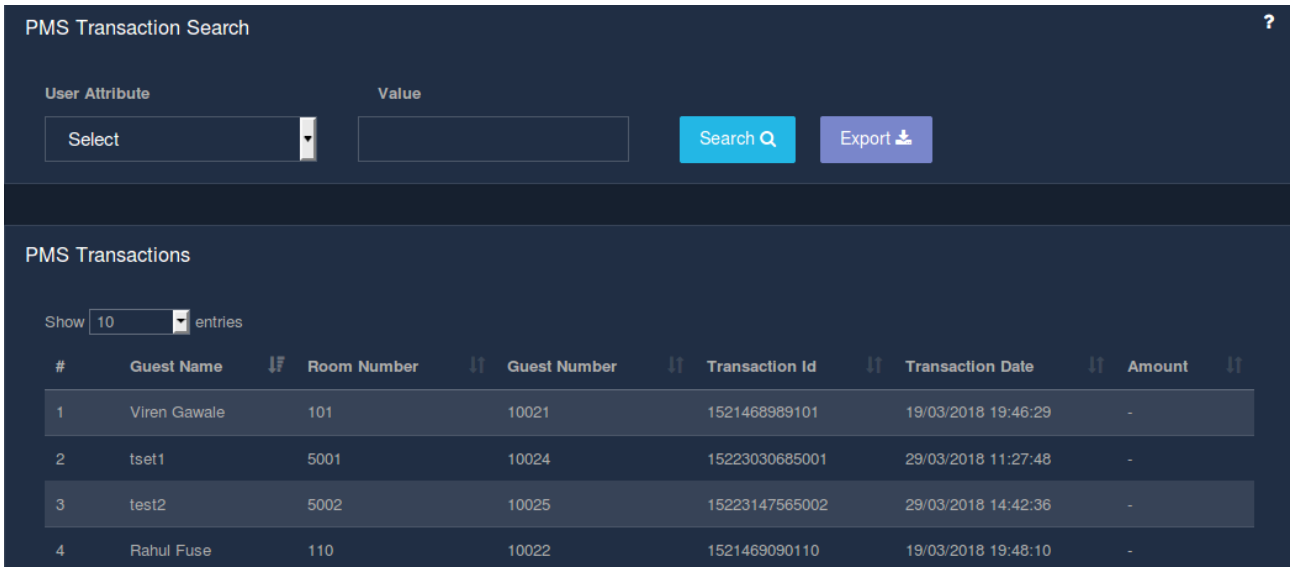
6.7.3.1 List PMS Guest Transaction

This page displays the list of all PMS guest transaction defined in the system. Each guest transaction is displayed in a tabular format with its name, room number, guest number, transaction id, transaction date and amount.

The username is linked to guest and can be reached for details when clicked on guest name. A PMS transaction entry is created when guest logins in using standard PMS portal using client machine. Guest will need to enter his room number and last name combination in portal during the login process.

To search for given guest transaction records, enter the search criteria and click the 'Search' button.

The list can be sorted in ascending or descending order using the icon on each column header.



Fig

6.7.3.2 Export PMS Guest Transaction

This page allows the administrator to export the transaction records for the given time interval. Click on the 'Export' button to export the PMS guest transaction. The transactions are exported in Excel (CSV) format. The csv file should be of the following format:

- Guest Name
- Room Number
- Guest Number
- Transaction ID
- Transaction Amount
- Transaction Date.

6.7.4 Monitor PMS Guest

For some PMS system, UniBox needs to maintain a TCP connection with the PMS server. This page displays the status of PMS client connection with PMS server. Select the time duration and the display type, and the report would be displayed accordingly.

Tabular view shows Status with Monitored Time records over give time period.

Graphical view shows Status with Monitored Time records over give time period.

7. TOOLS

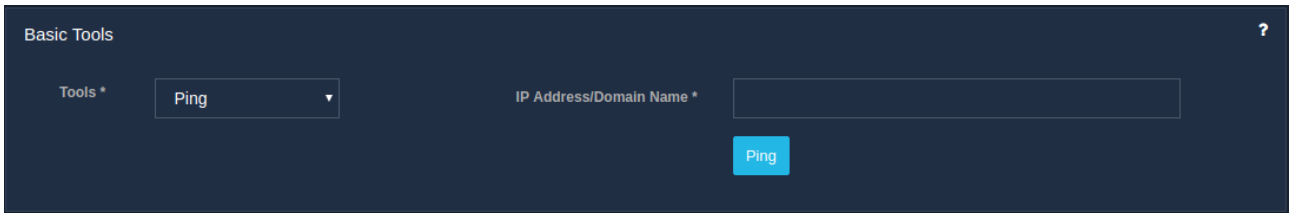
7.1 Diagnostic Tools

7.1.1 Basic Tools

7.1.1.1 Ping

This feature allows an admin to run ping utility in UniBox. The admin needs to enter the IP address or domain name for the server. Ping utility will help an admin to check the health and latency of the connection to a remote machine and whether the link to the remote machine is up or down.

To ping, go to the 'Basic Tools' section in the 'Diagnostic Tools' sub-module under the 'Tools' module. Then select the 'Ping' option from the drop-down menu. Type in the IP address or domain name and click on the 'Ping' button.



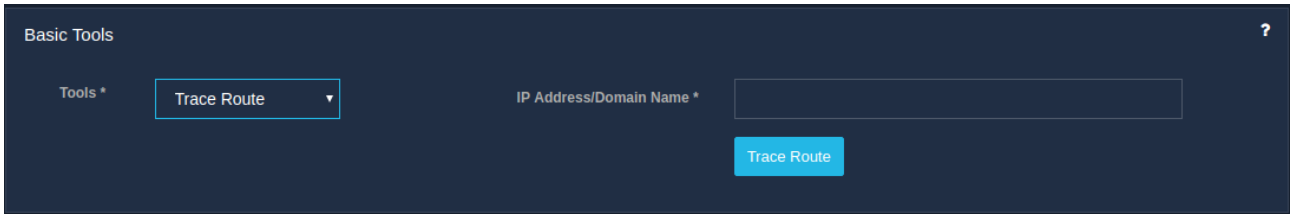
Fig

The output displays the ping response time in milliseconds, packet statistics and packet loss percentage to the user.

7.1.1.2 Trace Route

To find the network hops to a remote host, an admin is allowed to trace route. Trace route is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. Unibox will resolve the given URL and will attempt to find all the hops from its address to the remote address.

To trace route, select the 'Trace Route' option from the drop-down menu present in the 'Basic Tools' section in the 'Diagnostic Tools' sub-module under the 'Tools' module. Once the option is selected, type in the IP address or web URL of the remote host.

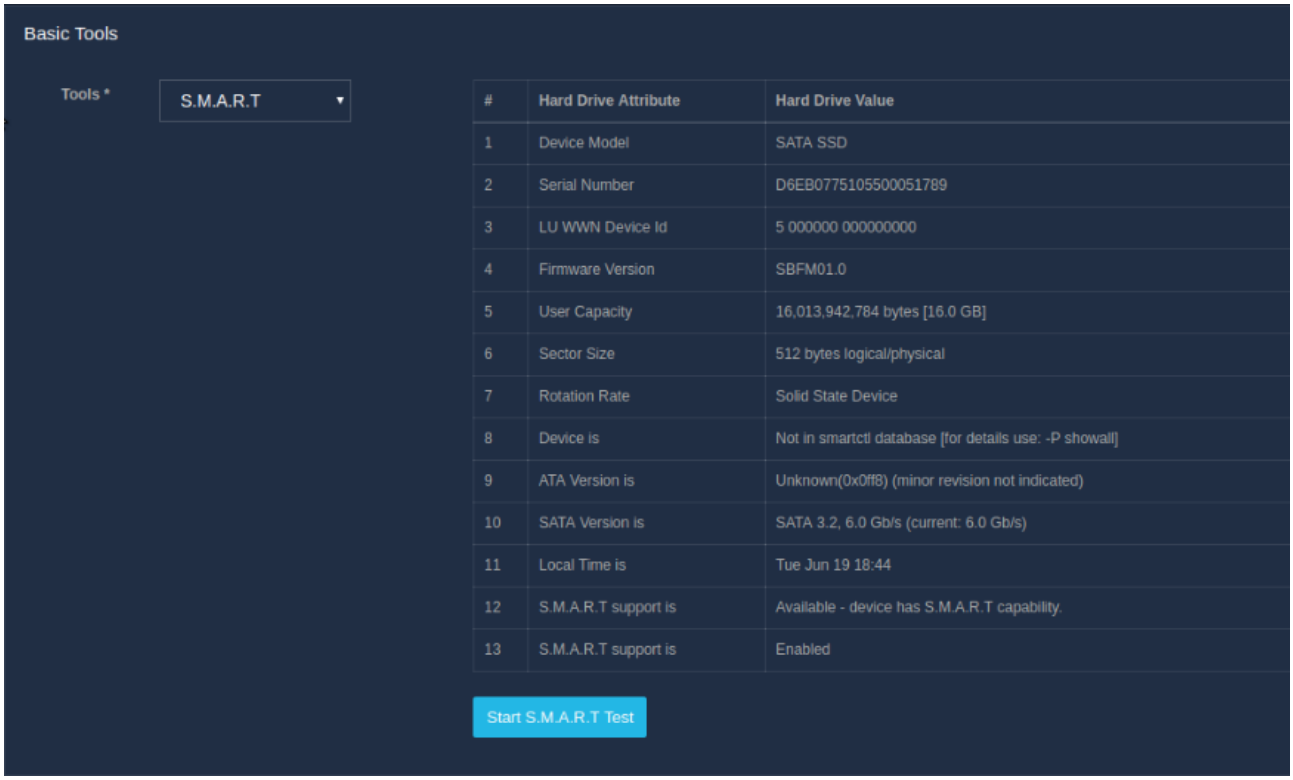


Fig

7.1.1.3 S.M.A.R.T

Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) system, built into many ATA-3 and later ATA, IDE and SCSI3 hard drives. The purpose of S.M.A.R.T is to monitor the reliability of the hard drive and predict drive failures. If your SSD/HDD does not support S.M.A.R.T test, then the S.M.A.R.T Test button will be invisible and likewise an information will be displayed.

To use the S.M.A.R.T tool, go to the 'Basic Tools' section in the 'Diagnostic Tools' sub-module of the 'Tools' module. Then select the 'S.M.A.R.T' option from the drop-down menu.



Fig

Attributes	***Description***
SSD Information Table	This table displays the S.M.A.R.T and general information about your SSD/HDD.
Start S.M.A.R.T Test	After clicking the button, the result of the S.M.A.R.T test for the whole disk is displayed.

Table

7.1.2 IP Scan

An admin is allowed to run IP Scan on the entire LAN subnet. This provides a list of IP addresses of the live machines which are connected to the network under UniBox.

To do an IP scan, select the 'IP Scan' section from the 'Diagnostic Tools' sub-module present in the 'Tools' module. Then select the LAN profile from the drop-down list and click on the 'Scan' button.

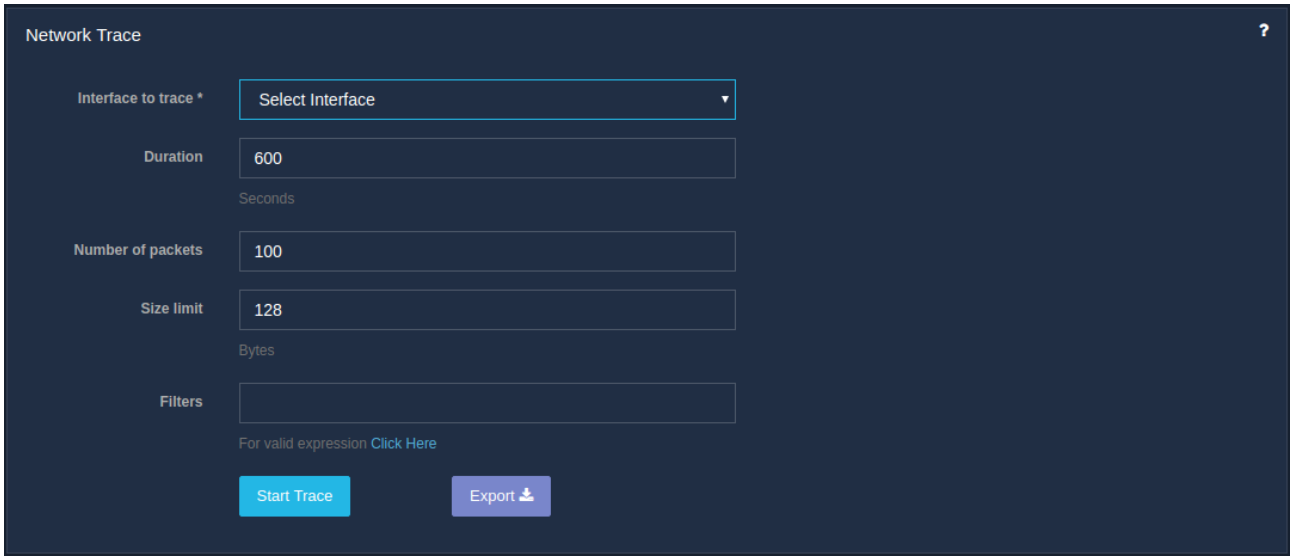
Fig

Note: The IP scan will take a few minutes to complete. So, it is requested for the admin to remain patient while the scan runs are calculated.

7.1.3 Network Trace

The network trace tool enables an admin to capture detailed information about data that are streaming through the network.

To use the network trace tool, go to the 'Tools' module followed by the 'Diagnostic Tools' sub-module. Then go to the 'Network Trace' section and fill in the form that is displayed on the page.



Fig

Fields	*Description*
Interface to Trace	Select the interface on which to track data.
Duration	Specifies the number of seconds over to which to capture data. Once this limit is reached, the trace stops. **Default is 600 seconds or 10 minutes.**
Number of Packets	Specifies the maximum number of packets to be captured. The rest of them are discarded.
Size limit	Specifies the maximum number of bytes to capture each packet. The rest of the data are discarded. **Default is 128 bytes.**

Filters	Enables to specify a filter expression that controls which packets the trace captures. Leaving the filter blank, captures all the packets.
Start Trace	Begins the trace.
Stop Trace	Ends the trace.

Table

7.1.3.1 Export Network Trace

This option allows an admin to export the network trace information. The network trace results are exported in PCAP format. To export the result, simply click on the 'Export' button.

7.1.4 Force Authentication

This tool allows an admin to authorize a user without the user needing to authenticate using the login page or captive portal. This is especially useful for the support technicians since they can remotely authenticate the user and get the user online. This list shows the authorized and unauthorized DHCP leases in the UniBox.

The admin can also search a specific MAC address or IP address in the list. The 'State' column indicates whether a user has authenticated successfully in the system or not.
The 'State' column also allows an admin to authenticate or logout DHCP lease using 'Authenticate' button or 'Logout' button.

To force authenticate or logout, go to the 'Tools' module in the sidebar, then go to the 'Diagnostic Tools' sub-module. Select the 'Force Authentication' section.

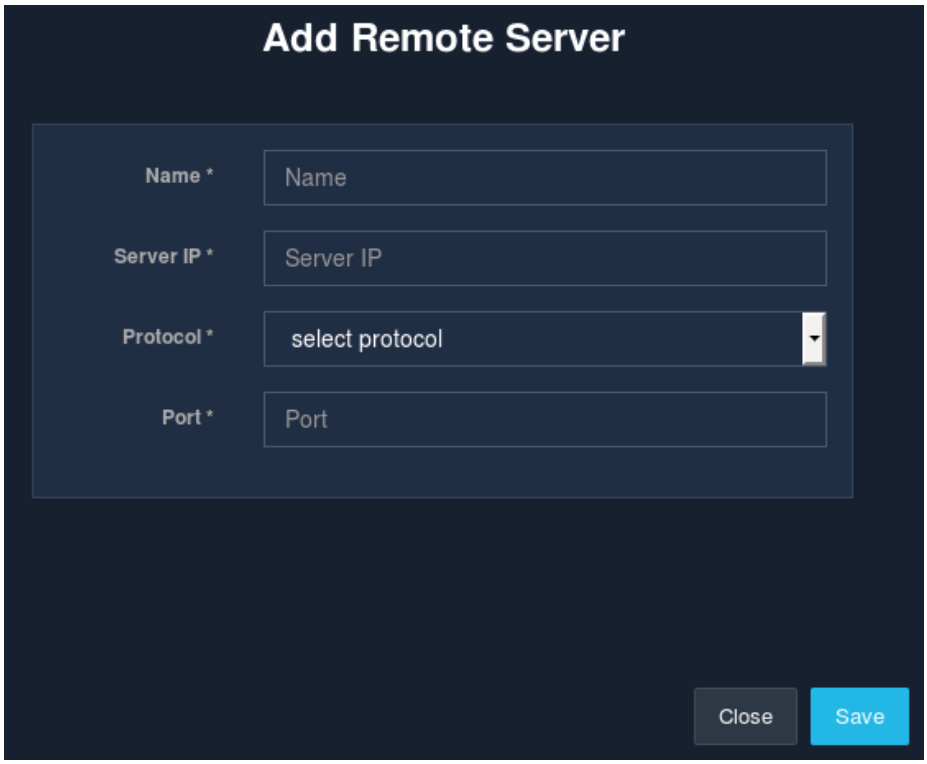
Fig

7.2 Remote SysLogs

7.2.1 Create / Add Remote Server

An admin is provided the facility to define a new remote syslog server. The remote syslog server is used for sending the syslog message for debugging and record keeping.

To create a remote syslog server, go to the ‘Tools’ module in the sidebar, then the ‘Remote SysLog’ section. Click on the ‘+’ icon where a window displays a form where the necessary details are to be filled to create a remote server.



Fig

Fields	*Description*
Name	Enter the name of the remote syslog sever.
Server IP	Enter the IP address of remote server.
Protocol	Select the protocol, either tcp or udp, for sending syslogs.
Port	Enter the port number on which the syslog messages will be sent.

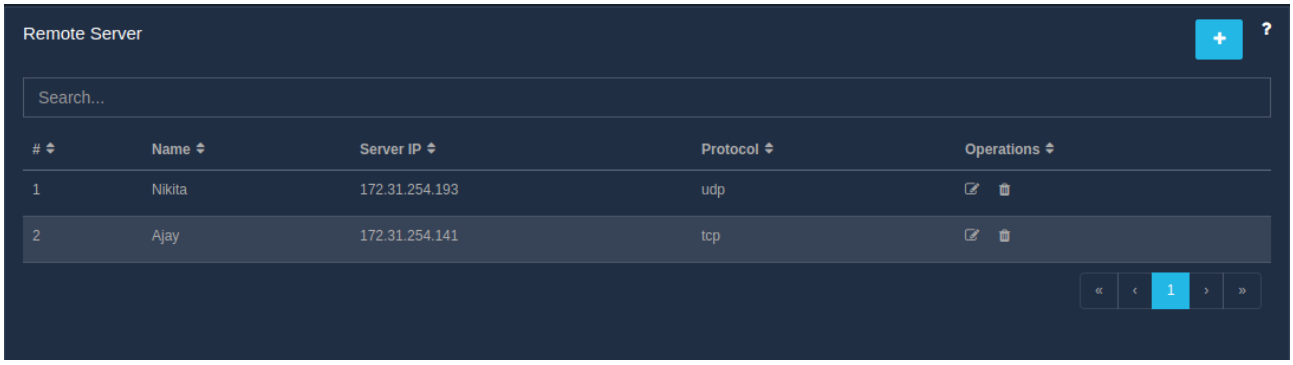
Table

Click on the ‘Save’ button to save the configurations and create a remote server.

7.2.2 List Remote Server

All the remote syslog servers defined by the admin in the UniBox, is listed down in a table. Along with the name of the server, the IP address and the protocol used for syslog are also displayed. The list also contains an ‘Operations’ column, which gives the options to either edit or delete severs.

To view the list of remote servers, select the ‘Remote SysLog’ section in the ‘Tools’ module.

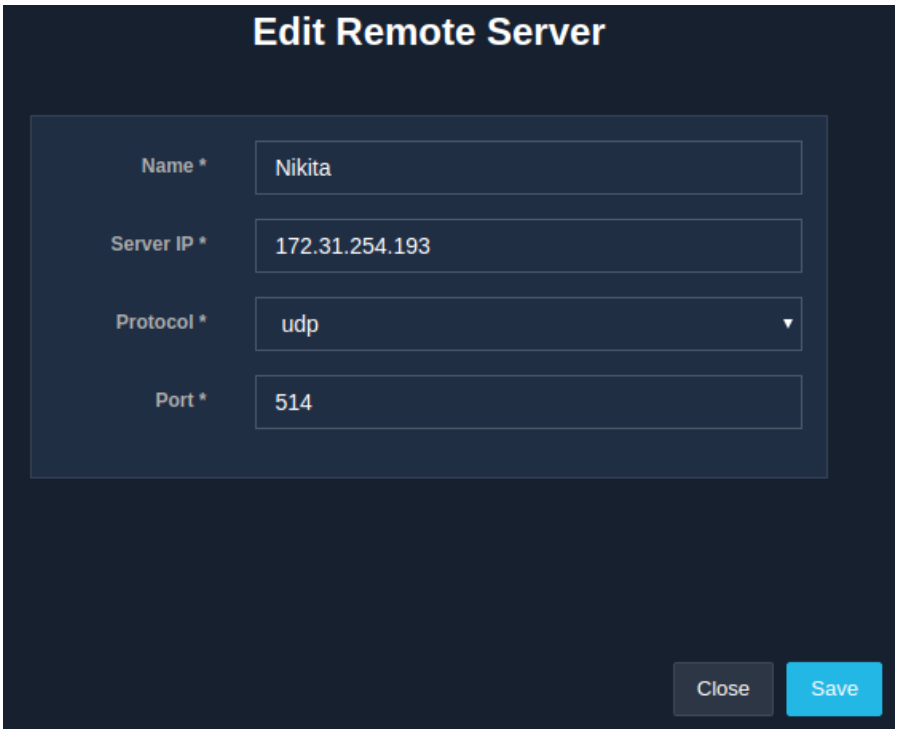


Fig

7.2.3 Edit Remote Server

This option allows an admin to make changes to the configuration of an already existing Remote Syslog server.

To edit a remote server, go to the 'Tools' module in the sidebar, then select the 'Remote SysLogs' section. The 'Operations' column in the listing table consists of the edit icon. Click on the edit icon. A window displays a form where the necessary changes can be made. Refer.



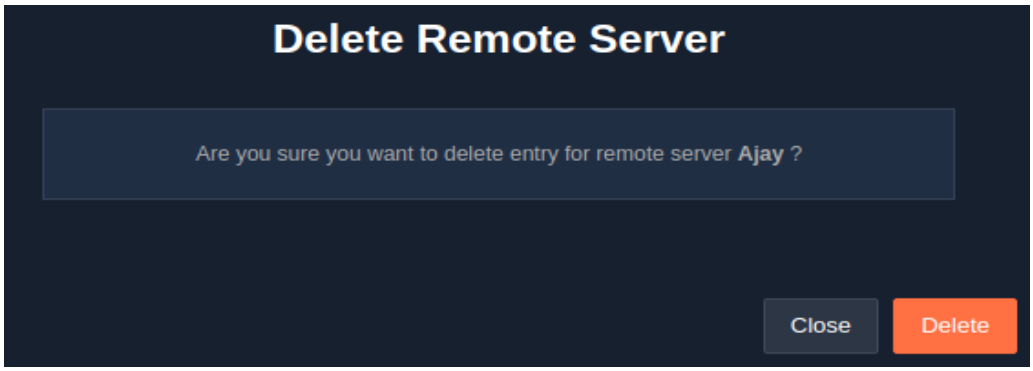
Fig

Click on the 'Save' button to apply the changes made.

7.2.4 Delete Remote Server

An admin can delete an existing remote syslog server entry. Once the entry is deleted, UniBox will stop sending messages to the remote server.

To delete a remote server, select the delete icon in the ‘Operations’ column present in the ‘Remote SysLogs’ section of the ‘Tools’ module. A message window pops up to confirm the delete action.



Fig

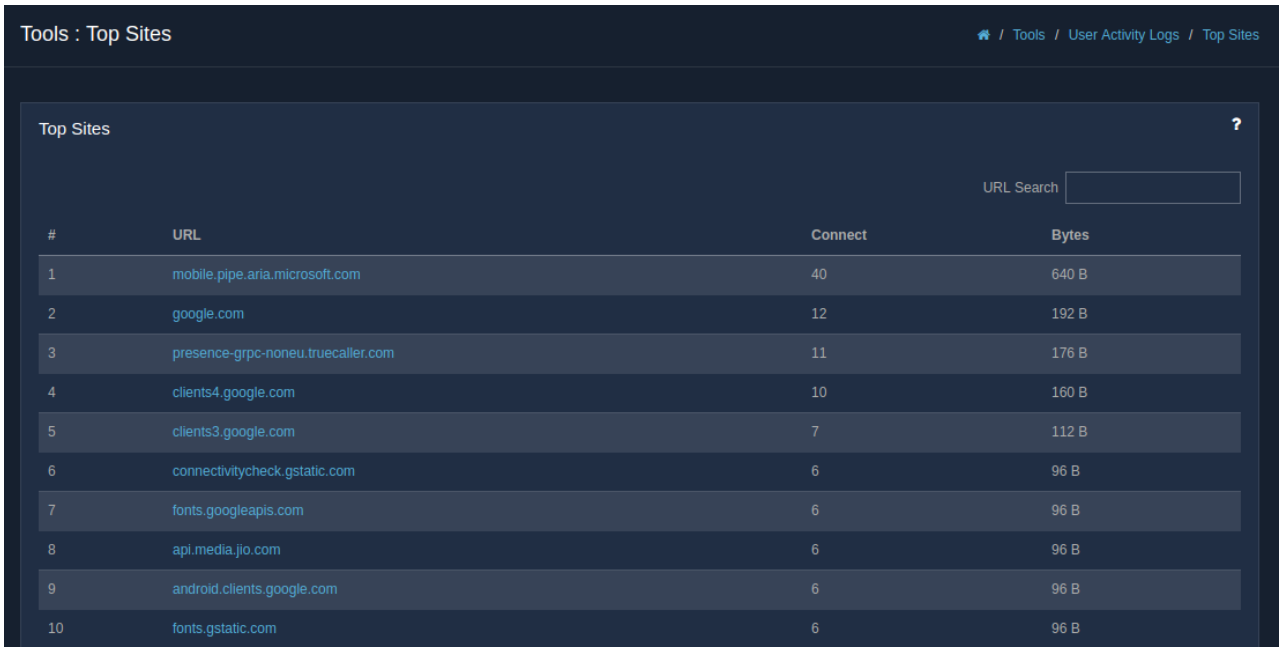
Click on the ‘Delete’ button to surely delete the remote server.

7.3 User Activity Logs

7.3.1 Top Sites

This feature displays a list of the top websites visited by UniBox users over a 24 hour period. The sites are displayed in descending order, i.e., the most frequently visited sites are at the top of the listing table. The list displays the URL, the connect which is the number of access to the site, and the bytes, i.e., the bandwidth consumed visiting that site. An admin also search based on specific URLs.

To view the top sites visited, go to the ‘User Activity Logs’ sub-module in the ‘Tools’ module. Then select the ‘Top Sites’ section.



Fig

7.3.2 Site & Users

The ‘Site & Users’ section allows an admin to search for the web browsing activities of specific users using the web address (URL) or Username or MAC address of a user’s system.

To find the web activities, go to the ‘Sites & Users’ section in the ‘User Activity Logs’ sub-module under the ‘Tools’ module. The page displays a set of fields required to search and find the web activities.

Fig

Fields	***Description***
Username	Enter the username whose activities need to be tracked.
MAC Address	Enter the MAC address to search.
URL	Enter the URL to search.

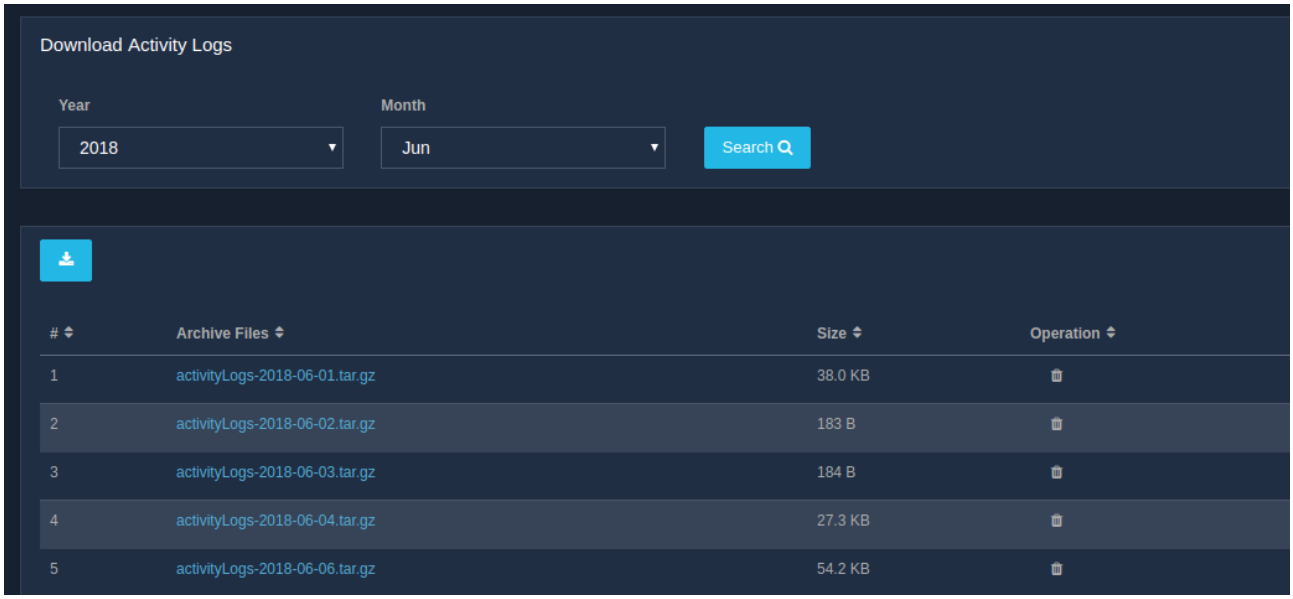
Table 1

Click on the ‘Search’ button and a list of a user’s web activities will be displayed.

7.3.3 Download Activity Logs

Admin can list out the Archived Activity for a specified time period by providing the month and year as input for search. All the activity logs are stored in a compressed CVS format only and are kept for 180 days.

To download the activities of all the users, go to the ‘User Activity Logs’ sub-module under the ‘Tools’ module present in the sidebar. Then click on the ‘Download Activity Logs’ section. Fill in the fields to find the activities as per the specific time period.



Fig

Fields	***Description***
Year	Select the year for searching Activity logs.
Month	Select the month for searching Activity logs.

Table

Specify the year and month, then click on the 'Search' button, a list of 'Archive' files will be displayed.

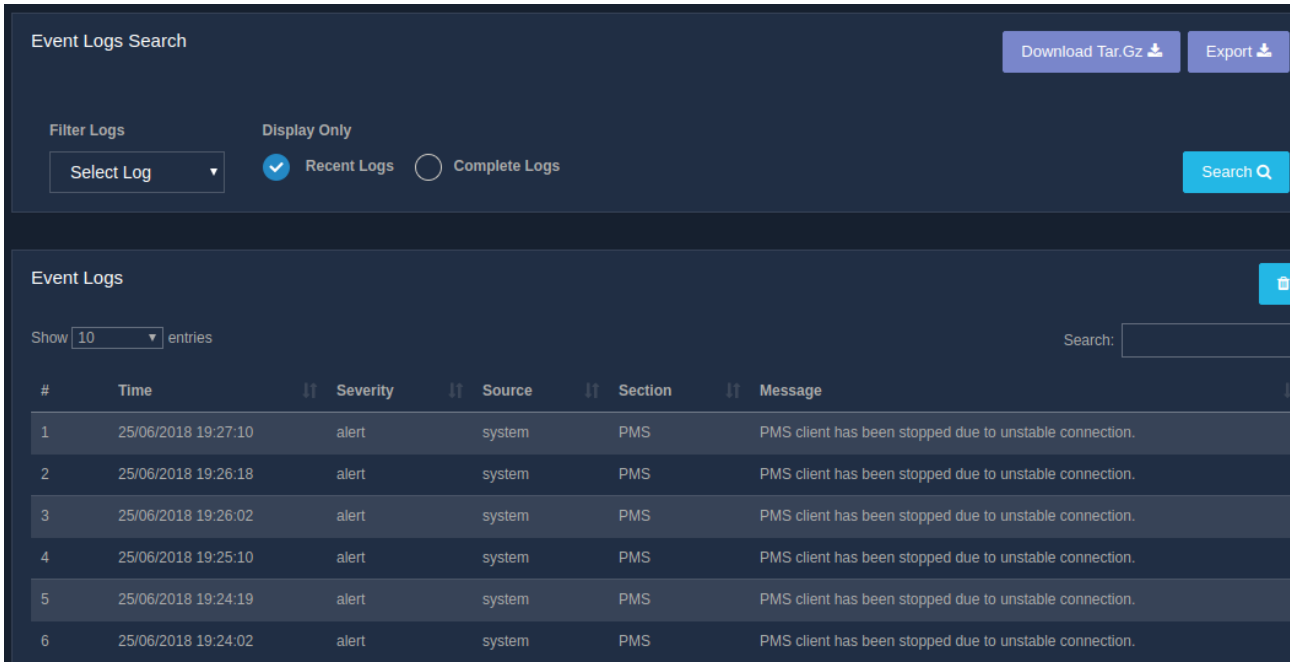
- To download one particular file, click on the specific file. The specific file will be downloaded.
- To download all the archive files, click on the download icon provided at the beginning of the list.

7.4 Event Logs

7.4.1 List Event Logs

Event logs provide an admin the complete view of the activities happening inside the UniBox. These logs are helpful in debugging user login issues and any other issue on the network. All the events in UniBox are logged in the event logs, allowing an admin to perform audit trails, troubleshoot and diagnose the problem easily.

To view the list of events, go to the 'Event Logs' section in the 'Tools' module present in the sidebar.



Fig

Fields	***Description***
Filter Logs	Select the condition for filtering logs – severity of the event, source of the event, module section of UniBox.
Display Only	Recent logs or complete logs. Recent logs will display logs with last 20 lines.

Table

Each entry has the date and time of the event, severity, source and module or section in which the event originated. In addition, there is a short description of the event.

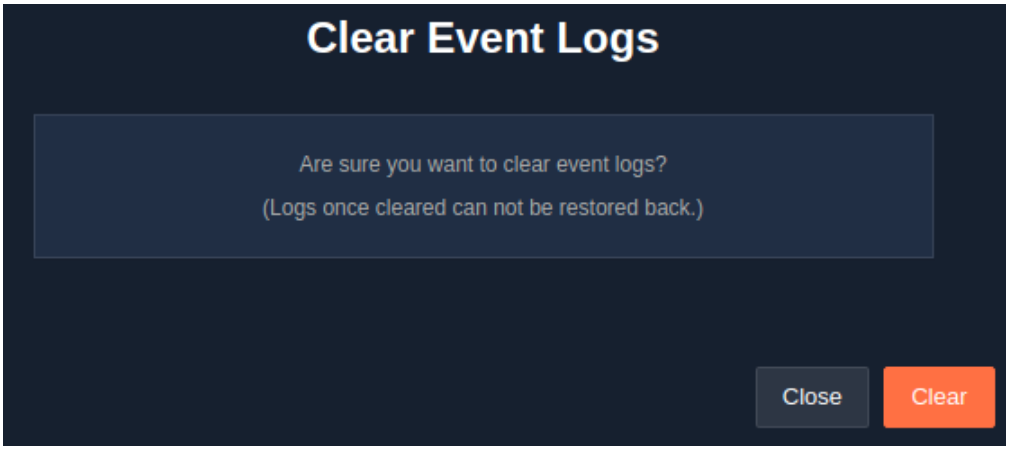
7.4.2 Export Event Logs

Through the export feature, an admin is provided the facility to export the logs locally for review and future reference. The logs are stored with the timestamp, severity, the source of the event, the UniBox module that generated the event and also the description of the event. The logs are stored in simple text file and are saved locally on the machine.

To export the event logs, go to the 'Event Logs' section in the 'Tools' module. Click on the export icon to download all the event logs.

7.4.3 Clear Event Logs

This option allows an admin to clear all event logs. Logs once cleared, cannot be restored back. To clear logs, click on the icon assigned to clear logs. A window pops up with a message to confirm the clear action.


Clear Event Logs
Are sure you want to clear event logs?
(Logs once cleared can not be restored back.)
Close
Clear

Fig

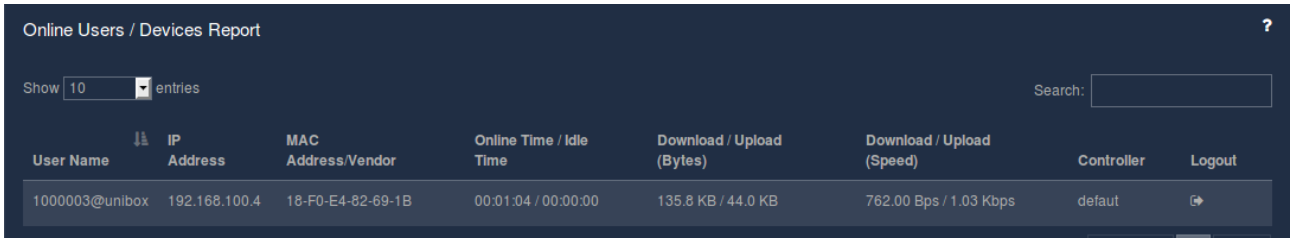
8. Reports

8.1 Online Users

This page displays the list of online users in Unibox. Each row displays the username, IP address, MAC address of the user's machine and the vendor name, Online Duration (online and idle), Bandwidth usage (upload and download), Bandwidth rate (up/down speed), controller name and Logout button.

The list is updated automatically in real-time after a few minutes. The administrator can use the logout button to close/logout the user's session.

The search fields allow administrator to search for specific users from the list.



Fig

8.2 User Agents

This page displays various user agent reports based on the browser, operating system and type of devices used by the end users. Following types of reports can be generated -

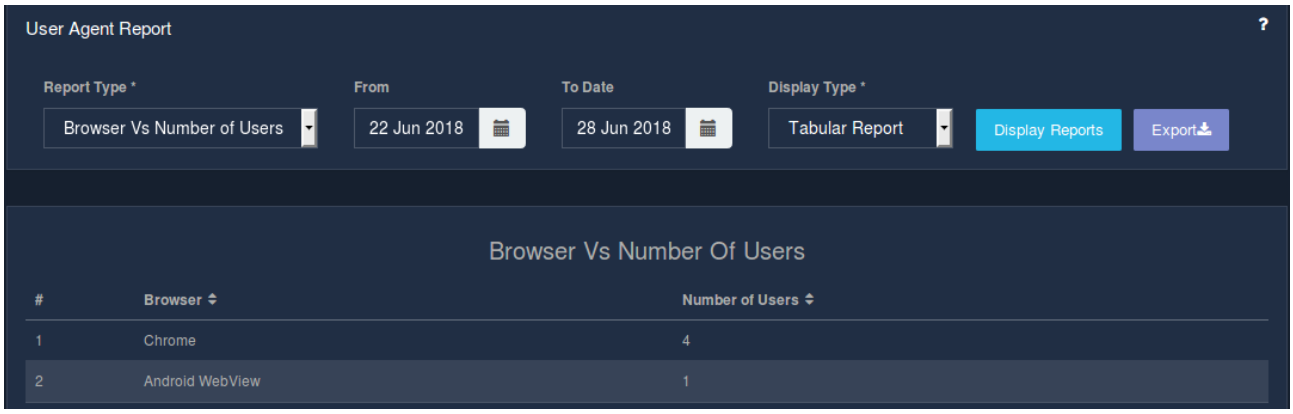
1. Browser Vs Number of Users: Display the total number of users who are using a particular browser within the time period. The report displays top 10 browsers only.

2. Operating System Vs Number of Users: Display the total number of users who are using various operating systems over a time period. The top 10 OS are displayed.

3. Vendors Vs Number of Users: Display the device vendor/types and corresponding number of users who are using them. The top 10 device vendors are displayed.

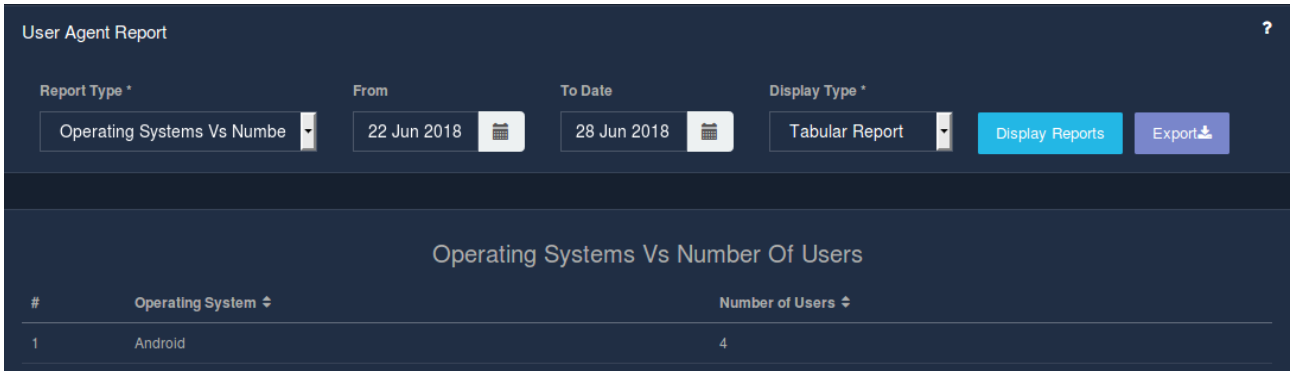
Lastly the administrator can select whether she wants to view the report in tabular or graphical format. The graphical report is displayed as a pie chart.

The screenshot below displays the user agent report where the report type is Browser Vs Number of Users.



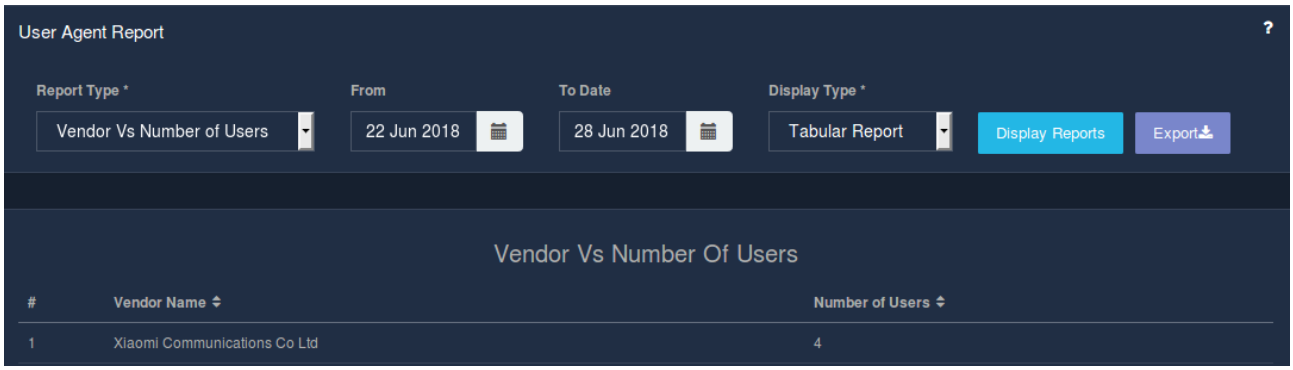
Fig

Report Type: Operating System Vs Number of Users



Fig

Report Type: Vendor Vs Number of Users



Fig

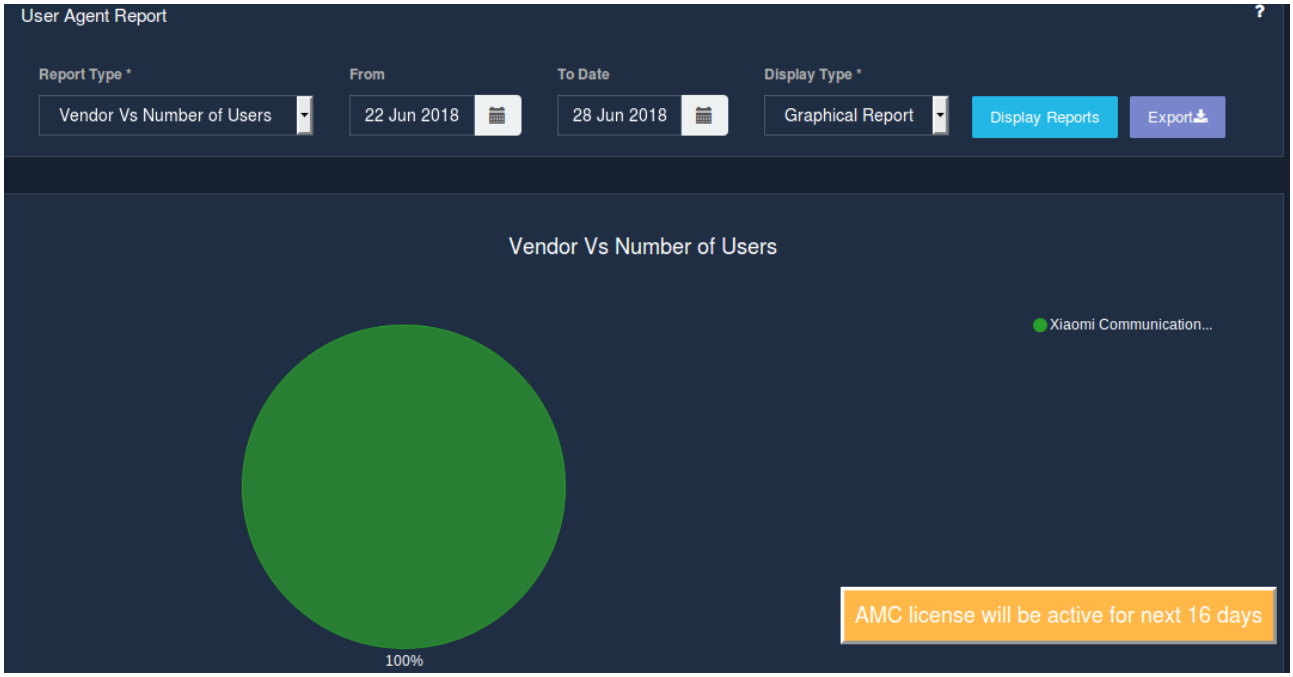
8.2.1 List User Agents

The reports are categorized in two types of display:

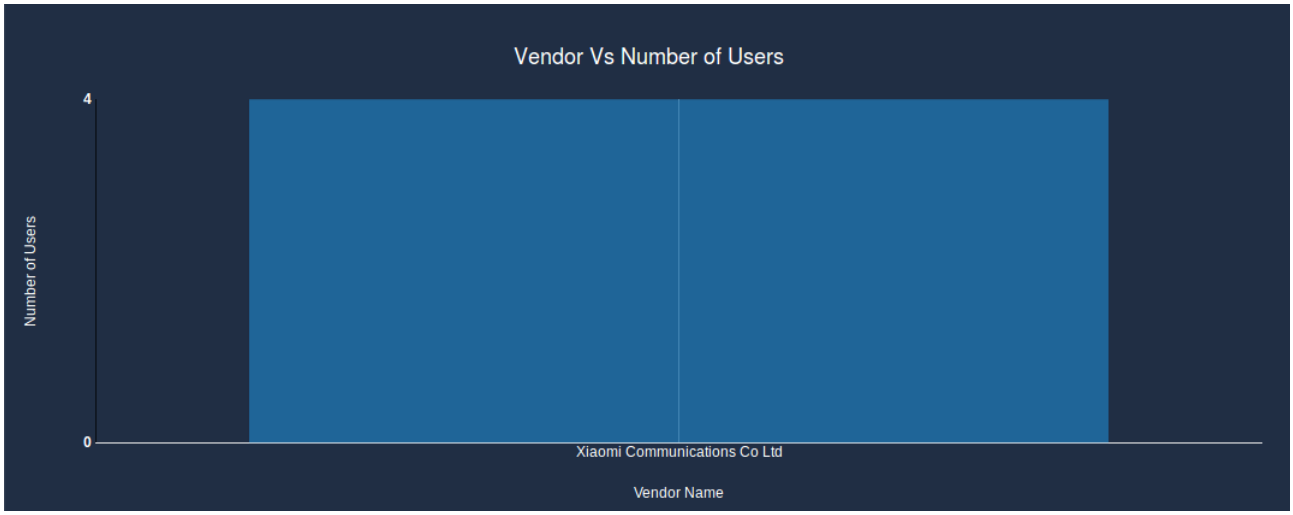
- Graphical
- Tabular

This section allows the administrator to select the type of report ,the type at which the report should be displayed for the specific time interval .To display a report, click on the 'Display Reports' button and it will display the report based on the report type selection.

The below screenshot displays the report in graphical format:



Fig



Fig

8.2.2 Export User Agents

This section allows an administrator to export various user agent reports based on the browser, operating system, device vendors and the number of users information.

The report is exported in csv format file and it is saved as a CSV file based on the report type selection.

If the file exported is Browser Vs Number of Users, then it follows the format:

- Browser
- Number of Users

If the file exported is Operating Systems Vs Number of Users, then it follows the format:

- Operating System
- Number of Users

If the file exported is Vendor Vs Number of Users, then it follows the format:

- Vendor Name
- Number of Users

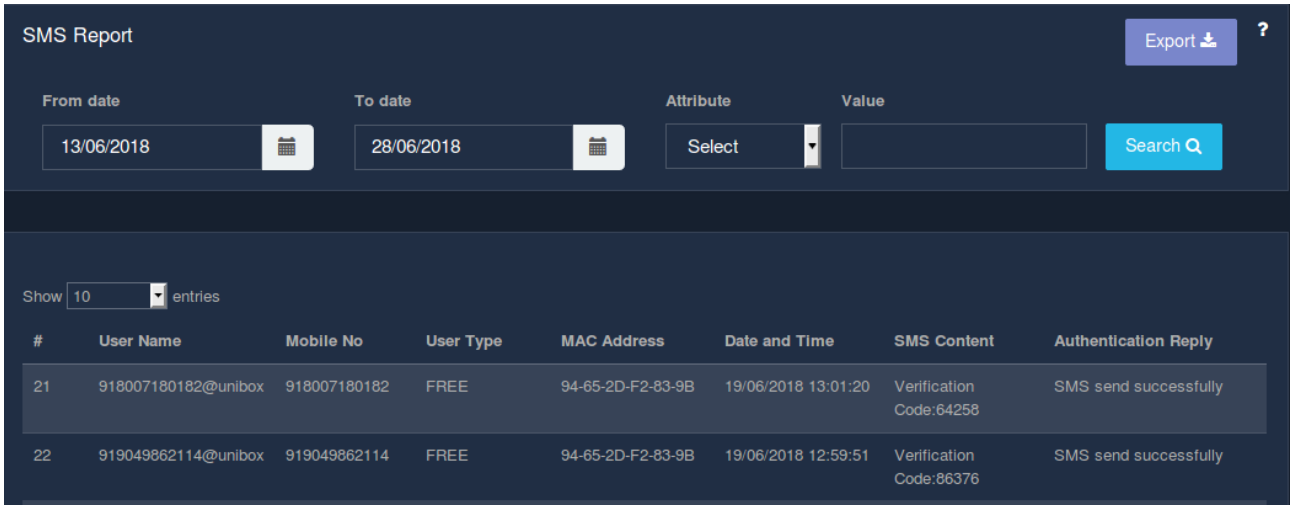
8.3 SMS

This section displays the report of all SMS sent from the system.

9.3.1 List SMS Report

The table shows the details of each SMS transaction. Each row displays Username,Mobile number,User Type,Mac Address,Date and Time and SMS Content from SMS server. The list can be sorted in ascending or descending order by using the icon on each column header.

Searching operation can also be performed on the time interval (from date – to date) and the user attributes.



Fig

8.3.2 Export SMS Report

The report exported contains detail description of Username, Mobile No, User Type, MAC Address, Date and Time and the SMS Content. To export a SMS report, click on the 'Export' button. This will then generate a csv file.

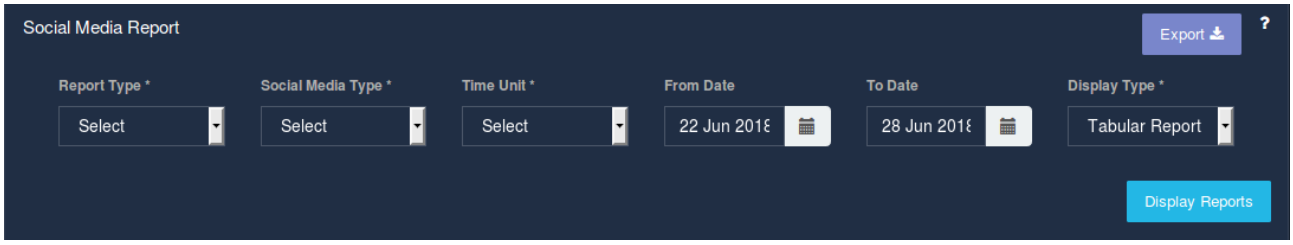
The CSV file exported follows the format:

- UserName
- Mobile No
- User Type
- Mac Address
- Date
- SMS Content
- Authentication Reply

8.4 Social Media Report

This section displays all the social media reports available in Unibox. The Social Media Type includes the following type of social media:

- Facebook Reports - Displays the different types of reports available for Facebook users.
- Google Reports - Displays the different types of reports available for Google users.
- LinkedIn Reports - Displays the different types of reports available for Linkedin users.
- Twitter Reports - Displays the different types of reports available for Twitter users.



Fig

8.4.1 List Social Media Report

It allows the administrator to perform searching based on the different report type followed by the social media type. Also, the time unit ranging from days to year is allowed. The display type allows you to select the type at which the report to be displayed taking into consideration the time interval. Click on the 'Display Report' will display the report of the selected social media type. Following is the detailed description of each of the social media types.

- Google

Displays all the google reports available in Unibox.

1. Gender Distribution - Displays the gender wise distribution of visitors over a given time period.

2. Social media Overview - Displays the number of Google logins over a given time period.

3. Visitor Loyalty -Displays the new and repeated login count of daily, weekly and monthly users over a given time period.

4. Visitor Log -Displays the visitor's google information from the logins over a given time period. It provides the list of all users who have logged in with their Google account.

5. Dwell Time - Displays the number of visitors against their dwell (session) time over a given time period. This report shows how long the users are waiting at the hotspot.

- Facebook

Displays all the facebook reports available in Unibox.

1. Gender Distribution - Displays the gender wise distribution of visitors over a given time period.

2. Social media Overview - Displays the number of logins over a given time period.

3. Visitor Loyalty - Displays the new and repeated user login of daily, weekly and monthly users over a given time period.

4. Visitor Log - Displays the visitor details over a given time period. Shows all the facebook users who have logged in.

5. Dwell Time - Displays the number of visitors against their dwell (session) time over a given time period.

6. Time Distribution of Traffic - Displays the count of visitors at various times during the day over a given time period.

- Twitter

Displays all the twitter reports available in Unibox.

1. Social media Overview - Displays the number of logins over a given time period.

2. Visitor Loyalty - Displays the count of new and repeat count for daily, weekly and monthly users over a given time period.

3. Visitor Log - Displays the visitor details visiting over a given time period.

4. Dwell Time - Displays the number of visitors against their dwell (session) time over a given time period.

5. Time Distribution of Traffic - Displays the count of visitors at various times during the day over a given time period.

- LinkedIn

1. Age Distribution - Displays the age wise count of visitors over a given time period.

2. Social media Overview - Displays the number of logins over a given time period.

3. Visitor Loyalty - Displays the count of new, daily, weekly and monthly users over a given time period.

4. Visitor Log - Displays the visitor details visiting over a given time period.

5. Dwell Time - Displays the number of visitors against their dwell (session) time over a given time period.

6. Time Distribution Of Traffic - Displays the count of visitors at various times during the day over a given time period.

8.3.2 Export Social Media Report

The report exported depends on the social media type selected along with the report type. To export a social media report, click on the 'Export' button. This will then generate a csv file which will be downloaded to the user's local machine.

8.4 System

This section provides various system related reports to the administrator. You can select the report of your choice by simply selecting the report type. Based on different type of reports, different fields would be generated.

All these reports can be further exported by clicking the button meant to export, named 'Export'. All the reports are exported in csv file extension.

Following reports can be viewed in this section -

- DHCP Leases - View the DHCP leases assigned to the LAN interfaces.

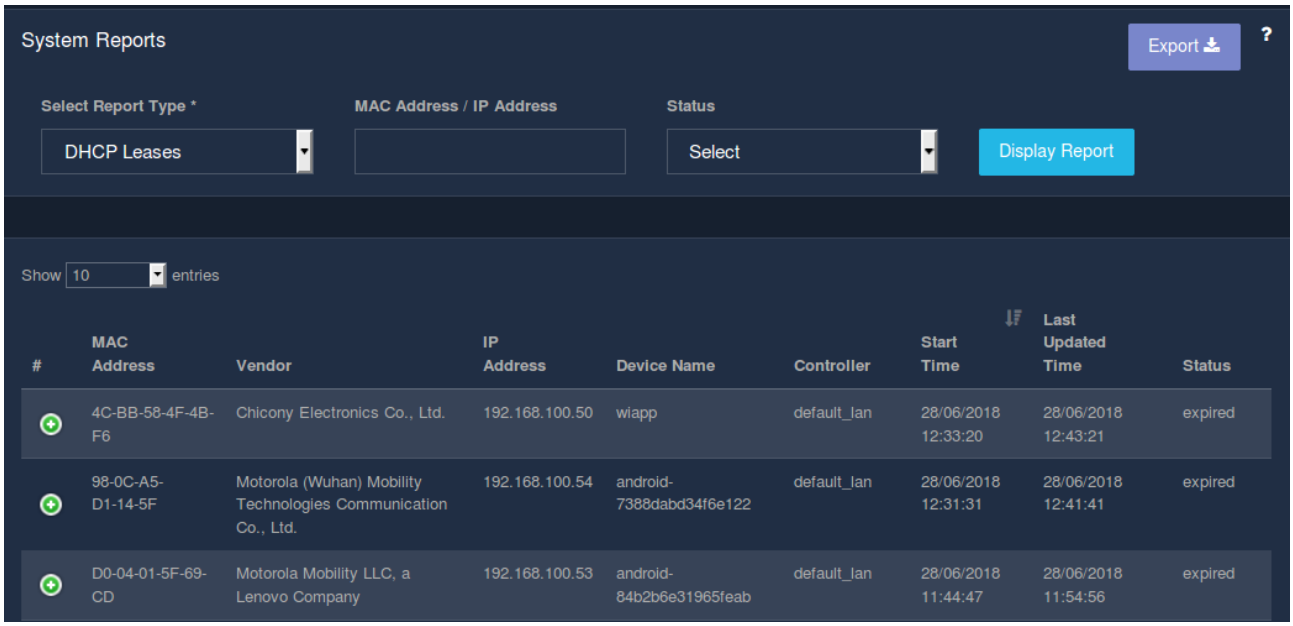
- Port Connections - Displays all the open ports for each user.
- Network Interface - Displays the statistics for each network interface.
- ARP Tables - Scans the network for available clients using ARP request. Provides the list of assigned IP addresses.
- System usage graphs - Shows the CPU, memory and port usage over 24 hours.
- System Information - Shows the system (hardware) information.
- System Power Cycle - Shows the report of system power cycles.

Each of these reports are explained in brief below.

8.4.1. DHCP Leases

This page displays the list of DHCP leases active in Unibox. It shows a list of DHCP addresses assigned to various clients on the network.

To display a DHCP lease report, the administrator must enter the IP/MAC address of the device and select the status of the device. After entering these values, a click on the 'Display Report' option would display the DHCP lease list. Each row displays the MAC address, Vendor name, IP Address, Device name, Controller ID, Start time of the lease, Last updated time of the lease and current status of the lease

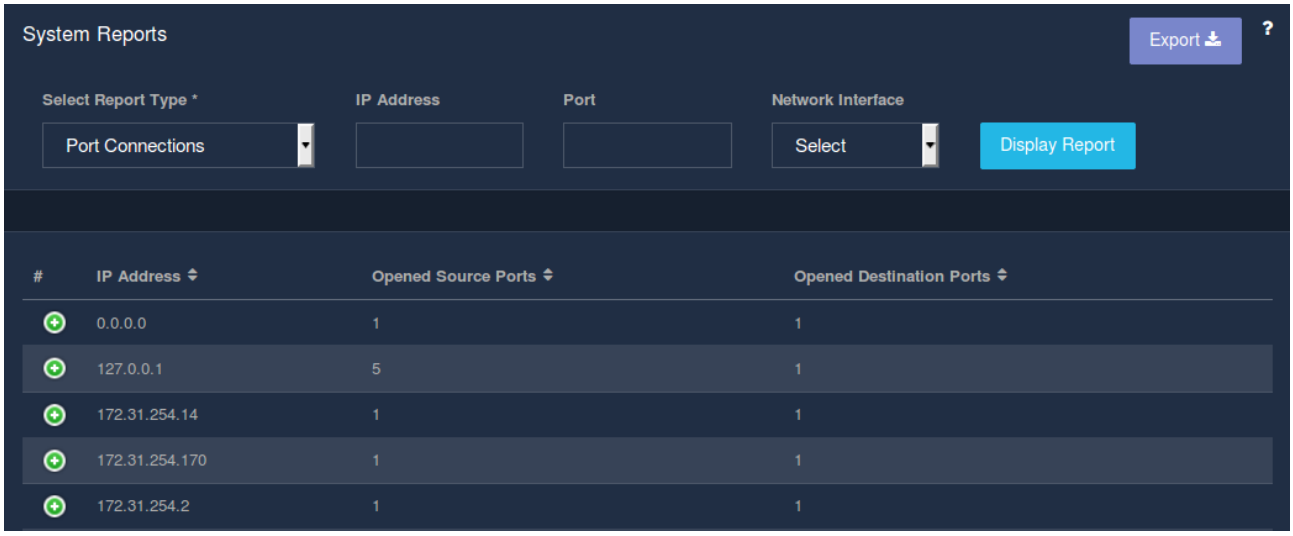


Fig

The administrator can also search a specific MAC address or IP address in the list. The administrator can expand each row to check the older leases assigned to the MAC address. The list can be exported using the export option.

8.4.2 Port Connections

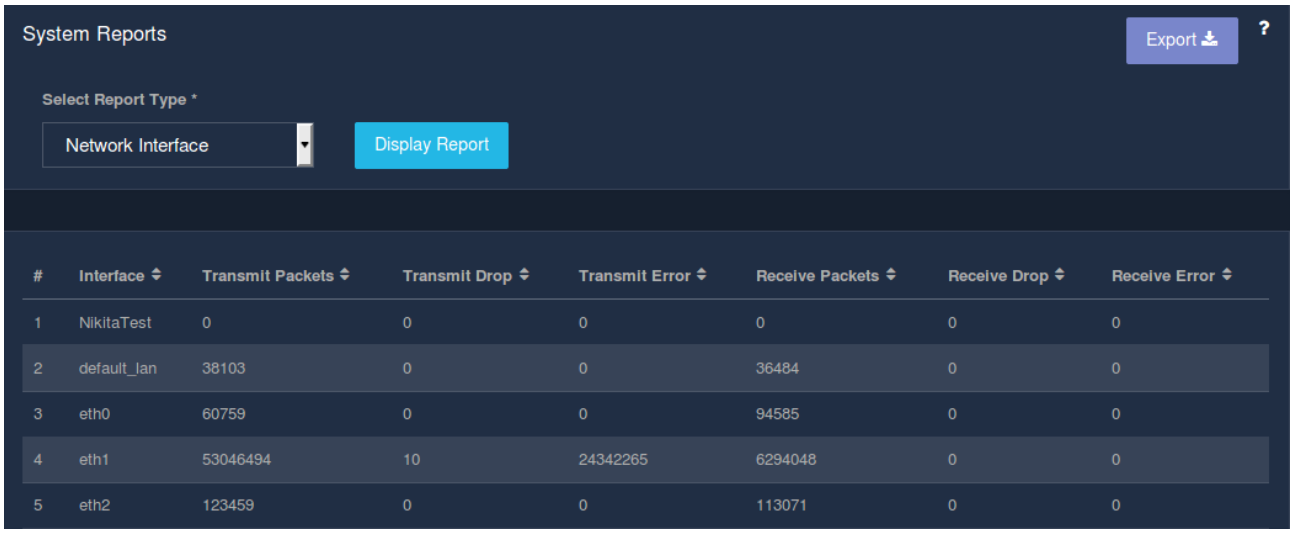
This page displays the list of ports opened in Unibox at a given time. It displays the list of all System IP addresses along with its open Source and Destination ports. Use refresh button to get the latest status. You can click on the '**+**' button against each IP Address to get the list of Source and Destination Ports opened. It allows to display the list by entering the IP address and the port.



Fig

8.4.3 Network Interface

This report displays the information for each network interface. Each row displays data for a physical or virtual network interface. The list displays each of the interface names along with the transmit and the receive section. The transmit section displays the total number of packets sent, dropped or had erred. The receive section displays the number of packets received, dropped or had erred.



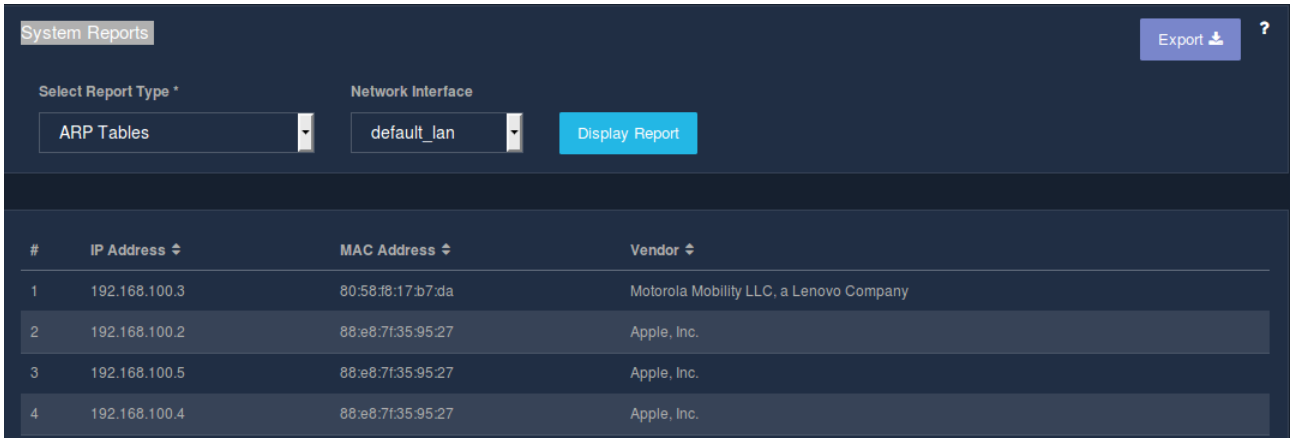
Fig

8.4.4 ARP Tables

This report displays the ARP (Address Resolution Protocol) table of Unibox. The ARP table is used to find all the clients in the network.

On initiating a scan, Unibox will send an ARP request to all the IP addresses in the subnet and will listen for a response from the clients. To display the ARP table list, select one of the network interface. It will build the table on receiving the responses or timing out. The table displays the IP Address,MAC Address and the name of the vendor.

Please note that this table takes some time to load.



Fig

8.4.5 System Usage Graph

This page displays various system related reports over a 24 hour period. The reports are displayed in a graphical format with time on X-axis and value on Y-axis.

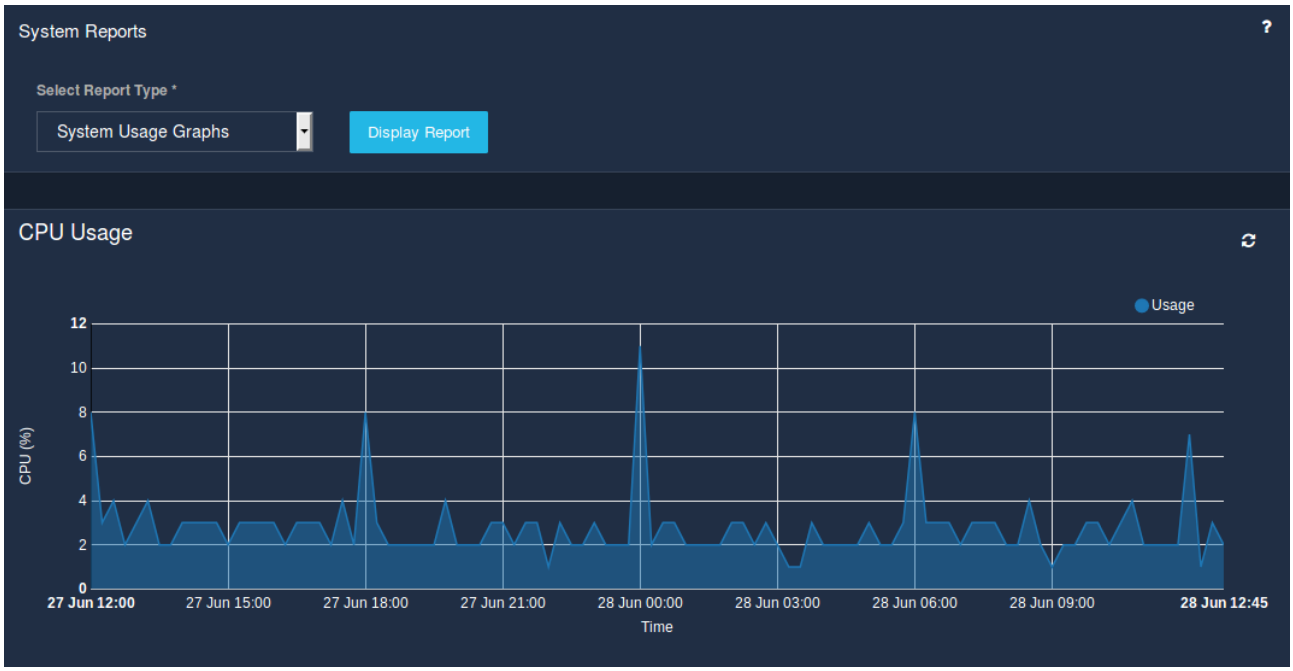
CPU Usage - Displays CPU usage over the given time period.

Memory Usage - Memory usage by Unibox over given time period.

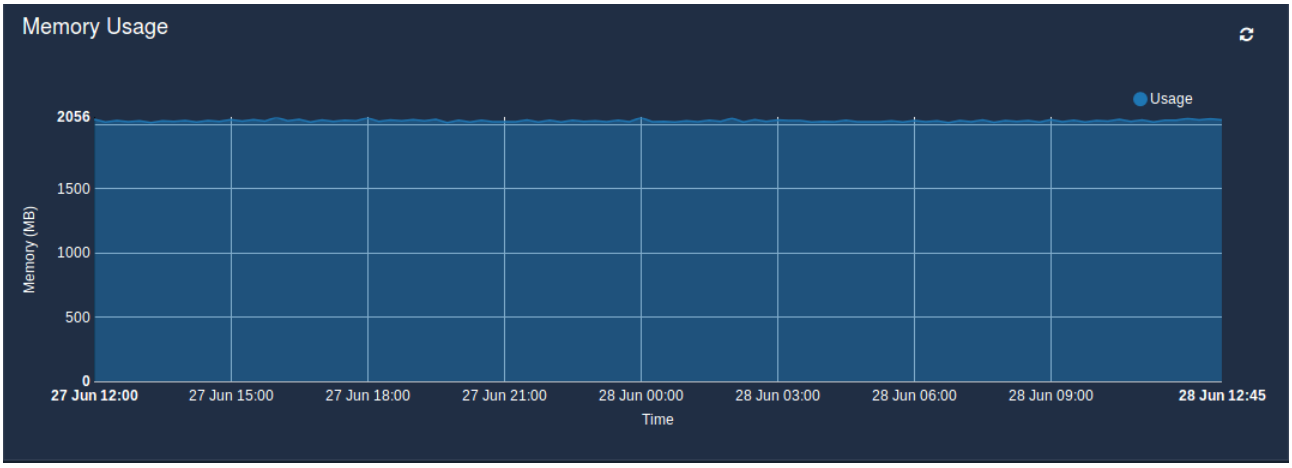
Disk Usage - Disk space usage by Unibox over given time period.

Ports Usage - Displays source and destination ports used on Unibox.

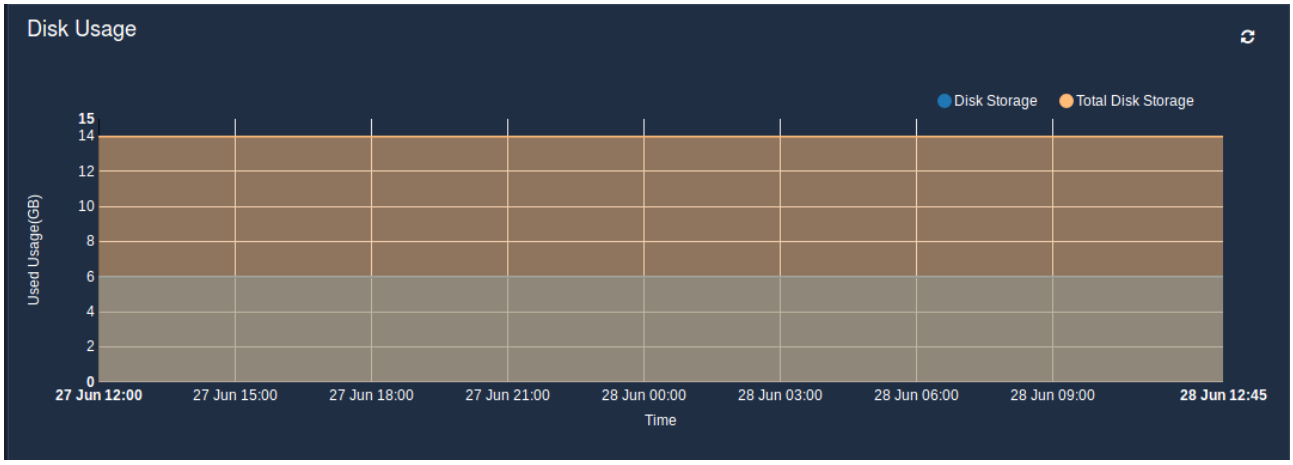
Unibox will take 24 hour time period from the current system time. The graph will progress forward automatically when displayed on the screen.



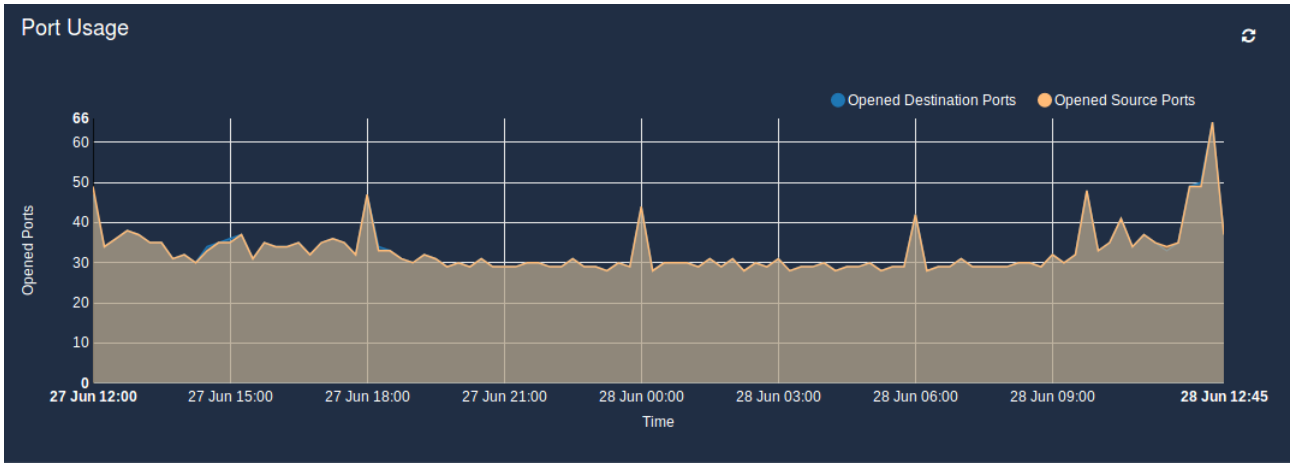
Fig



Fig



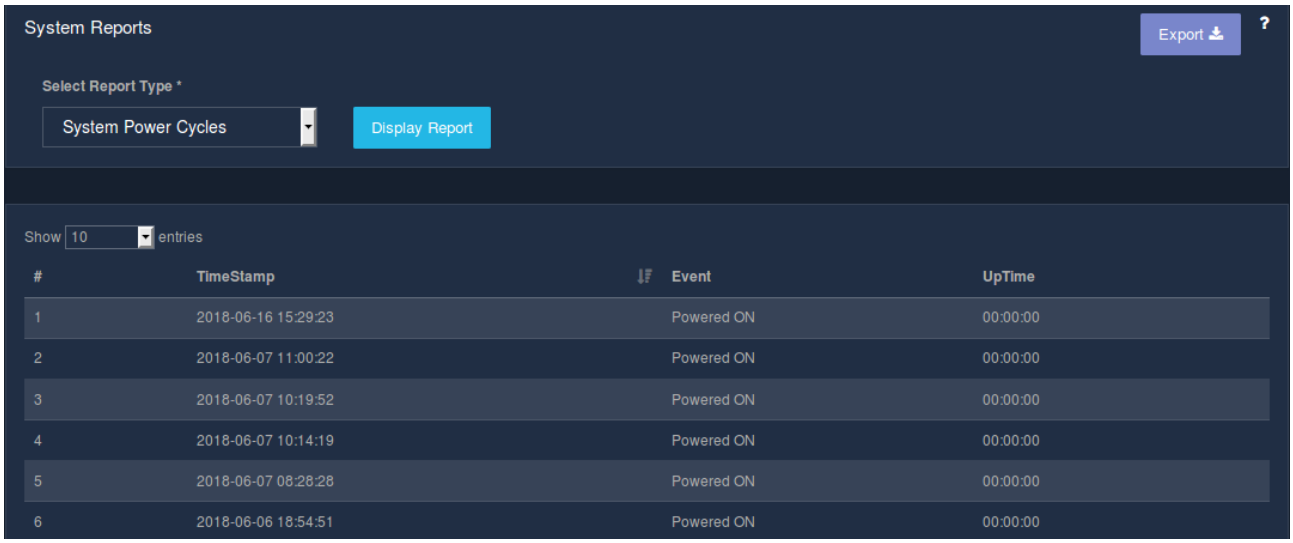
Fig



Fig

8.4.6 System Power Cycles

This page shows the power cycle history of the system. Every clean Power OFF/ON sequence of the system is marked and counted against Powered OFF/ON event. The list displays the timestamp, event and the Uptime of the system.



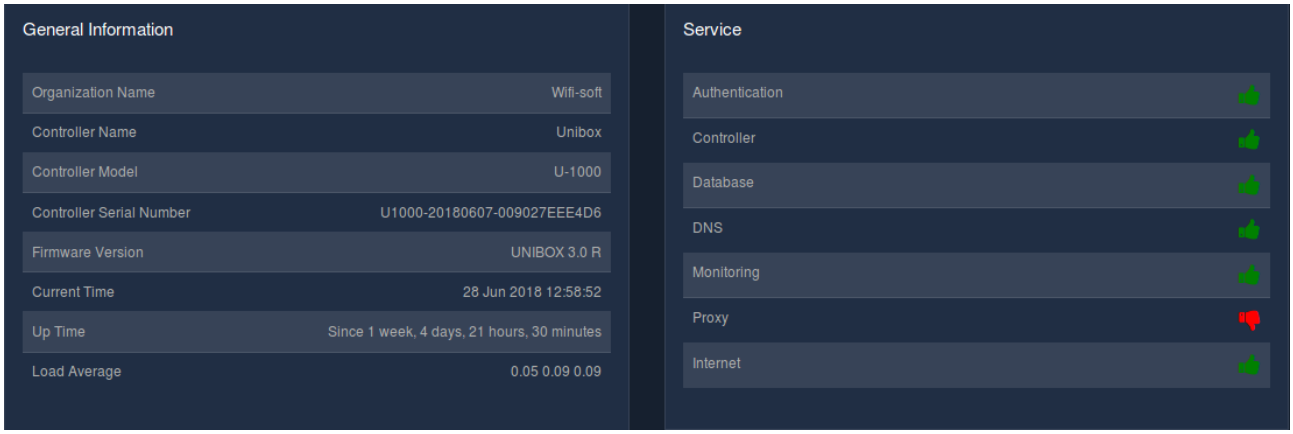
Fig

8.4.7 System Information

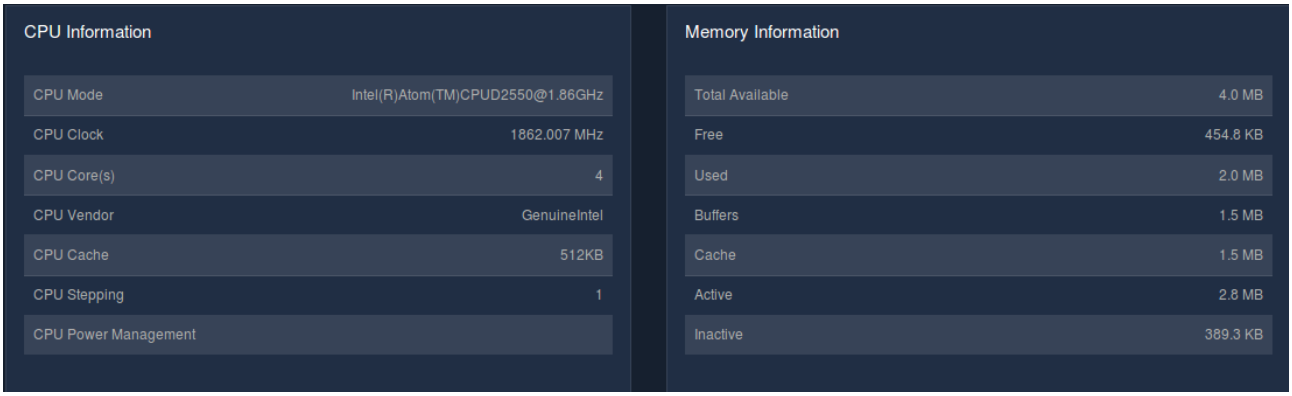
This page displays the important details like CPU/Memory/Storage/Services information on the System.

The following details are displayed:

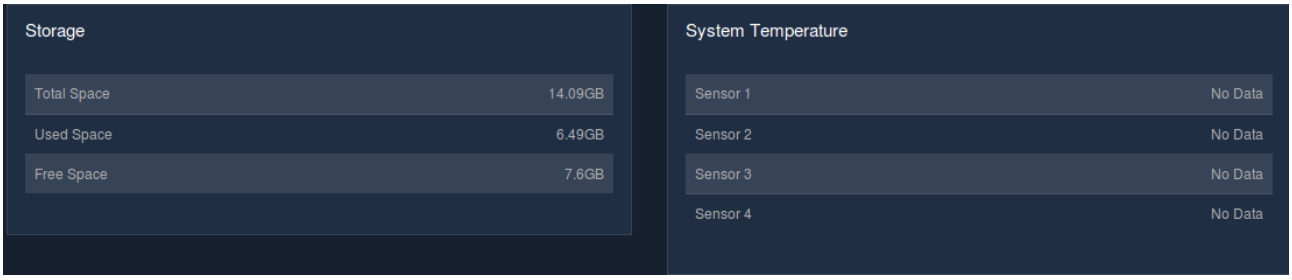
- General Information: Name of controller, firmware version, uptime, etc.
- Network Information: LAN and WAN IP, DNS server, IP connections.
- Services: Various services running on the controller.
- CPU Information: Information about Unibox CPU.
- Memory Information: Displays the RAM Memory usage on Unibox.
- Storage Information: Displays the Secondary Storage usage information.
- System temperature: Data about different sensors.


General Information
Organization Name
Wifi-soft
Controller Name
Unibox
Controller Model
U-1000
Controller Serial Number
U1000-20180607-009027EEE4D6
Firmware Version
UNIBOX 3.0 R
Current Time
28 Jun 2018 12:58:52
Up Time
Since 1 week, 4 days, 21 hours, 30 minutes
Load Average
0.05 0.09 0.09
Service
Authentication
Controller
Database
DNS
Monitoring
Proxy
Internet

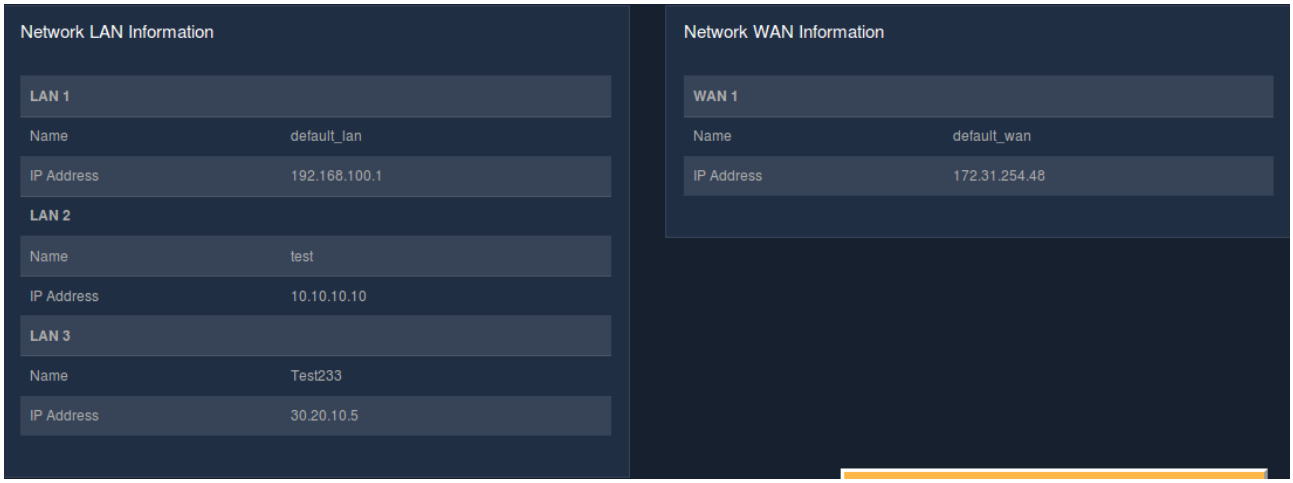
Fig


CPU Information
CPU Mode
Intel(R)Atom(TM)CPUD2550@1.86GHz
CPU Clock
1862.007 MHz
CPU Core(s)
4
CPU Vendor
GenuineIntel
CPU Cache
512KB
CPU Stepping
1
CPU Power Management
Memory Information
Total Available
4.0 MB
Free
454.8 KB
Used
2.0 MB
Buffers
1.5 MB
Cache
1.5 MB
Active
2.8 MB
Inactive
389.3 KB

Fig


Storage
Total Space
14.09GB
Used Space
6.49GB
Free Space
7.6GB
System Temperature
Sensor 1
No Data
Sensor 2
No Data
Sensor 3
No Data
Sensor 4
No Data

Fig



Fig

8.5 Usage

8.5.1 Usage Graphs

This page displays the Local bandwidth graph, ISP bandwidth graph, Packets downloaded/Uploaded graph and online Users.

This page displays various usage related reports over a 24 hour period. The reports are displayed in a graphical format with time on X-axis and value on Y-axis.

Local Bandwidth: Displays Local bandwidth over given time period.

ISP Bandwidth: Displays ISP bandwidth over given time period.

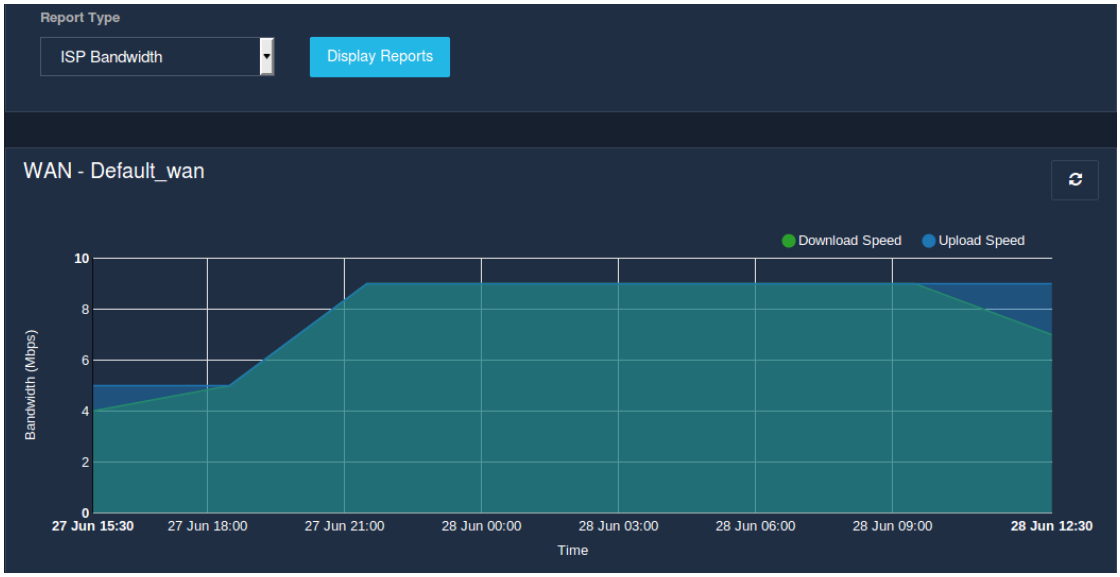
Packets: Displays Packets downloaded and uploaded on Unibox.

Users: Displays Online users.

Unibox will take 24 hour time period from the current system time. The graph will progress forward automatically when displayed on the screen.

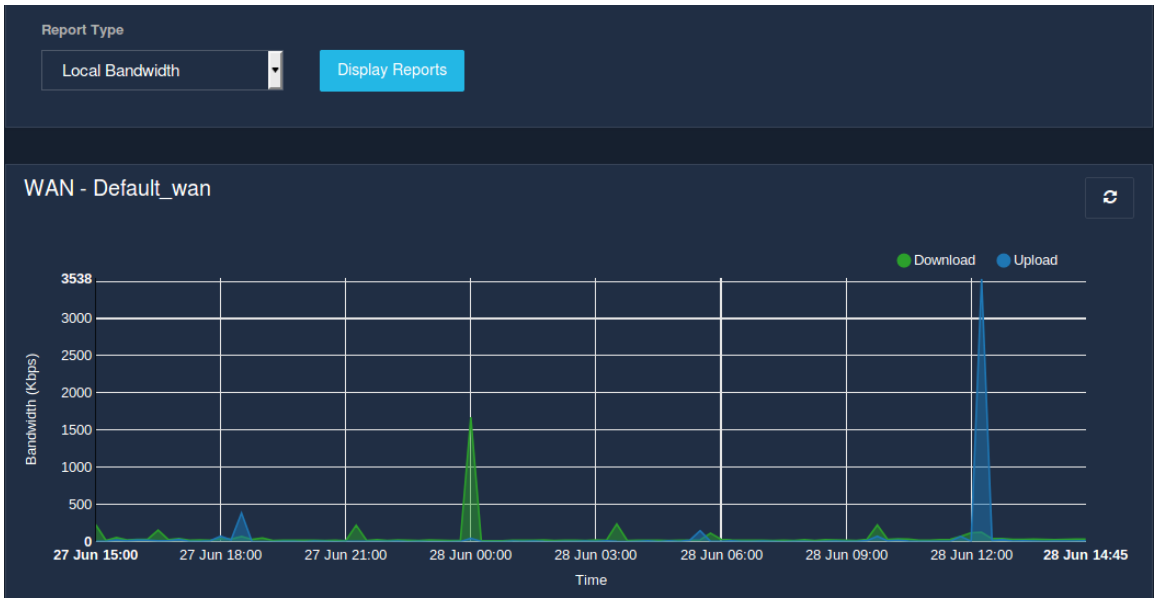
The area graphs displayed would be completely based on the report type selected.

Report Type is ISP Bandwidth:

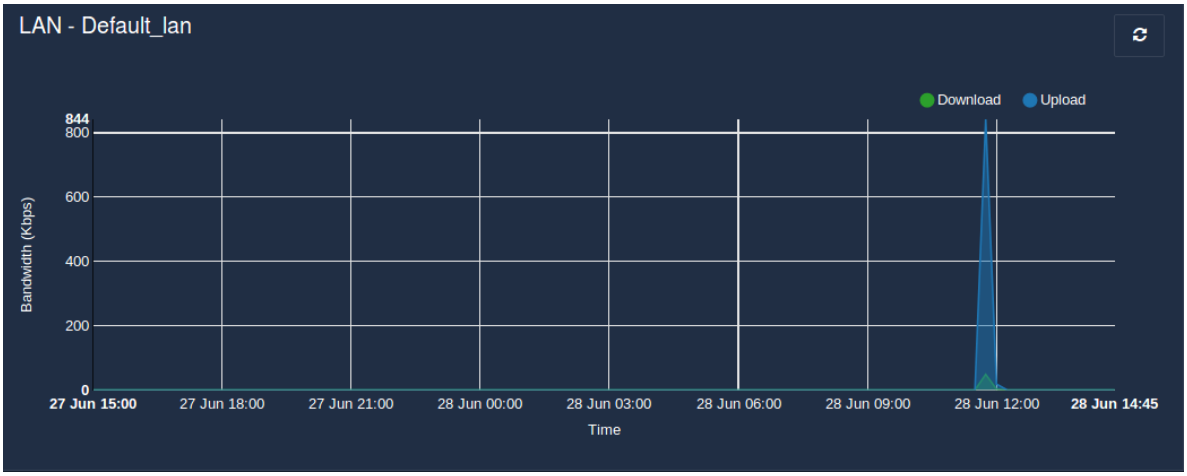


Fig

Report Type is Local Bandwidth

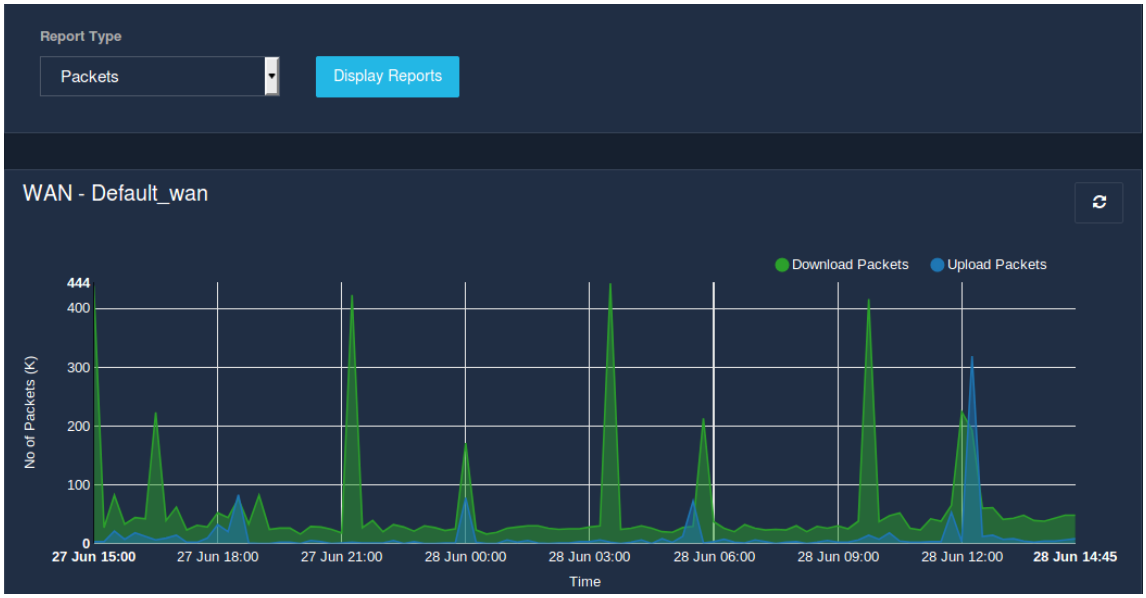


Fig



Fig

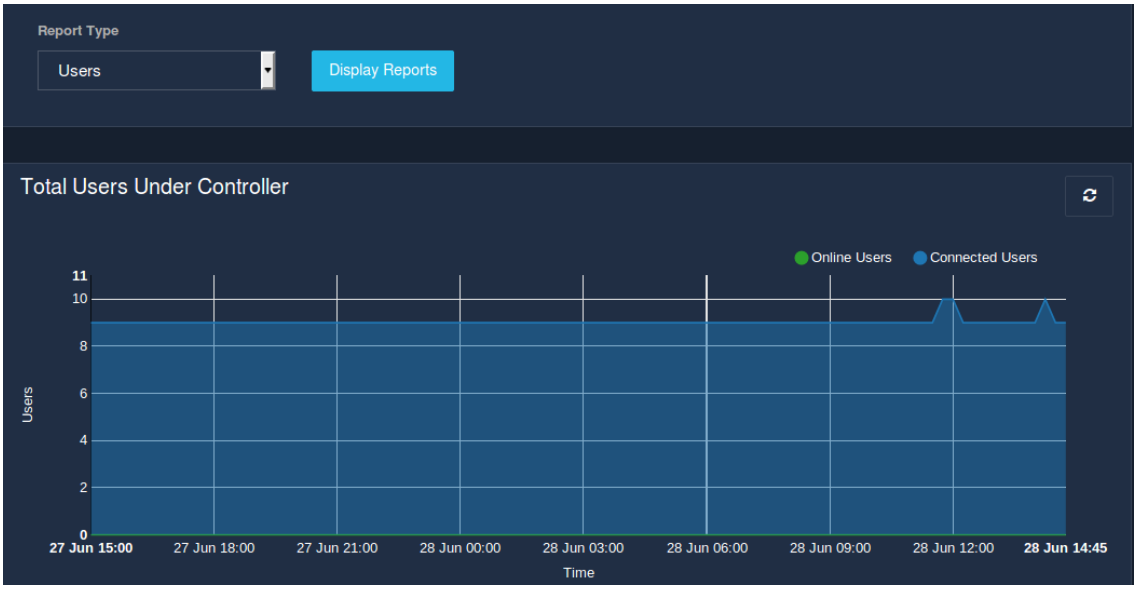
Report Type is Packets:



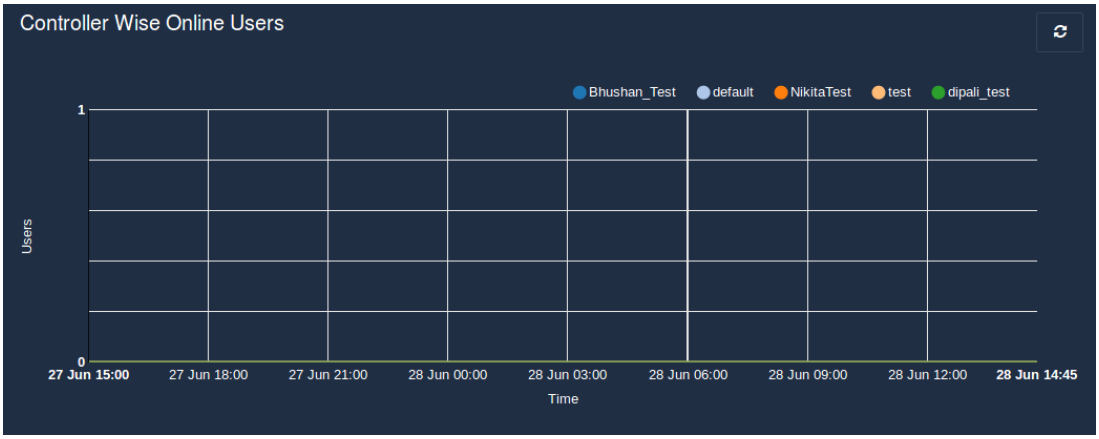
Fig

Fig

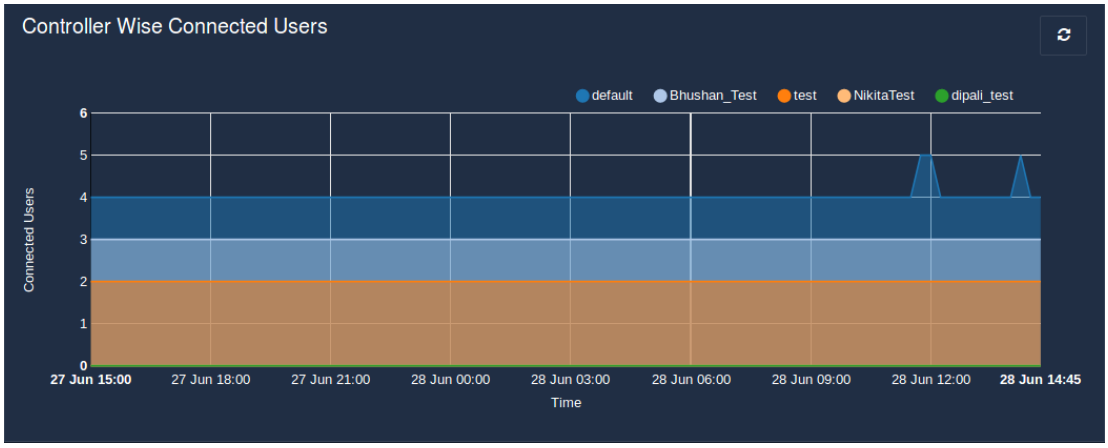
Report Type is Users:



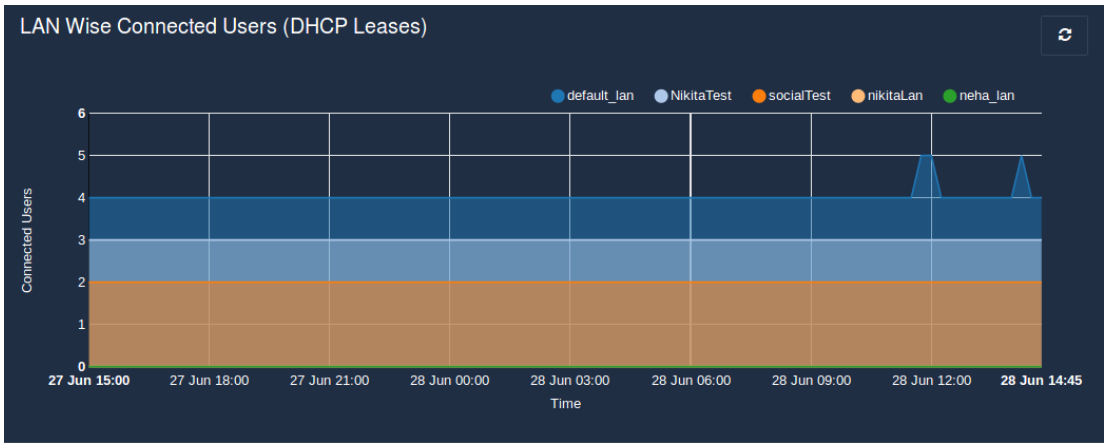
Fig



Fig



Fig



Fig

8.5.2 Usage Summary

This page displays various usage reports based on the session information. Following types of reports can be generated-

1. Total Session Vs Time: Display the total number of user sessions over a given time period.

2. Number of Sessions Vs. Days of Week: Display total number of sessions for a given day of the week. If the day occurs more than once during the given time period, then the sessions are added up for that day.

3. Number of Sessions Vs. Hour of the Day: Display the total number of sessions for a given hour of the day. All the sessions are added up for the given hour during the given time period.

4. Bandwidth Usage Vs. Time : Display the bandwidth usage over a given time period.

5. Top Users : Displays the total sessions, upload, download of the particular users.

The time interval defines the date range for the report. The administrator can choose any date range using the calendar icon. The time unit defines the unit of time (granularity of the report).

Moreover the administrator can select whether she/he wants to view the report in tabular or graphical format for a specific report type selected.

To display a usage summary report click on the 'Display report' button. The columns in the report would vary based on the report type selected.

8.5.2.1 Export Usage Summary Report

This section allows an administrator to export various usage reports based on the session information. Each of these reports would differ based on the report type selected. The report is exported in csv format file. To download a report, click on the 'Export' button provided.

8.5.3 ISP Bandwidth Usage

This page displays various bandwidth usage related reports over a time period. The search field allows to perform the search operation on the required column. The table displaying the ISP bandwidth usage is listed in the following order:

Time : Displays timestamp at which bandwidth details collected.

Public IP: Displays Public IP (with ISP Provider's name).

Speed Test Peer: Displays peer server details where speed test carried out.

Residual Upload Speed: Displays upload speed of residual ISP bandwidth.

Residual Download Speed: Displays download speed of residual ISP bandwidth.

WAN Upload Speed: Displays upload speed of Unibox WAN interface.

WAN Download Speed: Displays download speed of Unibox WAN interface.


ISP Bandwidth Usage

Show 10 entries

Search:

#	Time	Public IP	Speed Test Peer	Residual Upload Speed	Residual Download Speed	WAN Upload Speed	WAN Download Speed
1	28/06/2018 12:30:01	123.136.169.228	YOU Broadband India Pvt. Ltd Pune India	9.31 Mbps	7.29 Mbps	9.69 Mbps	9.69 Mbps
2	28/06/2018 09:30:01	123.136.169.228	YOU Broadband India Pvt. Ltd Pune India	9.81 Mbps	9.23 Mbps	10.17 Mbps	10.17 Mbps
3	28/06/2018 06:30:01	123.136.169.228	YOU Broadband India Pvt. Ltd Pune India	9.95 Mbps	9.33 Mbps	10.25 Mbps	10.25 Mbps
4	28/06/2018 03:30:01	123.136.169.228	YOU Broadband India Pvt. Ltd Pune India	9.73 Mbps	9.34 Mbps	10.10 Mbps	10.10 Mbps
5	28/06/2018 00:30:01	123.136.169.228	YOU Broadband India Pvt. Ltd Pune India	9.99 Mbps	9.23 Mbps	10.26 Mbps	10.26 Mbps
6	27/06/2018 21:30:01	123.136.169.228	ICC Netspeed Pune India	9.90 Mbps	9.26 Mbps	10.21 Mbps	10.21 Mbps

Fig

8.6 Billing

8.6.1 Revenue Report

This page displays various revenue reports based on revenue information.

Revenue reports are of the following types :-

1. Prepaid Revenue Report: Displays total prepaid revenue for given time interval.

2. Credit Card Revenue Report: Displays total credit card revenue for a given time interval.

3. Total Revenue Report: Displays the prepaid revenue , credit card revenue and the total revenue.

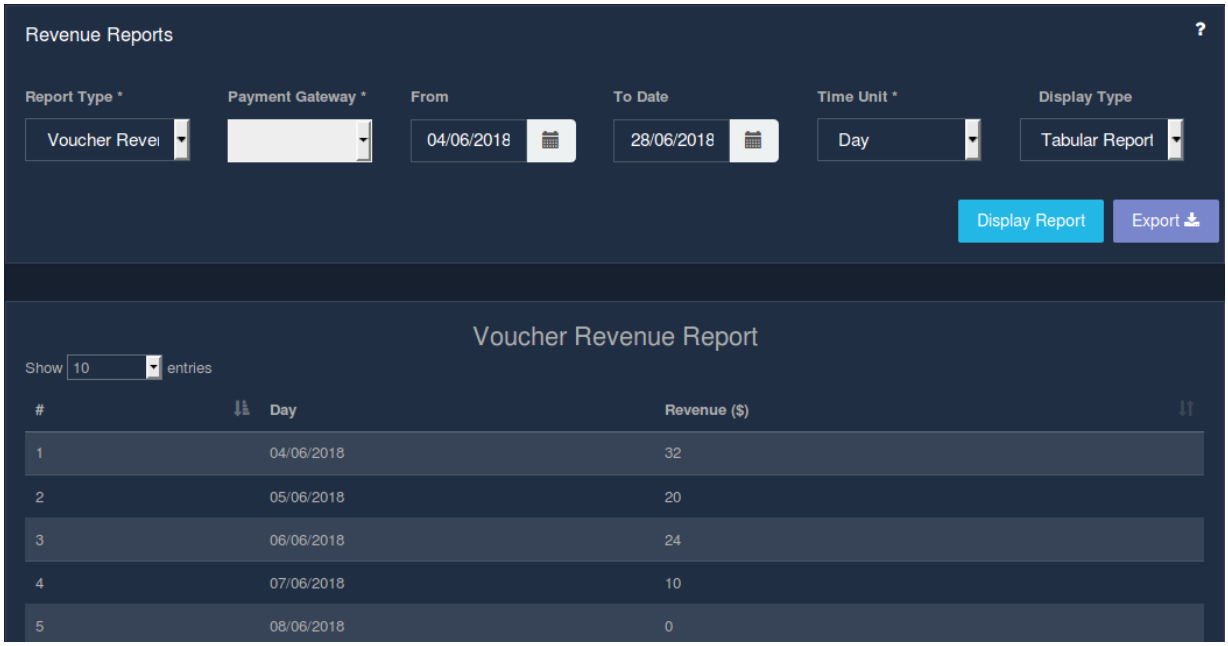
The time interval defines the date range for the report. The administrator can choose any date range using the calendar icon. The time unit defines the unit of time (granularity of the report).

Moreover the administrator can select whether she/he wants to view the report in tabular or graphical format. The payment gateway selection is also provided.

The Plan Revenue report type has a dependency on the payment gateway. So whenever the report type selected is Plan revenue, it prompts for the payment gateway selection. The report displayed varies based on the time unit selection.

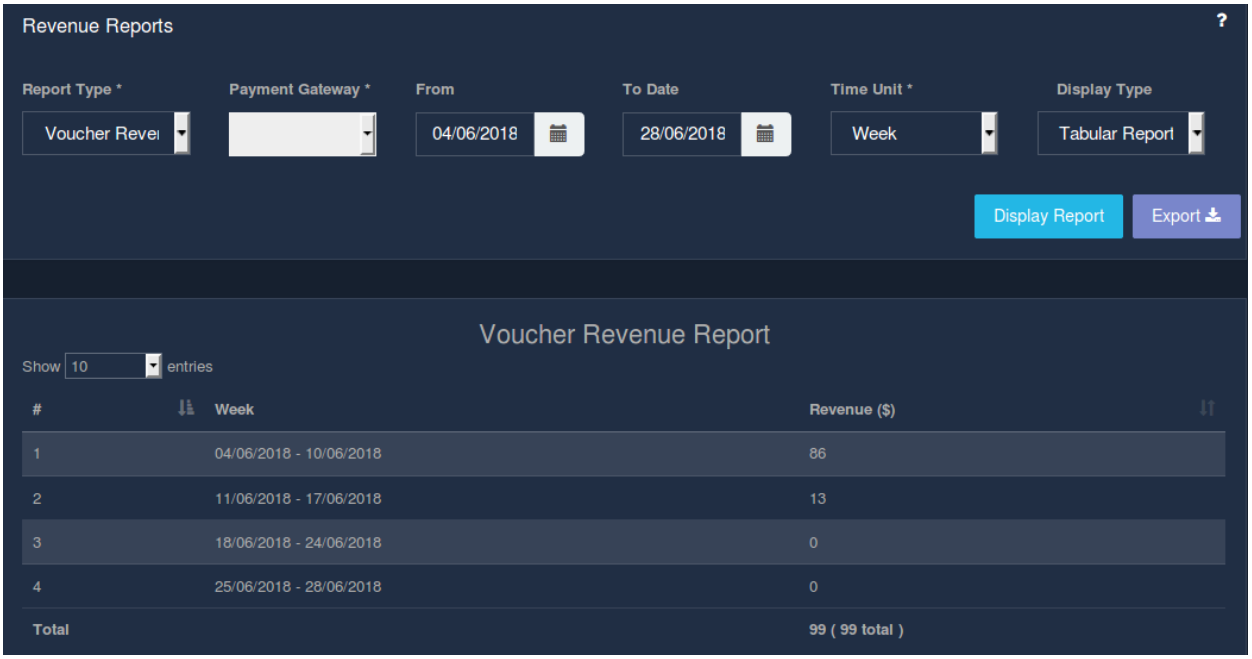
To display the revenue report, click on the 'Display Report' button.

When the time unit is, a day, report is displayed as:

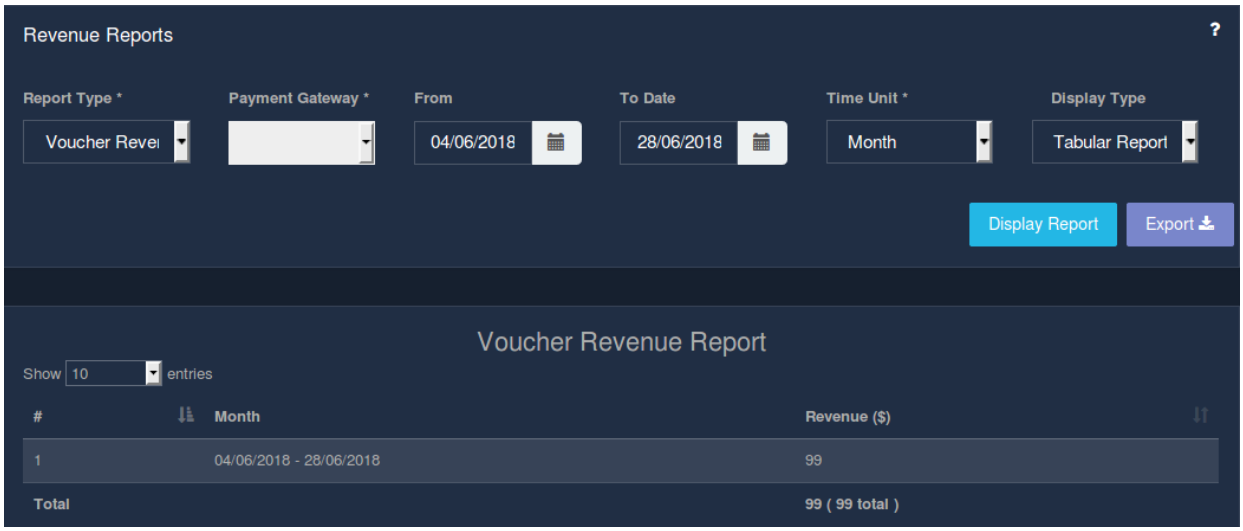


Fig

Time Unit is Week:



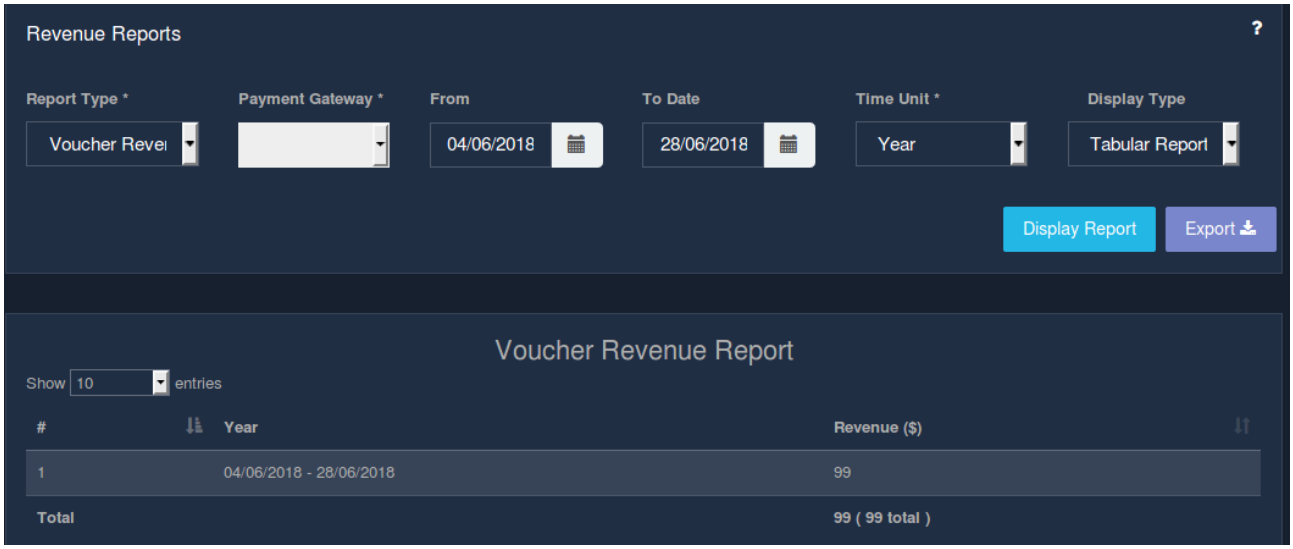
Fig



Fig

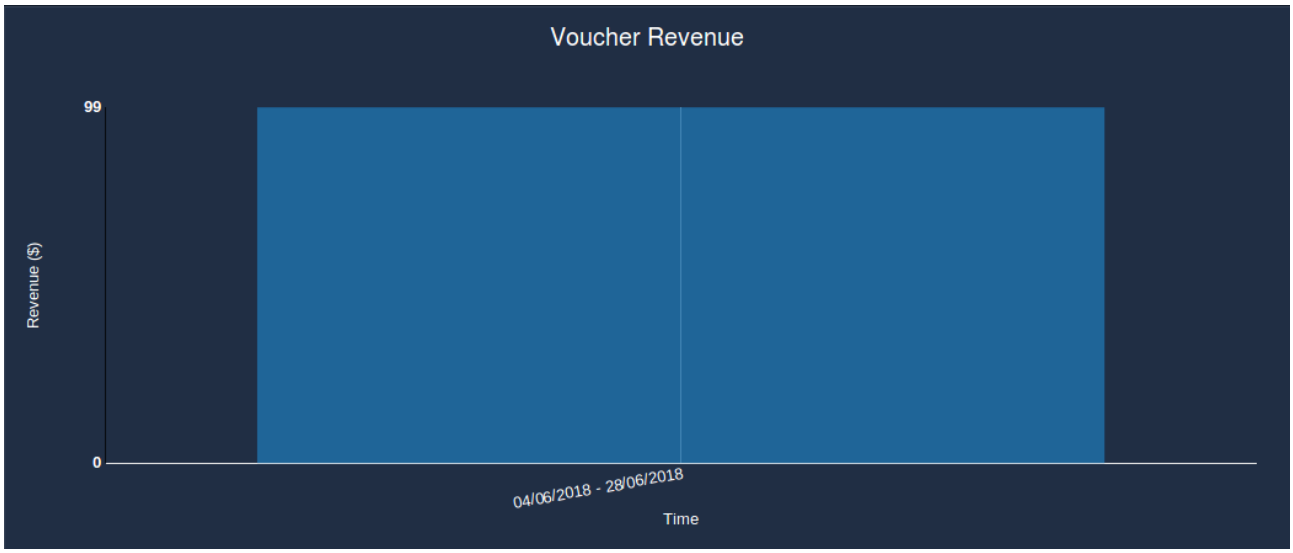
Time Unit is Month:

Time Unit:



Fig

The above screenshots were displayed in the tabular format. But when the display type is selected as graphical, the report is displayed as:



Fig

Fields	***Description***
Report Type	Select the type of report.
Payment Gateway	Select the payment gateway.
From Date	Select From which date the revenue report should be exported.
To Date	Select till which date the revenue report should be exported.
Time Unit	Select the time unit. (day,week,months,year)
Display Type	Select the type in which the report should be displayed (graphical, tabular)

Table

8.6.1.1 Export Revenue Report

This section allows an administrator to export the revenue report based on the date. To export a revenue report, click on the 'Export' button. A csv file would then be downloaded to your local machine.

The CSV file exported follows the format:

- Date
- Revenue

8.6.2 Revenue by Plan

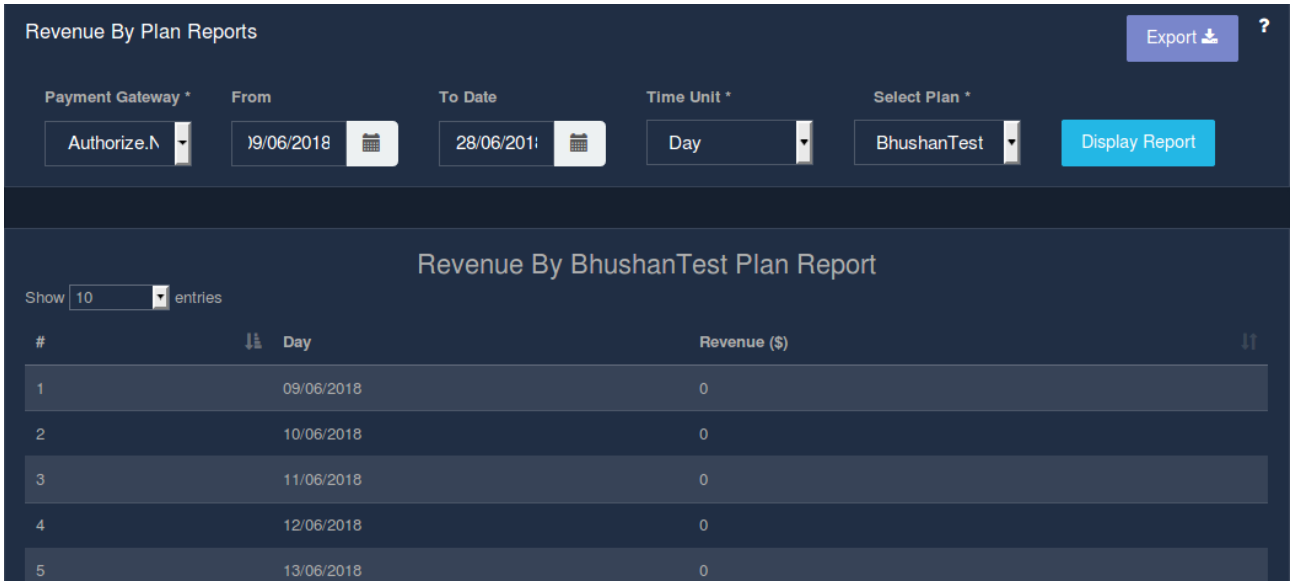
This page displays the revenue report by plan over a given time period. The report displays the revenue generated based on billing plans. The administrator needs to select the payment gateway, time interval, time unit and the plan to generate the report in tabular format.

The time unit will decide the granularity of the report. To display a revenue report, click on the 'Display Report' button.

The report displayed is listed in two columns. Column1 representing the date and column2 showing the revenue generated.

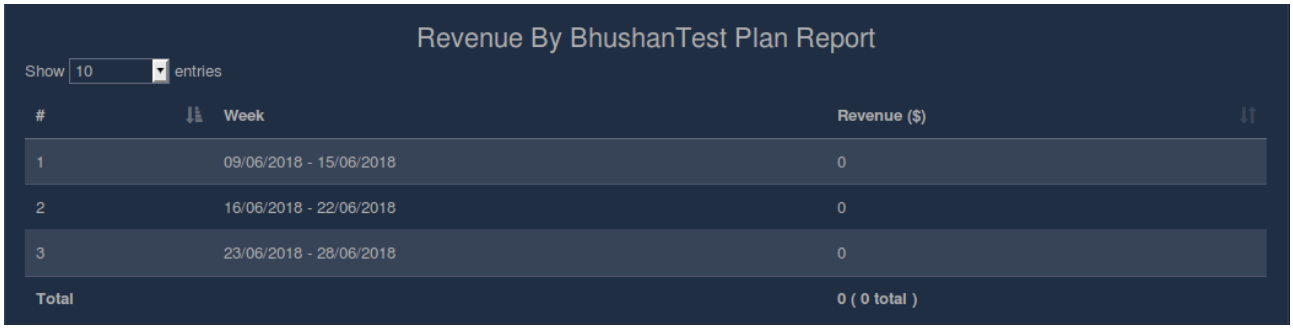
The report is displayed based on the payment gateway selected, the time interval, time unit and the plan selected. The report displayed varies based on the time unit selection.

When the time unit is, a day, the report is displayed as:



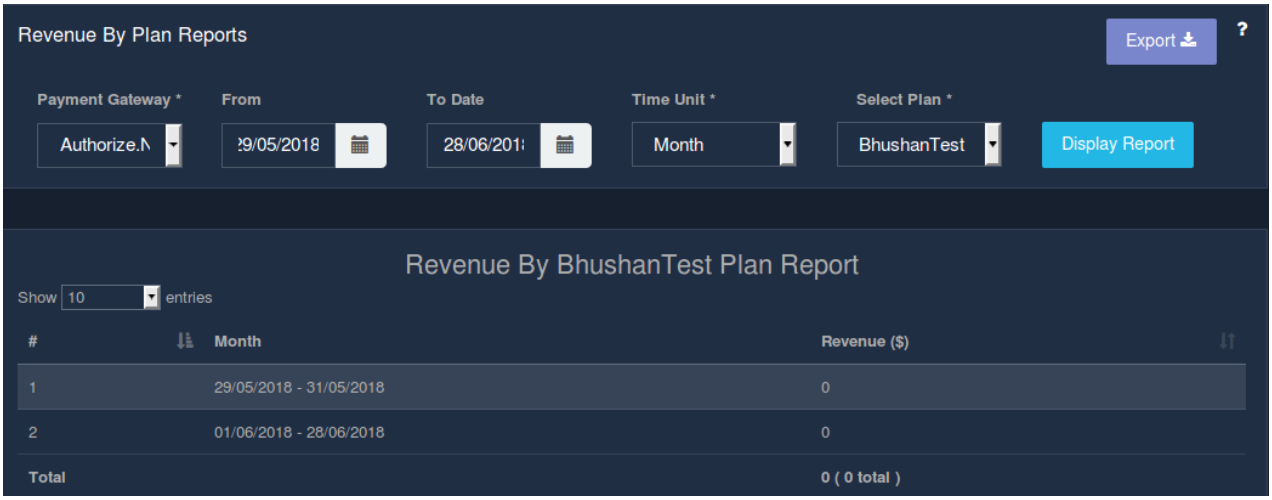
Fig

Time unit is week:



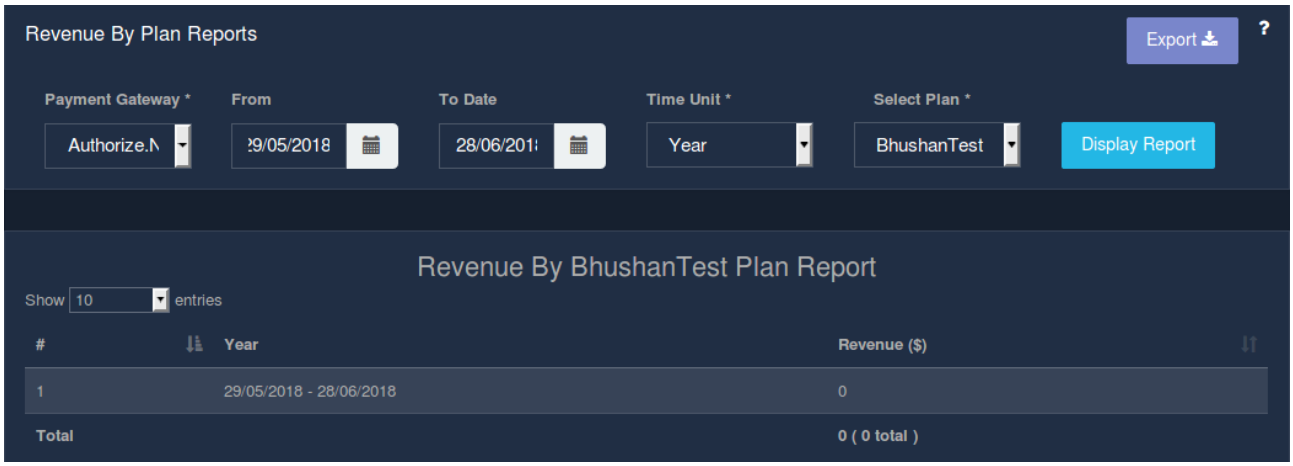
Fig

Time Unit is month:



Fig

Time Unit is Year:



Fig

8.6.2.1 Export Revenue Report

This section allows an administrator to export the revenue report based on the plan. To export a revenue report, click on the 'Export' button. A csv file would then be downloaded to your local machine.

The CSV file exported follows the format:

- Date
- Revenue

8.6.3 Voucher Usage

This page displays the prepaid usage report over the given time interval. Following types of prepaid usage reports are displayed -

1. Voucher users Vs time

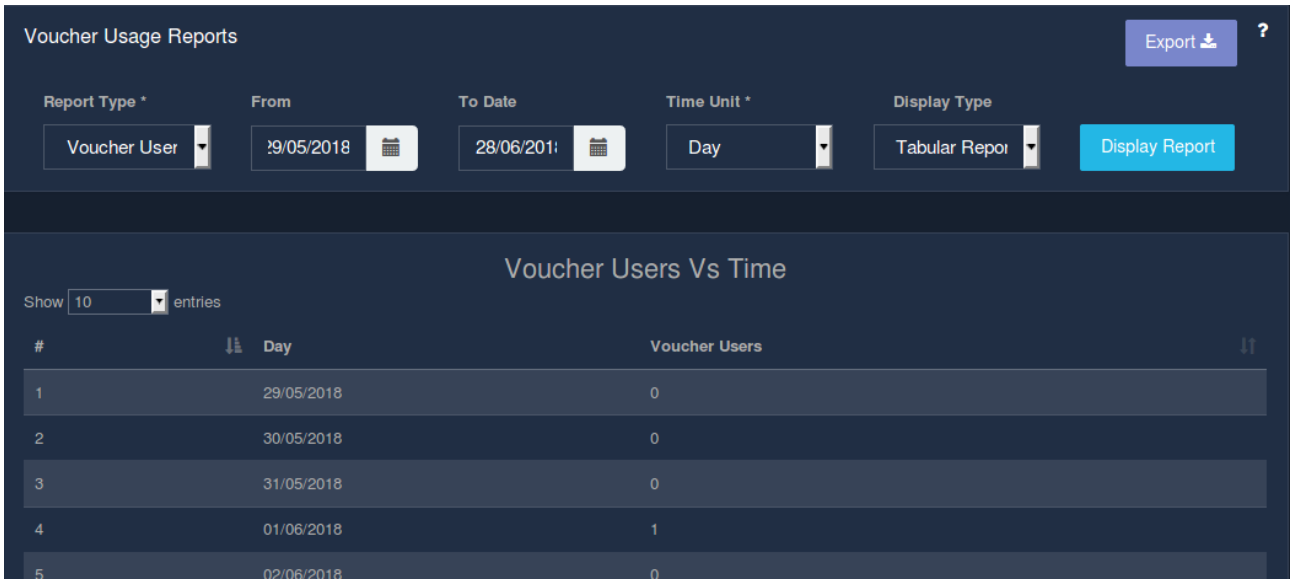
2. Voucher sessions Vs time

3. Total Time Used Vs time

Administrators can select on one of the reports along with the time interval and time unit to generate the report. All reports are displayed in a tabular format & graphical format. Click on the 'Display Report' button to generate a report.

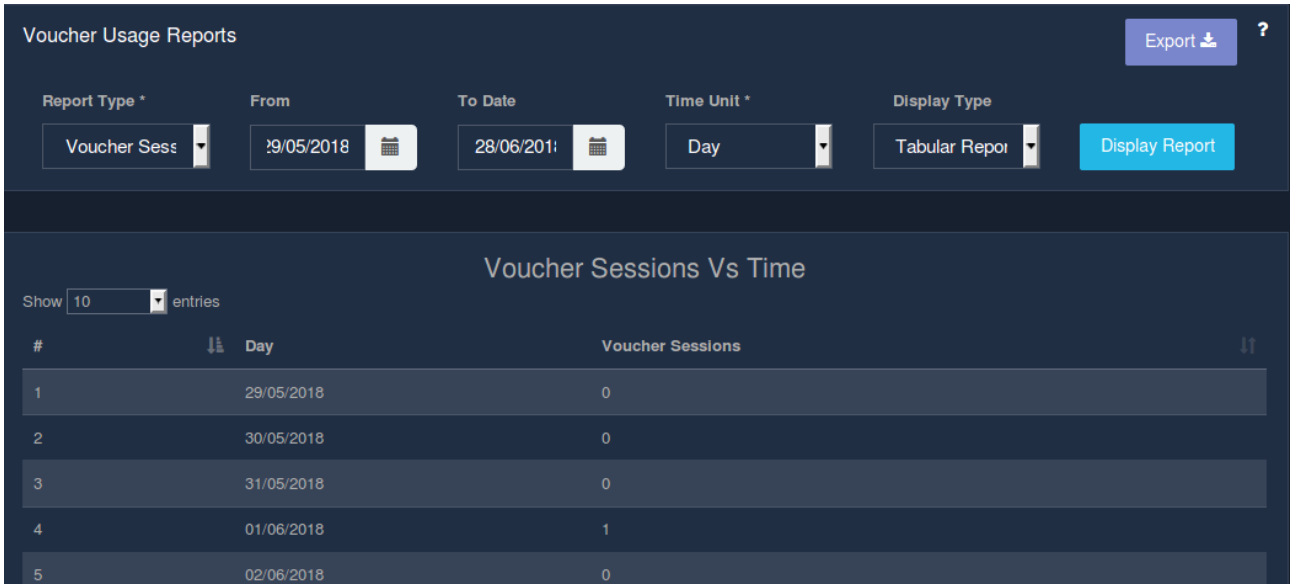
The report displayed differs based on the selection of report type and the time unit.

If the report type selected is Voucher users Vs time and the time unit is a day:



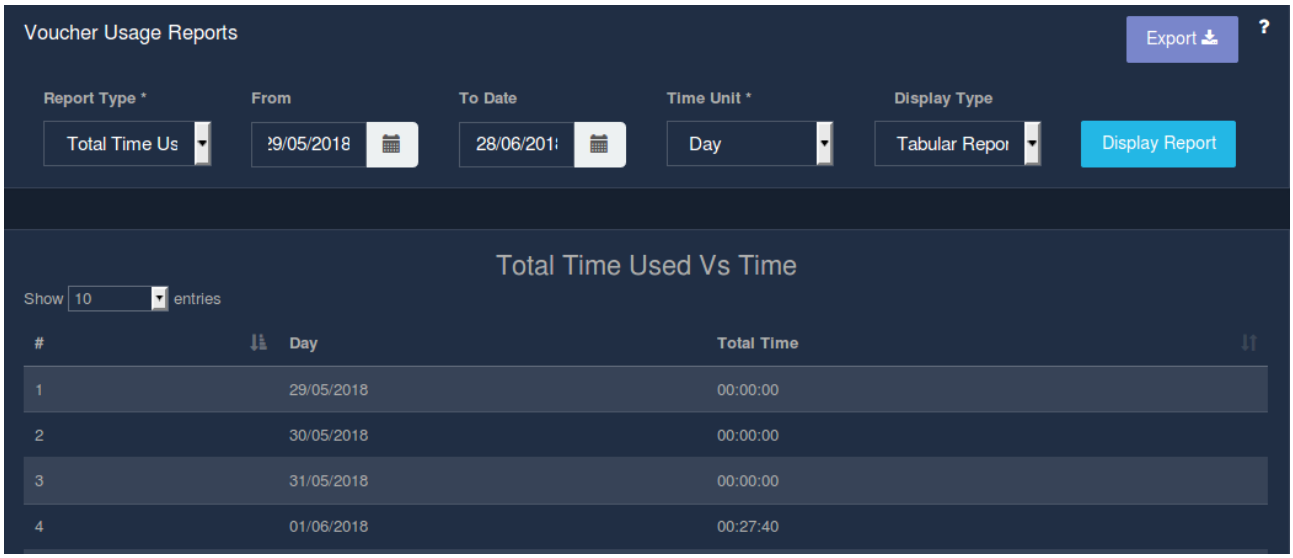
Fig

If the report type selected is Voucher sessions Vs time and the time unit is day:



Fig

If the report type selected is Total time Used Vs Time and the time unit is day:



Fig

8.6.3.1 Export Voucher Usage List

This section allows an administrator to export the voucher usage report over the given time interval. To export a voucher usage report,click on the 'Export' button. A csv file would then be downloaded to your local machine.

The CSV file exported follows the format:

- Date
- Revenue

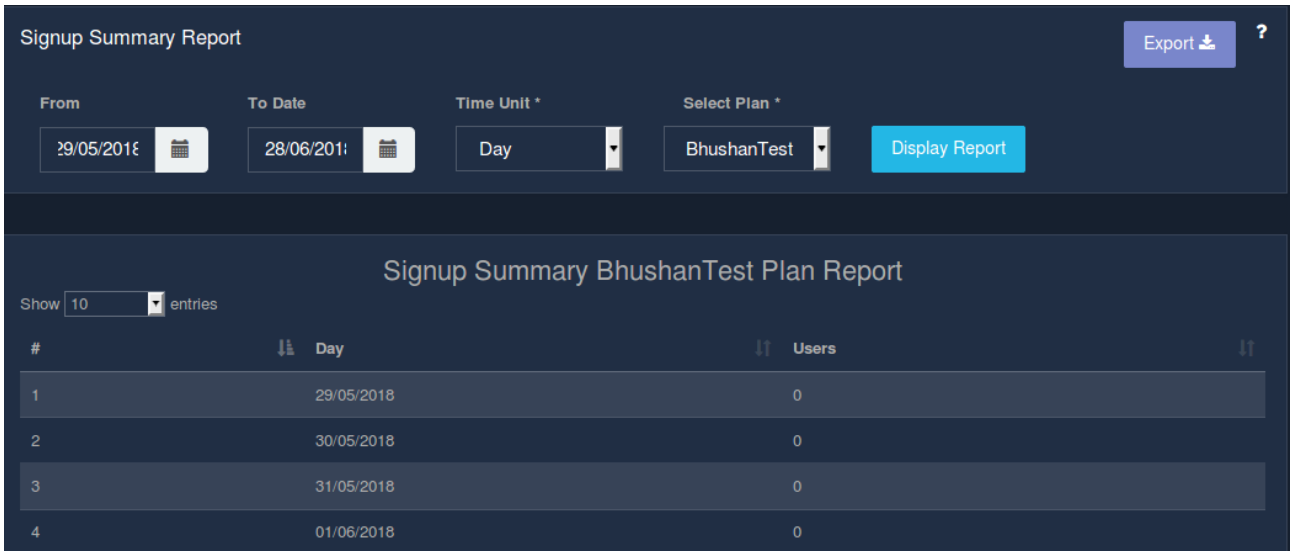
8.6.4 Signup Summary

This page displays the number of users signed up for the service using the Unibox registration interface for the given time period.

The tabular report displays the date, the total number of new users who signed up for the service using plans. It also displays the number of users who signed up for a specific plan over a given time period. The Signup summary report is displayed based on the time interval, time unit and the billing plan. To display the Signup summary report, click on the 'Display Report' button.

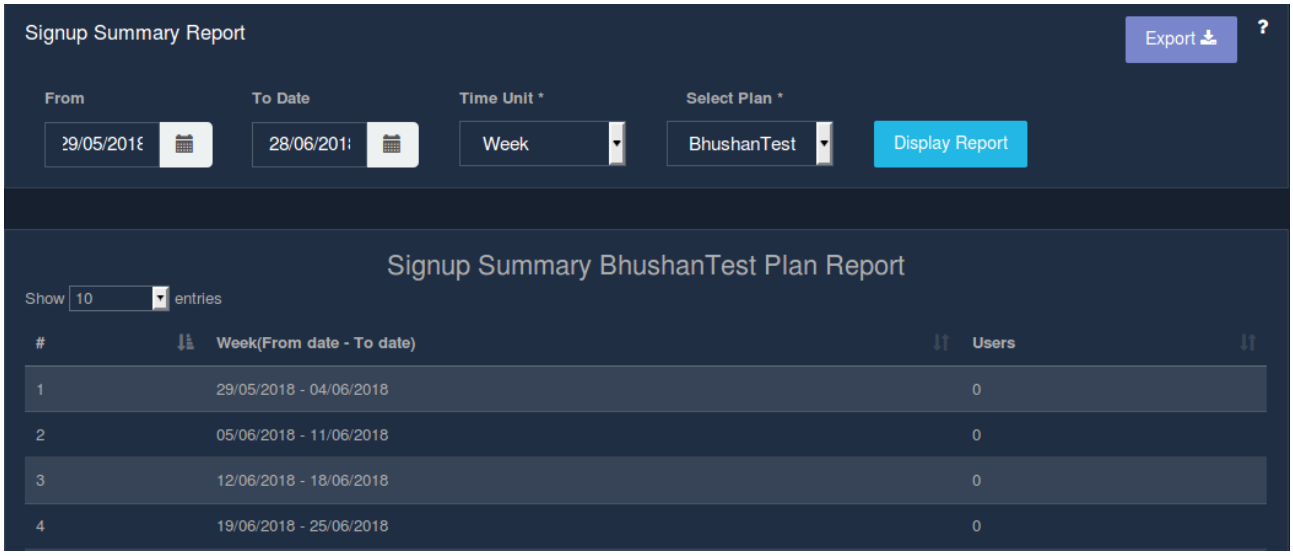
The report displayed differs based on the selection of the time unit.

If the time unit selected is day, report is displayed as:



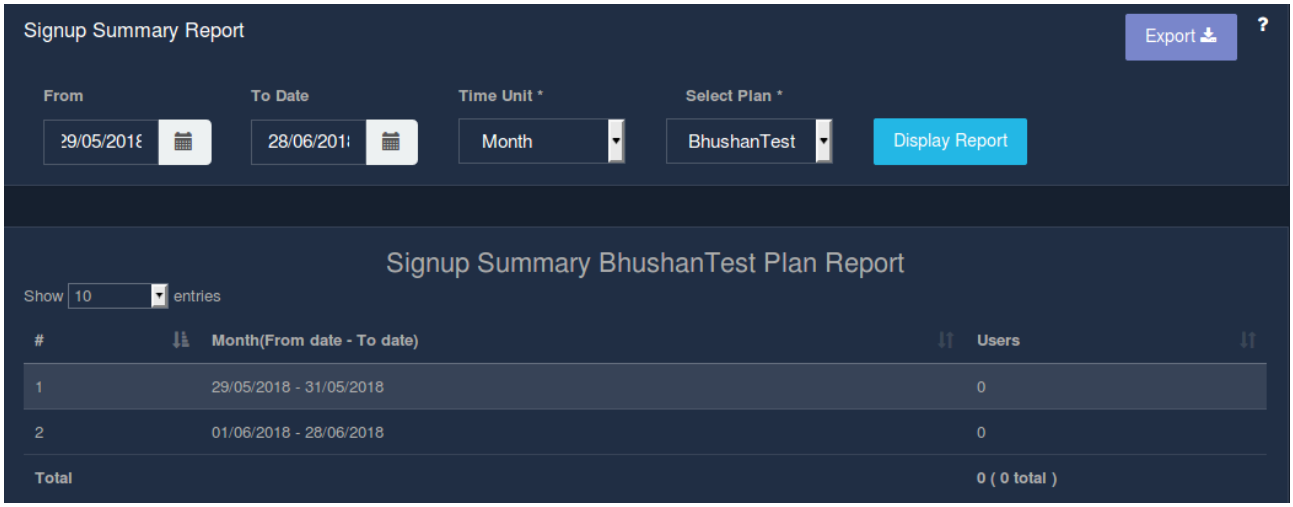
Fig

Time Unit is Week:



Fig

Time Unit is Month:



Fig

Time Unit is Year:

Fig

8.6.4.1 Export Signup Summary Report

This section allows an administrator to export the existing number of users signed up for the service using the Unibox registration interface from the database.

Click on the 'Export' button to download the Signup summary report on your local machine. A csv file is generated having the format as follows:

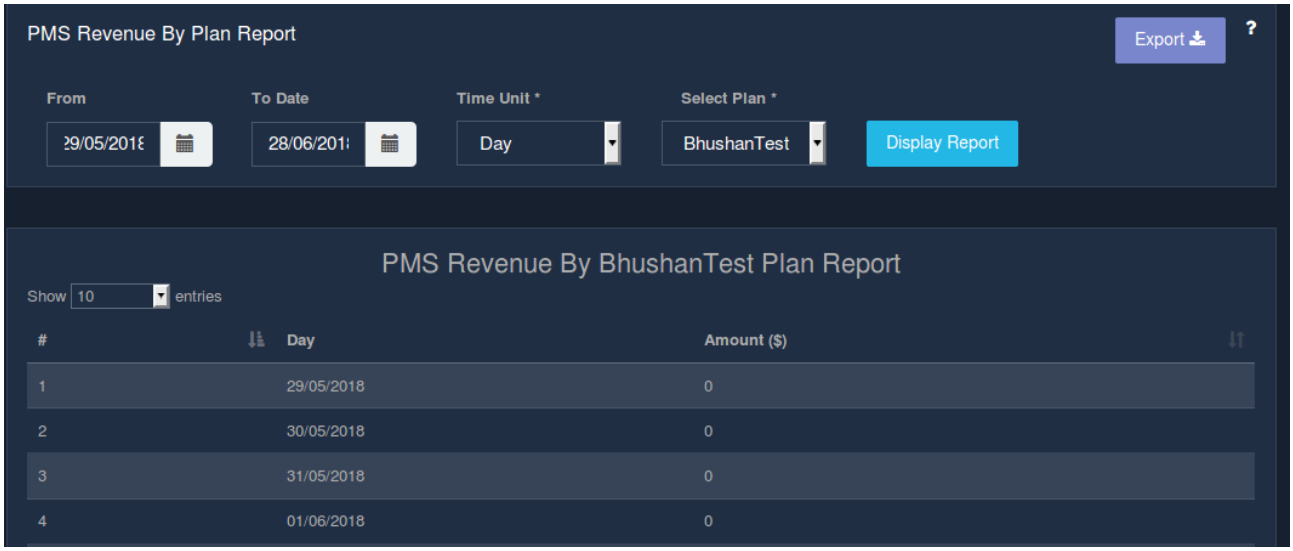
- Date
- User

8.6.5 PMS Revenue by Plan

This page displays the PMS revenue report generated by PMS based on billing plans over a given time period. The administrator needs to select the time interval, time unit and the plan to generate the report in tabular format. The time unit will decide the granularity of the report. The PMS revenue list displays the date and the amount.

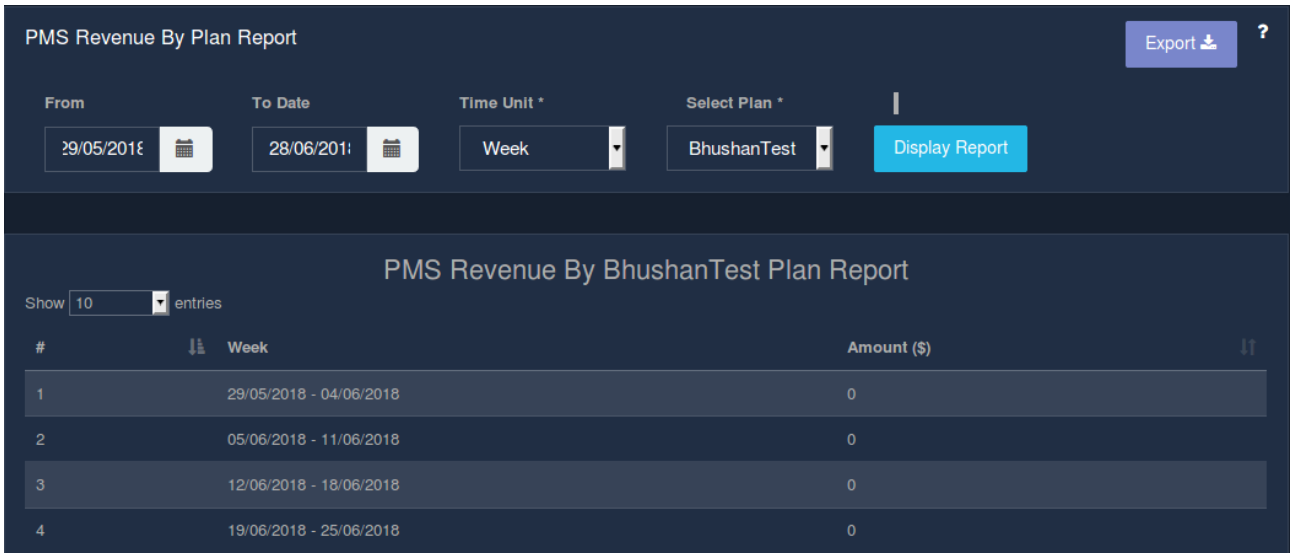
To display a PMS revenue report, click on the 'Display Report' button by selecting the time interval, time unit and the billing plan field.

If the time unit selected is, a day, then the report is displayed as:



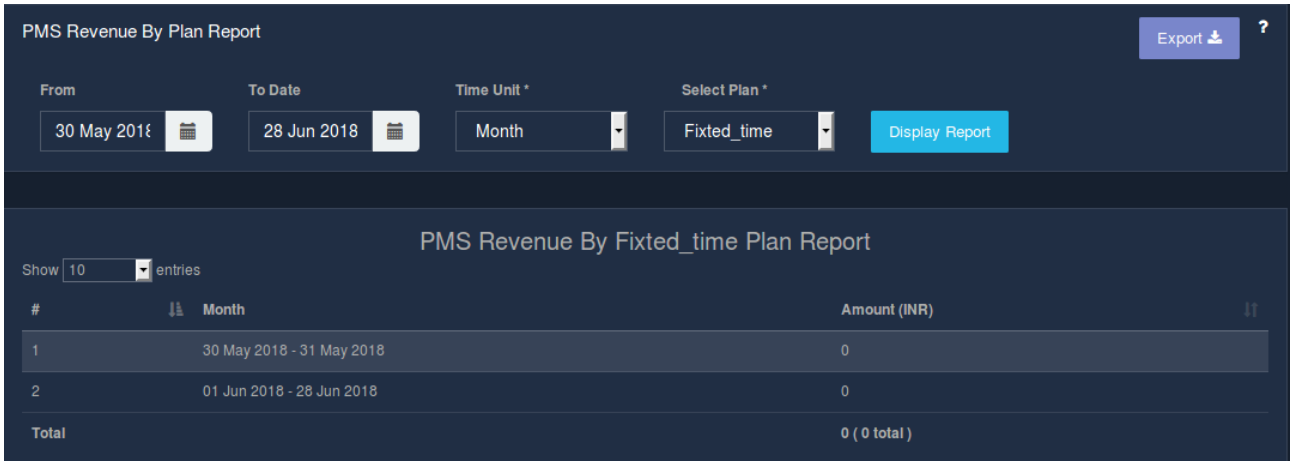
Fig

Time Unit is Week:



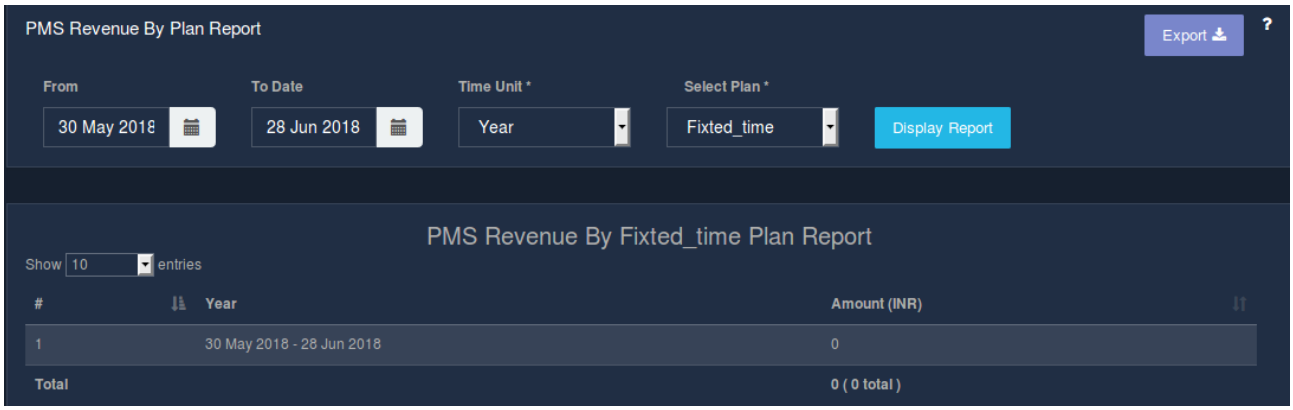
Fig

Time Unit is Month:



Fig

Time Unit is Year:



Fig

8.6.5.1 Export PMS Revenue by Plan Report

This section allows administrator to export the PMS revenue report over a given period of time. Click on the 'Export' button to download the signup summary report on your local machine

The CSV file exported follows the format:

- Date
- User

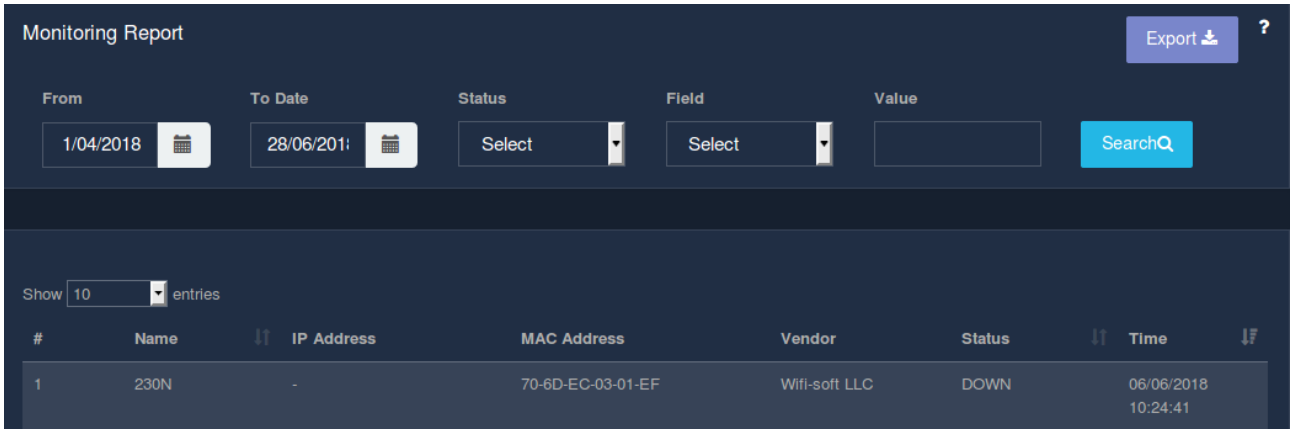
8.7 Monitoring

This page displays the monitoring status of devices. One should ensure that Device Monitoring is enabled in Network Section of Unibox.

This page displays the real-time network status in a tabular format. If the devices are down, the entry will be shown in red. All up devices are shown in green. The table displays the name of the device, IP address, MAC address, vendor, status and monitored time for each device. The searching is based on the time interval, status and various other fields like device name, IP address and MAC address. The status value

indicates whether an AP is UP/Down. The list can be sorted in ascending or descending order by using the icon on each column header.

The administrator can also view the devices on Google map (if latitude and longitude are configured) by clicking the View Map option.



Fig

8.7.1 Export Monitoring Devices

This section allows the administrator to export existing monitoring status of devices from the database.

To export a monitoring device status report, simply click on the 'Export' button. The report is exported in csv format file and it is saved by name MonitoringReport.csv

The CSV file exported follows the format:

- Name
- IP Address
- Mac Address
- Vendor
- Status
- Time

9. Admin

9.1 Accounts

This section in Unibox displays all the administrative account of Unibox. The main administrator can create any number of accounts with specific access privileges for managing Unibox.

9.1.1 Creation

Select the 'Accounts' section from the 'Admin' module present in the sidebar. Click on the '+' icon to create or add a new administrator account. A modal will be displayed that collects the information required to create a new admin account. A modal is displayed which is sectioned into two parts:

- 'Authentication Information' which collects the information required for authenticating the admin.
- 'Access Control' which describes the access permissions for that admin.

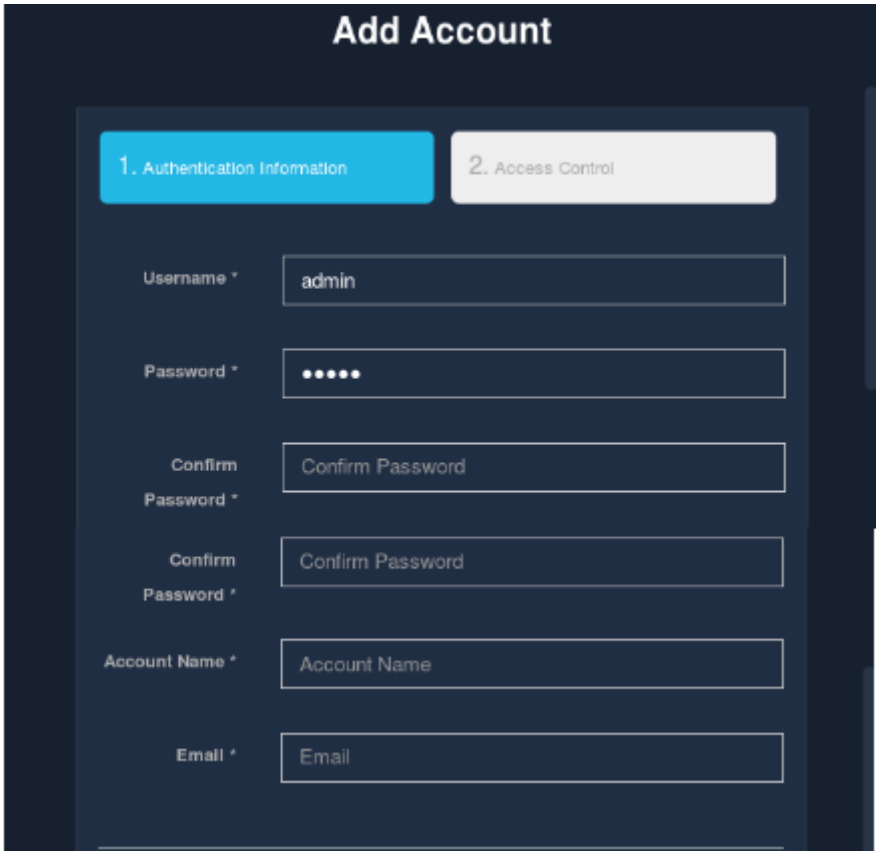
The access control has four values:

- **Full control** – When you select the **Full Access** radio button **Unibox** gives the account holder full access to the feature including delete.
- **Edit** - When you select the **Edit** radio button, **Unibox** gives the account holder edit access to the feature.
- **Read Only** - When you select the **Read Only** radio button, **Unibox** gives the account holder read-only access to the feature.
- **Hidden** - When you select the **Hidden** radio button, **Unibox** hides the feature from the account holder, and account holder cannot view that feature.

Fields	*Description*
Username	Enter an unique username for the account.
Password	Enter the password for the account.
Confirm Password	Confirm the password for the account.
Account Name	Enter the first name and last name of the account holder.
Email	Enter the email address of the account holder.
Access Control	Select the appropriate access control for various Unibox features.

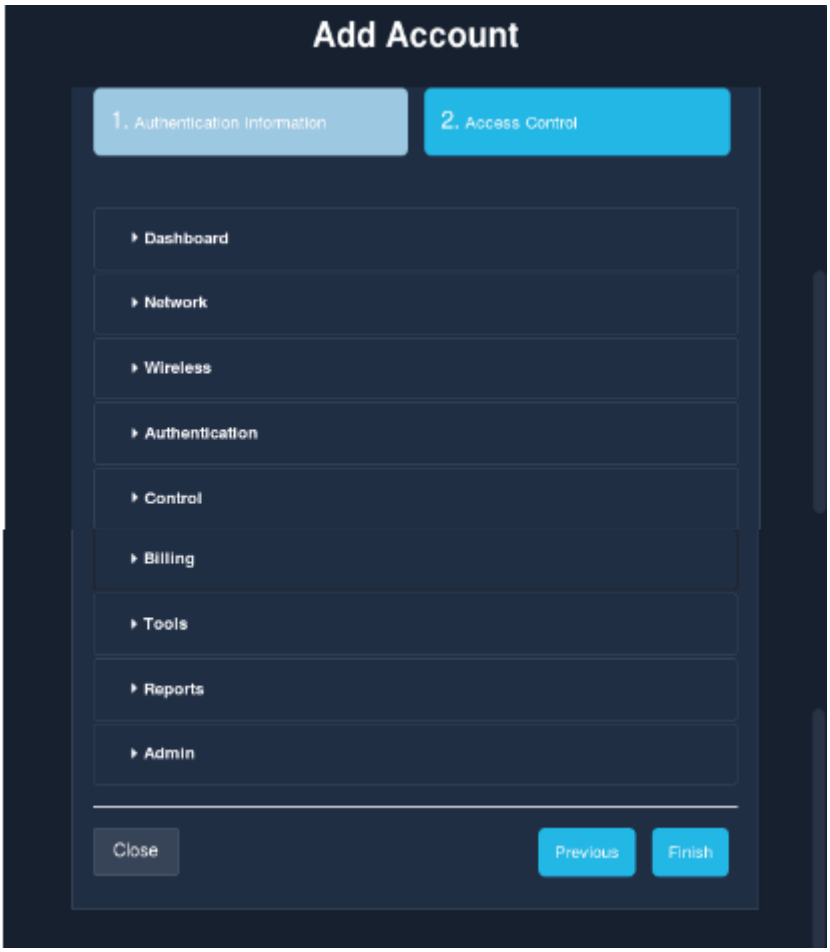
Table

The first section captures the data associated with the admin that includes the following fields:


Add Account
1. Authentication Information
2. Access Control
Username *
admin
Password *
Confirm Password *
Confirm Password
Confirm Password *
Confirm Password
Account Name *
Account Name
Email *
Email

Fig

The second section is the access control section that allows you to select the modules to which the admin will have access to.



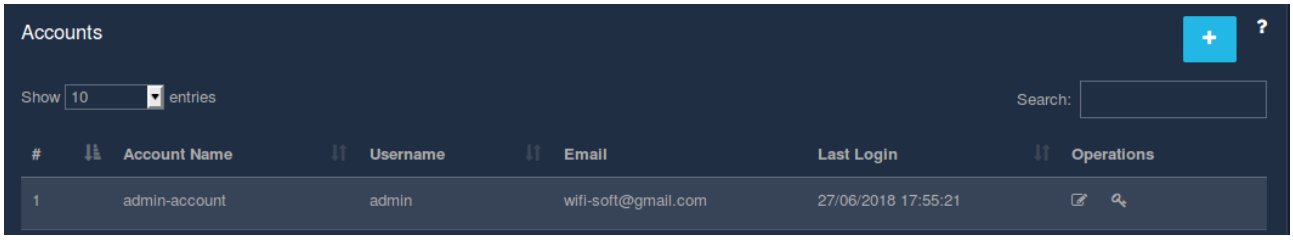
Fig

Click ‘Finish’ and a new admin would be added in the Unibox.

9.1.2 List Accounts

Each account has an account name (username) and password. The list shows the last time the account was accessed. The list can be sorted in ascending or descending order using the icon on each column header. The tabular representation consists of Account name, username, email and the last login.

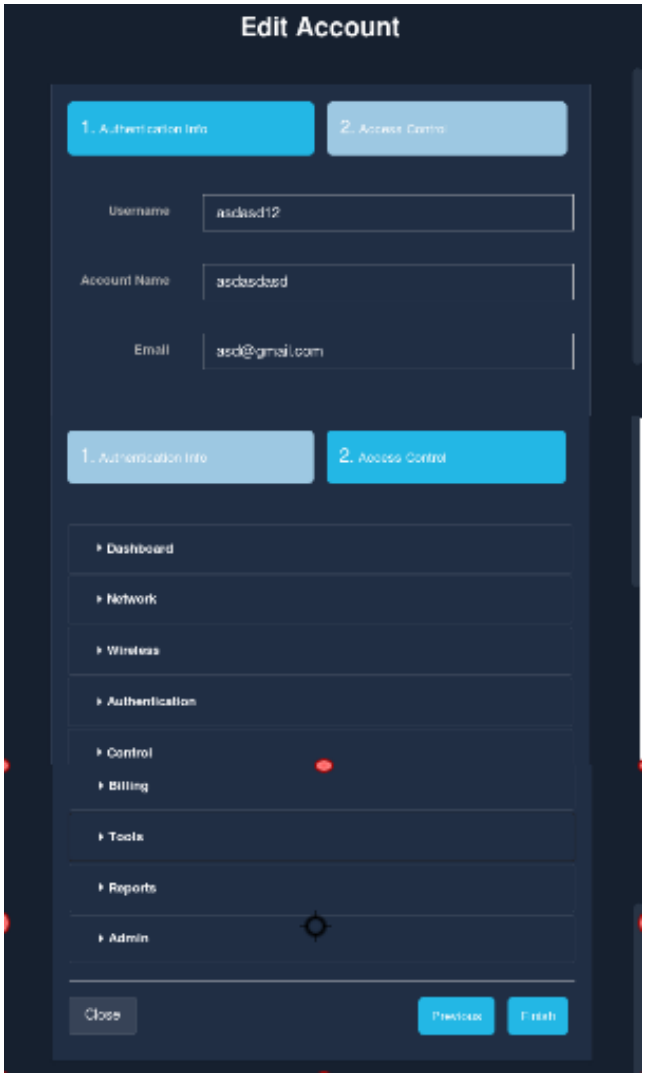
The admin account is non-mutable i.e. the access privileges on this account cannot be modified. Also, this account can't be deleted.



Fig

9.1.3 Edit Account

The ‘Edit’ option allows to make changes to the information about the existing admin account. Click on the edit icon in the ‘Operations’ column to edit an admin’s account. A modal, similar to the one that was displayed while creating a new account, will be displayed.



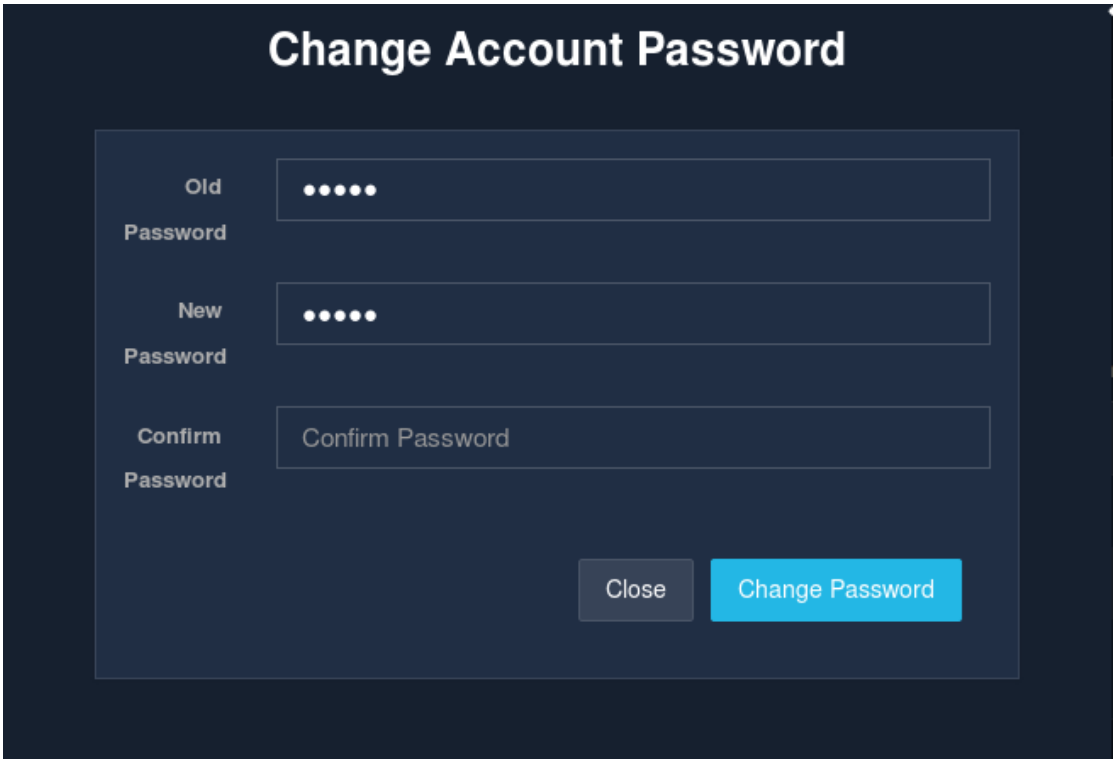
Fig

Click on ‘Finish’ to save and apply all the changes made.

9.1.4 Change Password

This page allows an administrator to change the account password. The new password should be at least 6 characters and different from the old one.

To reset password of an admin account, click on the ‘Change Password’ button in the ‘Operations’ column. It would then prompt you to enter the new password.

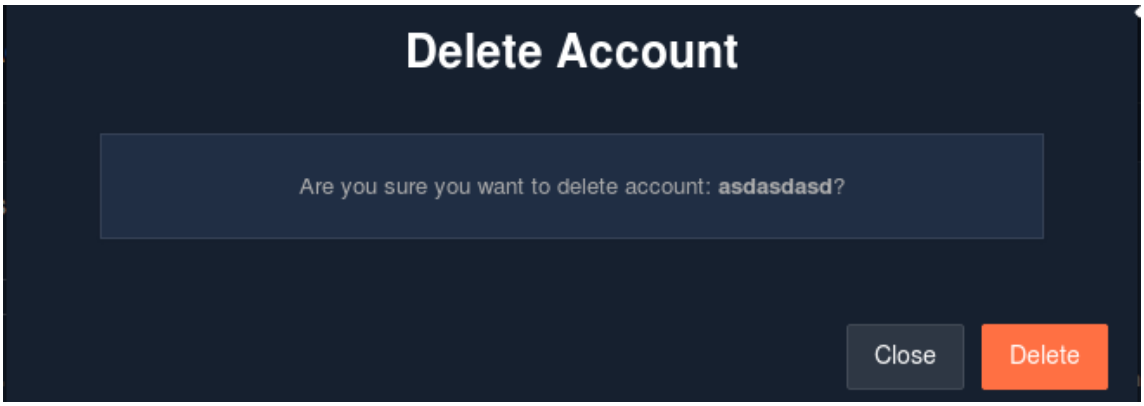


Fig

9.1.5 Delete Account

To delete an admin account, click on the delete icon in the 'Operations' column. A message pops up to confirm the delete operation.

If sure, click on the 'Delete' button.



Fig

9.2 Profile

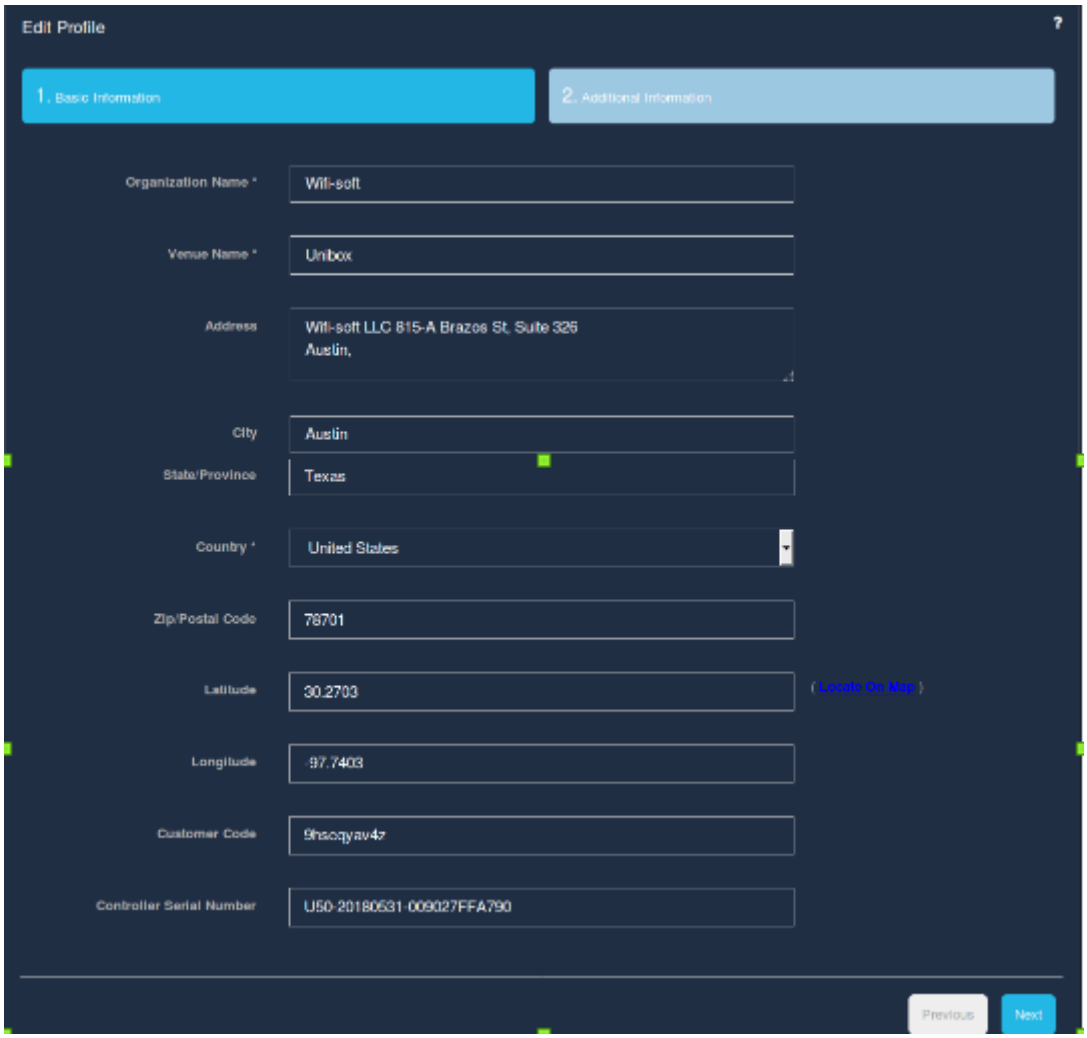
The profile page allows administrators to edit the general information of Unibox. The administrator can enter information about the location where Unibox is installed.

In addition, this page also displays the unique code, realm and prepaid password for Unibox. This information is needed if you are implementing external login/portal pages.

Lastly administrator can define the date format, currency and language for Unibox. Changes to these settings will take effect on next login.

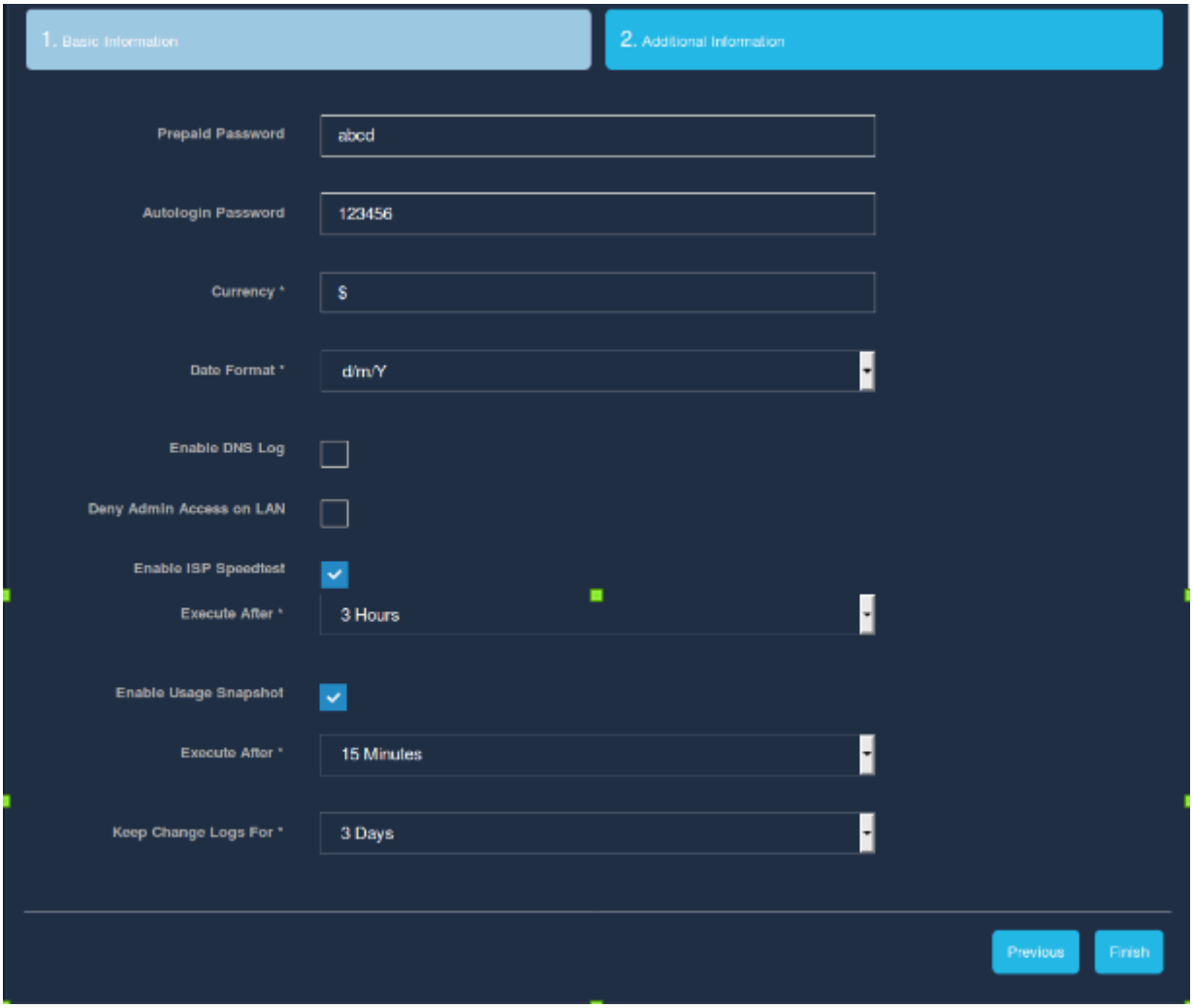
The edit profile page is sectioned into two sections:

Basic Information: Capturing all the basic information about the organization.



Fig

Additional Information: Captures the additional information about the organization.



Fig

Fields	***Description***
Organization Name	Enter the name of the organization using Unibox in the **Organization Name** field.
Venue Name	Name of the place where Unibox is installed.
Address	Enter the address where the Unibox is installed in the **Address** field.
City	Enter the name of the city where the Unibox is installed in the **City** field.
State	Enter the name of the state where the Unibox is installed in the **State** field.

Country	Enter the name of the country where the Unibox is installed in the **Country** field.
Zipcode	Enter the Zip code where the Unibox is installed in the **Zip Code** field.
Latitude/longitude	Enter the Latitude/Longitude of the location where the Unibox is installed in the **Latitude/Longitude** field.
Customer Code	Enter the unique code of Unibox in the **Customer Code** field.
Controller Serial Number	Enter the unique serial number of Unibox in the **Controller Serial Number** field.
Prepaid Password	Enter the unique serial number of Unibox in the **Controller Serial Number** field.
Autologin Password	Enter the Autologin of Unibox in the **Autologin Password** field.
Freelogin Password	Enter the free login password of Unibox in the **Free Login Password** field.
Currency	Enter the currency code/ symbol of the currency to be used in the **Currency** field.
Date Format	Select the date to be used in Unibox in the **Date Format** field.
Enable DNS Log	Select the **Enable DNS Log** check box to enable the DNS log in Unibox.
Deny Admin Access on LAN	Select the **Deny Admin Access on LAN** check box to deny access of the admin on LAN side in Unibox.
Enable ISP Speed Test	If enabled, UniBox will test the speed of Internet connection periodically.
Execute After	Time period after which the speedtest is executed.
Enable Usage Snapshot	If enabled, UniBox will take usage snapshot.
Execute After	Time period after which the usage snapshot is executed.
Keep Logs For	Time period for which the logs will be kept.
Enable Application Tracking	If enabled, UniBox will track application usage on the network. This is an expensive operation so please use it with caution.
Execute After	Time period after which the application tracking will take a snapshot.

Table

Once the form is filled, click on the 'Finish' button. The profile details are being added into the Unibox.

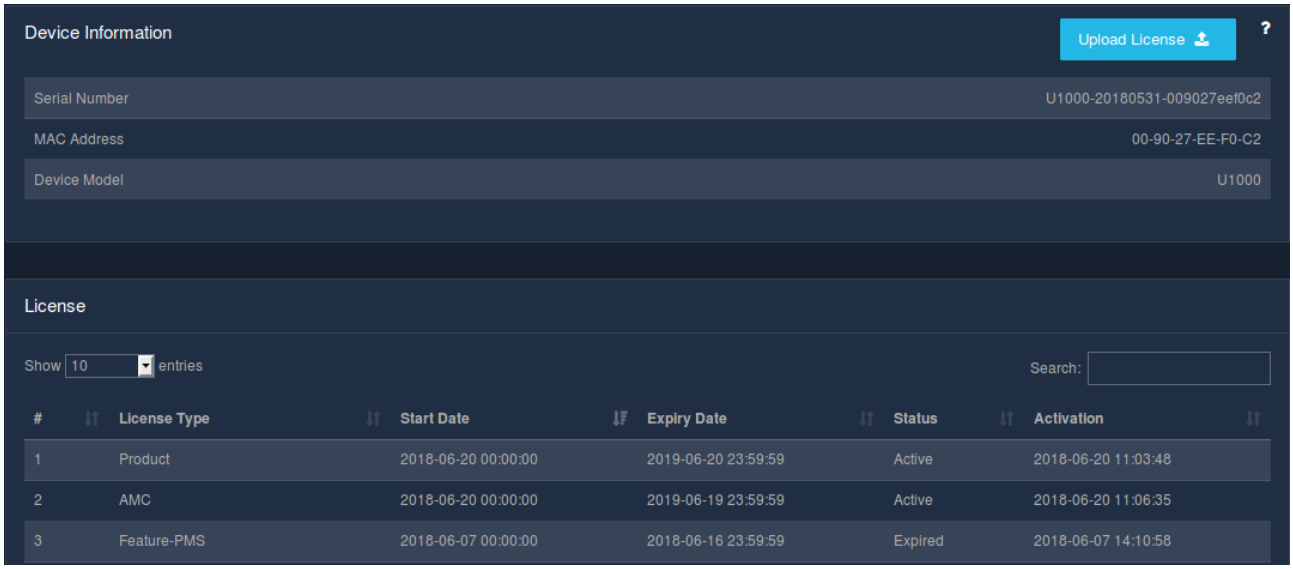
9.3 License

9.3.1 List License

This page displays the current UniBox license along with the serial number, MAC address and model number.

It also displays the list of current and expired licenses. Certain modules in Unibox are licensed separately and the license for these features need to be obtained separately and applied to unibox.

The tabular representation displays the license type, start date, expiry date ,status and the activation date and time of the license.



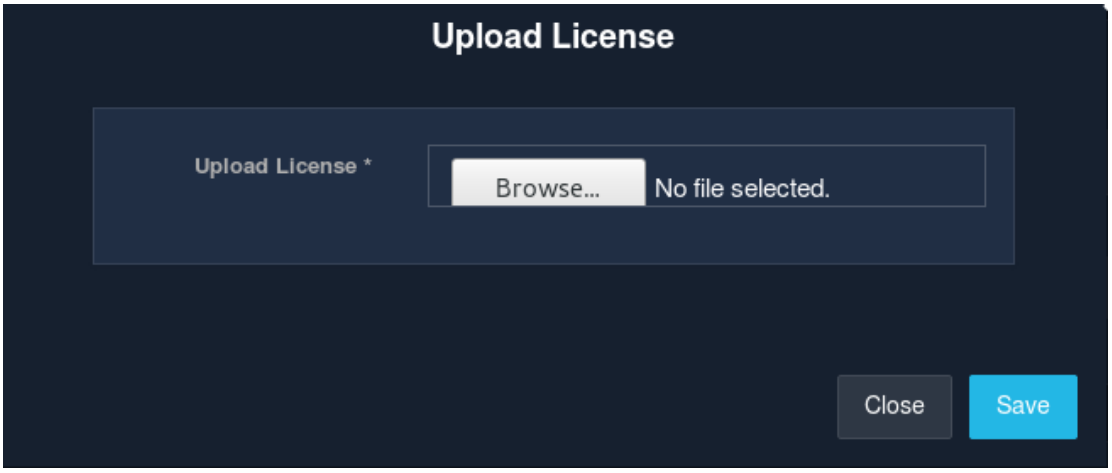
Fig

9.3.2 Upload License

This page allows admin to apply a new license file to UniBox. Admin needs to get the license file from Wifisoft and then apply the license.

The license will take effect immediately and will be displayed in the License Manager.

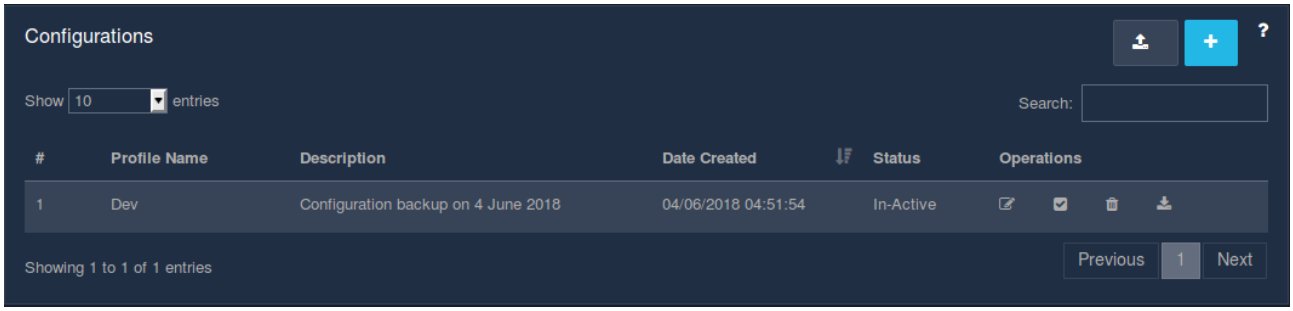
In order to upload the license, click on the button named ‘Upload License’. Select the valid file you wish to upload. Click on ‘Save’ button would then upload this file containing a valid license.



Fig

9.4 Configuration

UNIBOX displays the list of backup configurations saved in Unibox. The administrator can take backup of Unibox configuration periodically to recover Unibox in case of a problem.

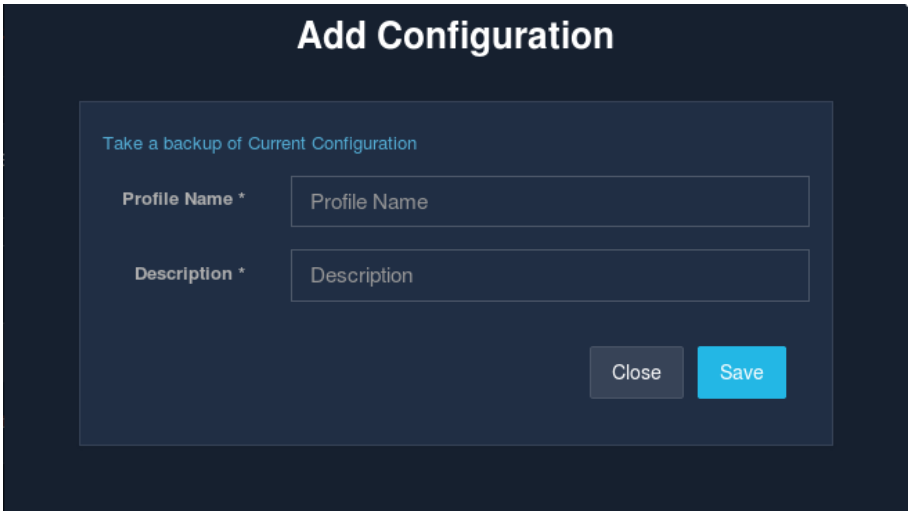


Fig

9.4.1 Creation

This page allows the administrator to create a backup of the current configuration. The configuration is stored under the given profile name. The administrator can apply the backup configuration in the future to revert Unibox to the saved settings. UniBox generates a config file and stores the file on the local disk.

To add a new configuration, click on the + icon.



Fig

Fields	***Description***
Profile Name	Enter the name of the configuration profile.
Description	Enter a short description of the profile.

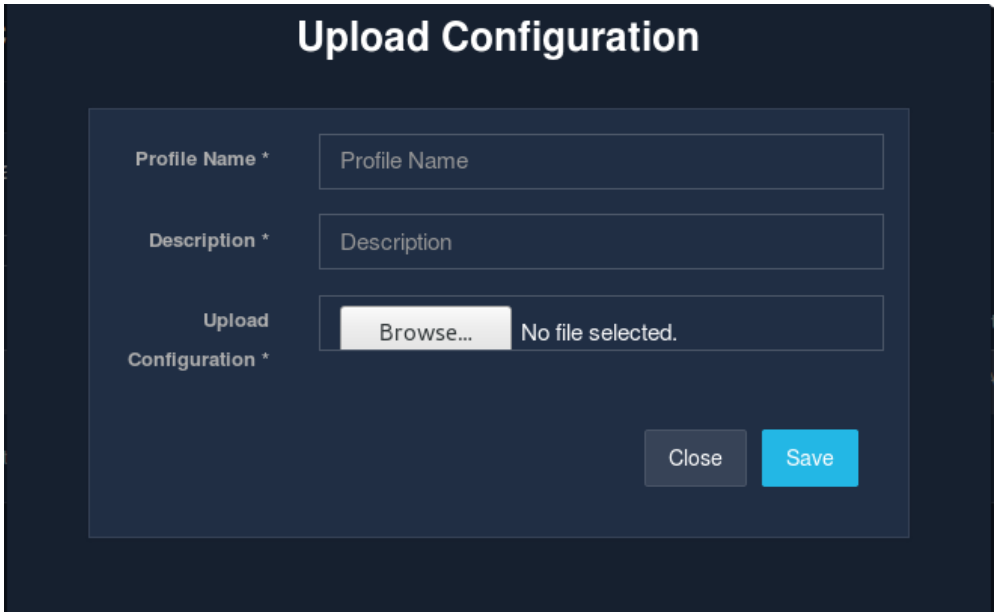
Table

On click of the 'Save' button,will add a new configuration in the Unibox.

9.4.2 Upload Configuration

This section allows administrators to upload a configuration file from the local machine into Unibox. The uploaded configuration will be saved under the given profile name. The administrator can separately apply the configuration to the Unibox.

All the configurations are saved with a profile name. Click on the profile name to change an existing configuration. UniBox will try to load the new configuration on reboot. Please make sure that the config file is correct before upload.



Fig

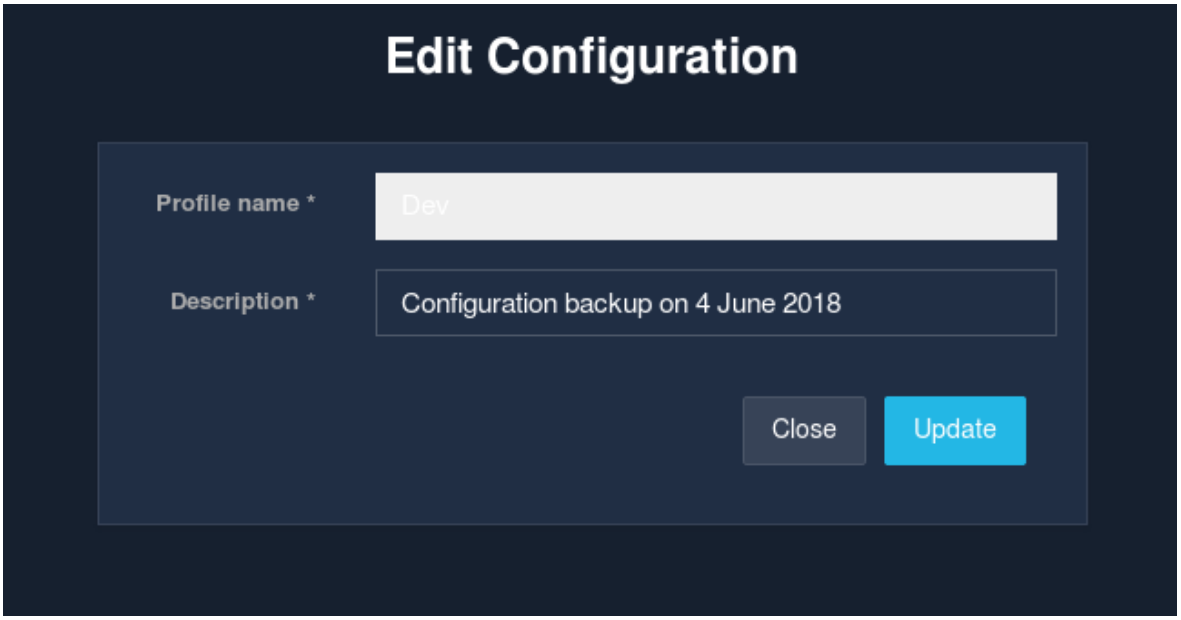
Fields	*Description*
Profile Name	Enter the profile name.
Description	Enter a short description.
Upload Configuration	Upload a valid file containing the configuration.

Table

9.4.3 Edit Configuration

This section allows an administrator to make changes to an existing configuration. The administrator can change the name of the profile or description.

The option to edit a configuration can be found either in the ‘Operations’ column . When the edit icon in the ‘Operations’ column is clicked, a modal is displayed which is similar to the create configuration modal.



Fig

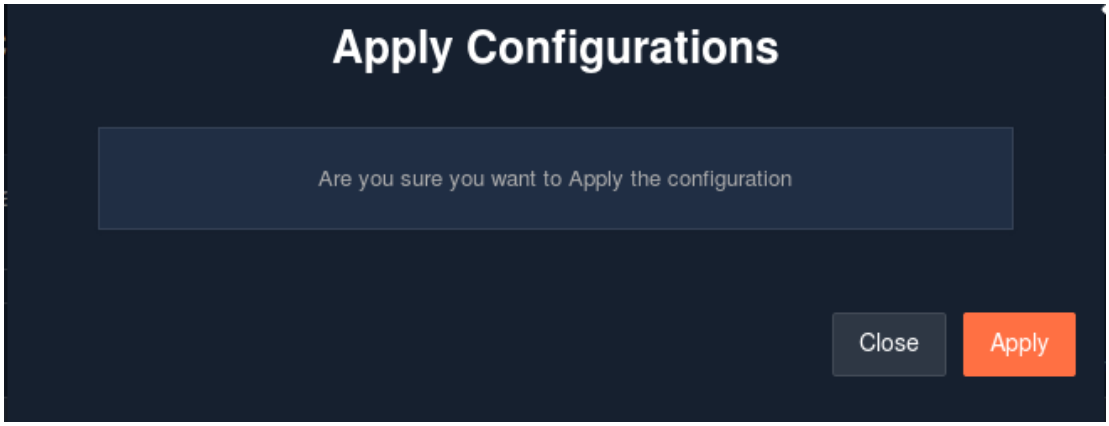
Only the description can be changed. The profile name cannot be edited. Once the changes are made, click on 'Update' to save the changes made.

9.4.4 Apply Configuration

This section allows the administrator to apply the configuration added in the unibox.

Once applied, the previous configuration would be replaced by the new configuration.

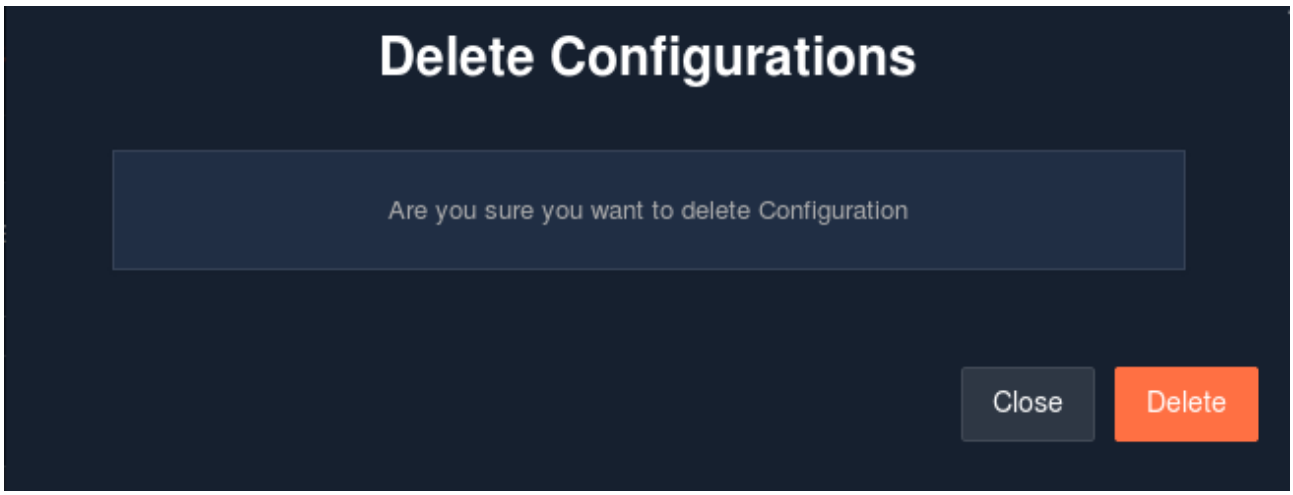
In order to apply the configuration, click on the 'Apply' button in the 'operations' column. A confirmation message pops up to confirm the apply action. Once sure, click on the 'Apply' button.



Fig

9.4.5 Delete Configuration

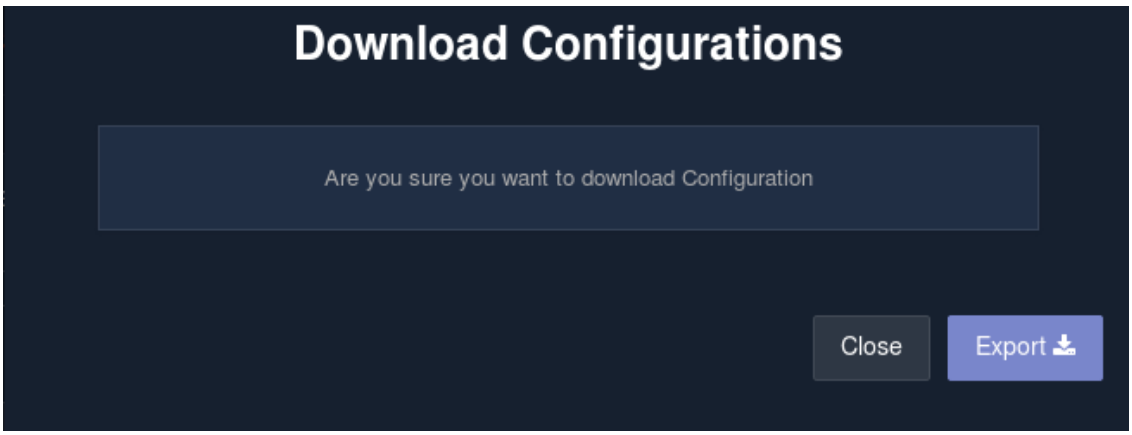
This option allows the admin to delete an existing configuration from the database. Configuration once deleted, cannot be restored. To delete the configuration, click on the 'Delete' button in the 'Operation' column. A confirmation message pops up to confirm the delete action. Once sure, click on the 'Delete' button.



Fig

9.4.6 Download Configuration

This section allows the admin to download an existing configuration,
To download a configuration, click on the download icon in the 'Operations' column. A confirmation message pops up to confirm the download/export action. Once sure, click on the 'Export' button .This saves the downloaded file on the local disk.



Fig

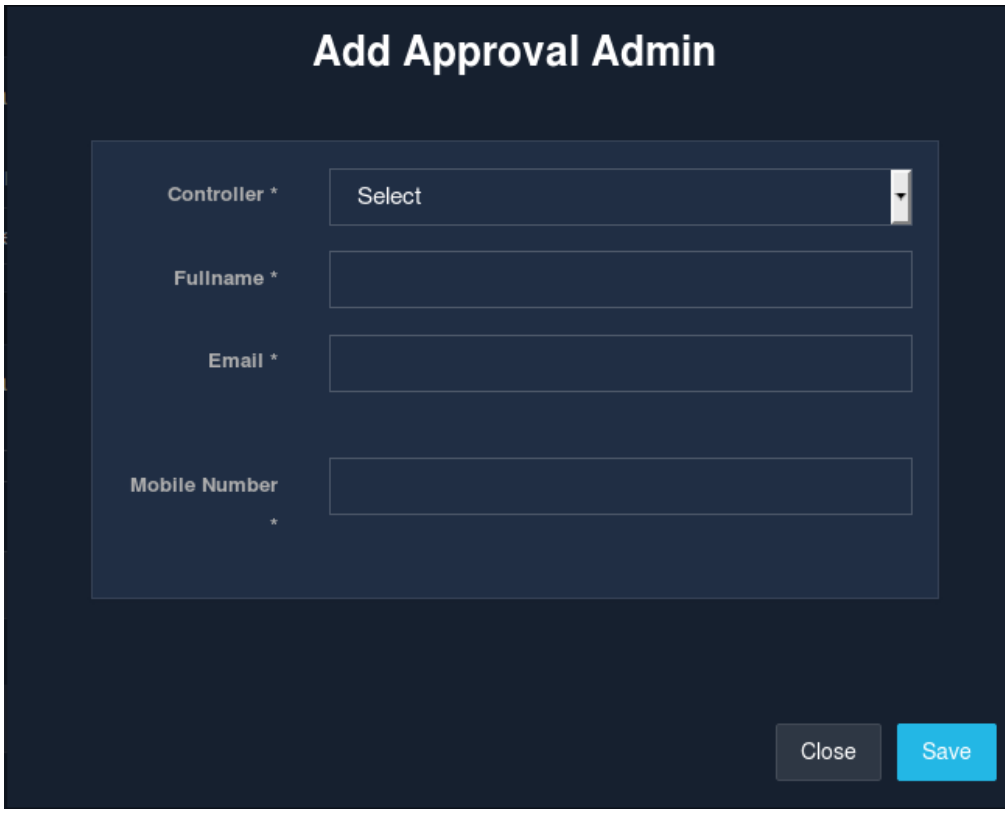
9.5 Approvals

This page displays the list of all the approval admins managing the approval process. The approval admin is the person who is responsible for approving the user's internet access request.

9.5.1 Creation

This section allows the administrator to create an approval admin for approving the user internet request. The approval admin can then decide whether to approve or deny the user's internet request.

To add an approval admin, click on the '**+**' icon.A modal will than appear that captures the admin's personal details.



Fig

Fields	*Description*
Controller	Select the controller profile.
Fullname	Enter the fullname of the admin.
Email	Enter the email id of the admin.
Phone Number	Enter the phone number of the admin.

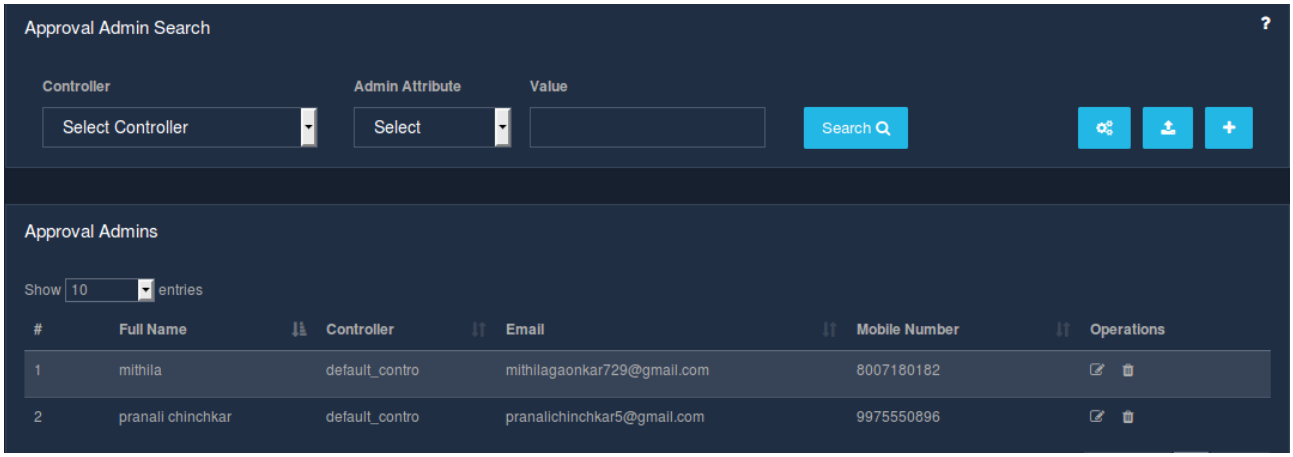
Table

Click on the 'Save' button will add a new approval admin.

9.5.2 List Approval Admin

This page displays all the admins managing the approval. The main administrator can add, import, delete and edit an admin details. The list can be sorted in ascending or descending order using the icon on each column header. Approvers are responsible for approving the user's internet access request when the approval based registration portal is used. The approval admin is further allowed to configure the notification template as per his/her wish.

Note: In order to use Approval Portal, the approver needs to access the UniBox and hence needs to be in the same network. If the approver is remote, then the approval process may not work.

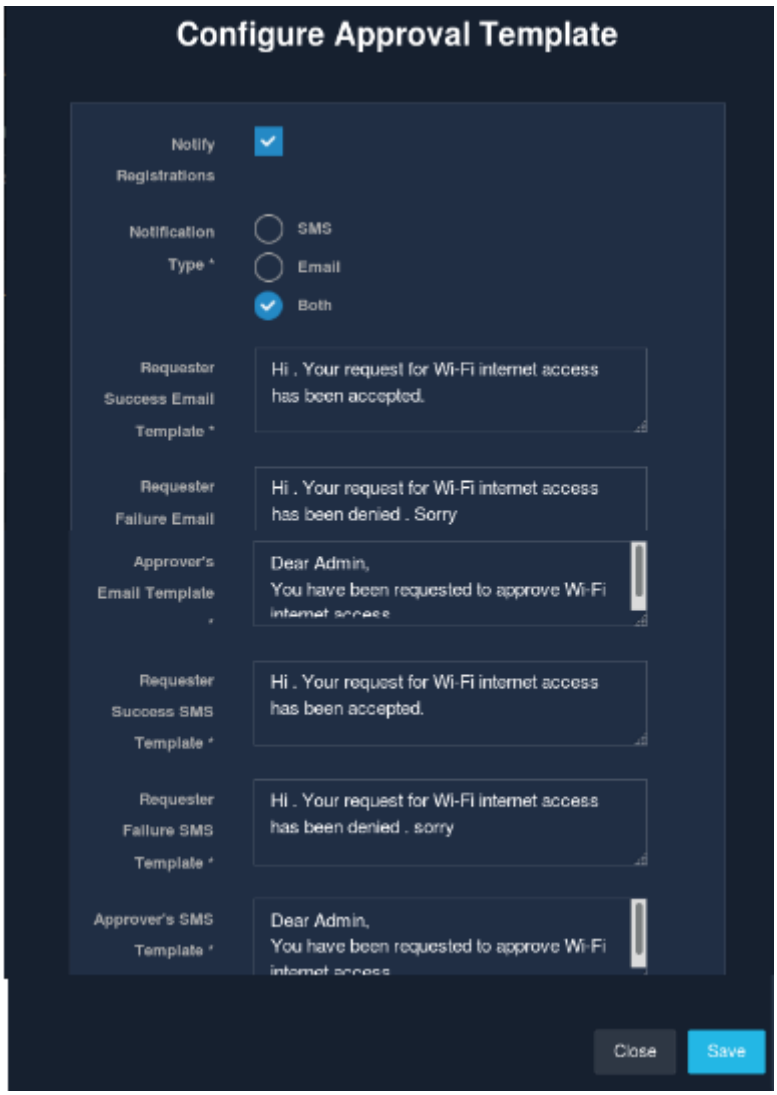


Fig

9.5.3 Configure Template

This section allows the approval admin to configure the approval template for notifying the user and the approver. A pre-defined template is set already. If in case the admin wants to modify it, he/she can update the template by adding the new template.

To configure an approval template, click on the 'Configure' button. A modal will pop-up that consists the pre-defined template. You can modify the template and click on the 'Save' button to update the template. This will update the template in the database.



Fig

Fields	***Description***
Notify Registration	Checking this checkbox would enable the notifications of approval request.
Notification Type	Select the notification type - sms, email or both.
Requester Success Email Template	Enter the requester success email template. This email template is sent to the user requesting the internet access on successful approval.
Requester Failure Email Template	Enter the requester failure email template. This email template is sent to the user requesting the internet access on denial of request.
Approver's Email Template	Enter the approver's email template. This email template is sent to the approver who is responsible for approving the user's request.
Requester Success SMS Template	Enter the requester success sms template. This SMS template is sent to the user requesting the internet access on successful approval.

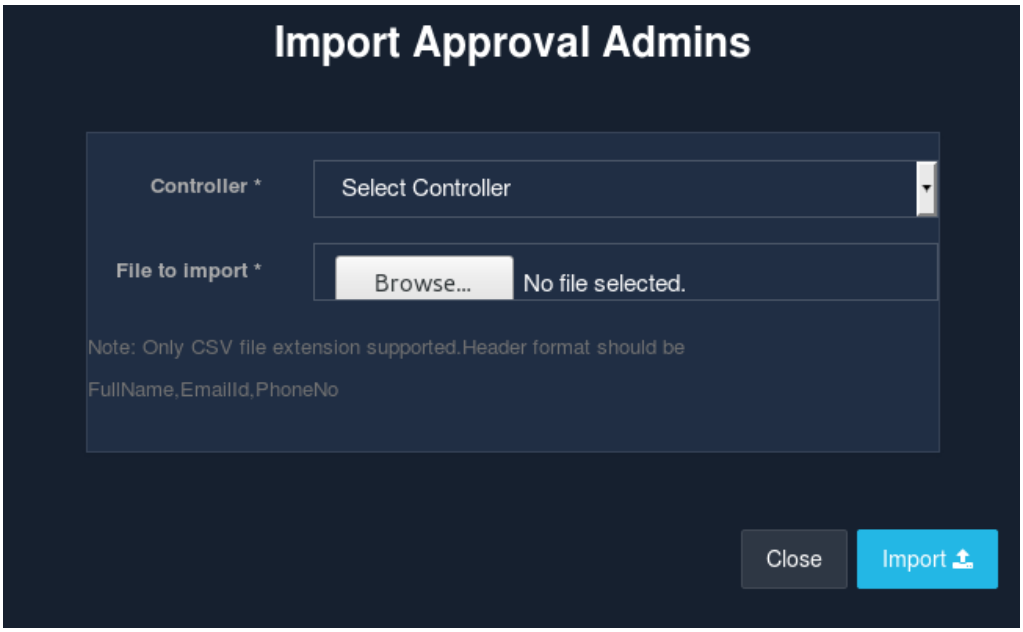
Requester Failure SMS Template	Enter the requester failure sms template. This SMS template is sent to the user requesting the internet access on denail of user's request.
Approver's SMS Template	Enter the approver's sms template. This SMS template is sent to the approver who is responsible for approving the user's reqeust.

Table

9.5.4 Import Approval Admin

This section allows the administrator to import new approval admins by importing the csv file that consists the admin data. Existing approval admins will get updated while importing all other approval admins. On clicking the 'Import' button, a modal is displayed that gathers the information about the controller and the valid file to be imported containing the approval admin's data.

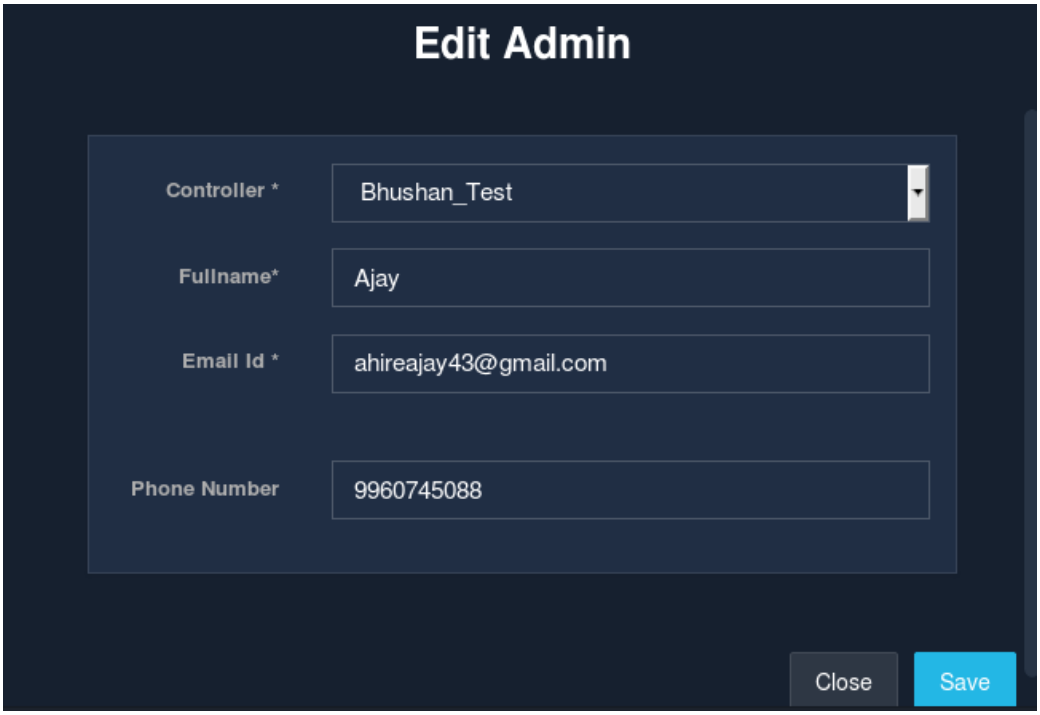
Click on the 'Import' button would then add the approval admins in the database.



Fig

9.5.6 Edit Approval Admin

This section allows an administrator to edit/change an existing approval admin. The option to edit an approval admin's information can be found in the 'Operations' column. When the edit icon in the 'Operations' column is clicked, a modal is displayed which is similar to the create approval admin .



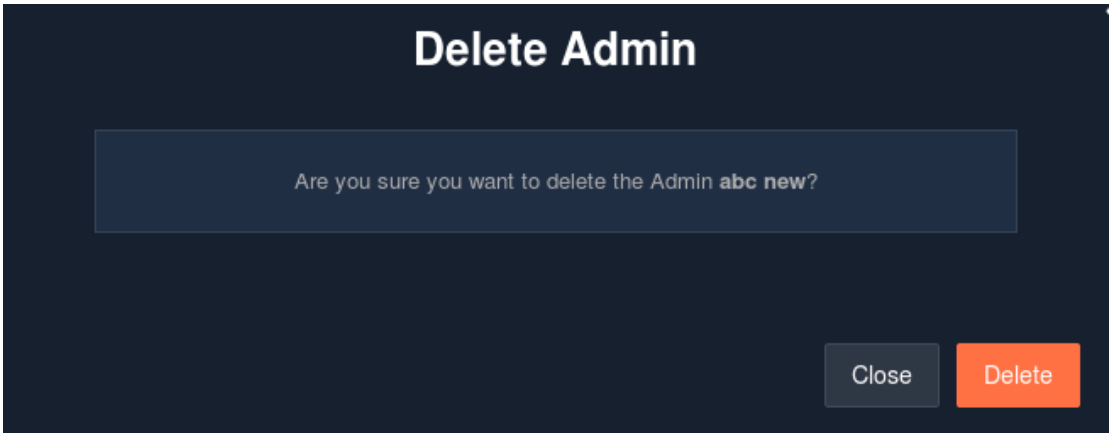
Fig

Once the changes are made, click on 'Save' to save the changes made.

9.5.7 Delete Approval Admin

This option allows the admin to delete any existing approval admin from the database. Approval admins once deleted, cannot be restored.

To delete the approval admin, click on the 'Delete' button in the 'Operations' section. A confirmation message pops up to confirm the delete action.



Fig

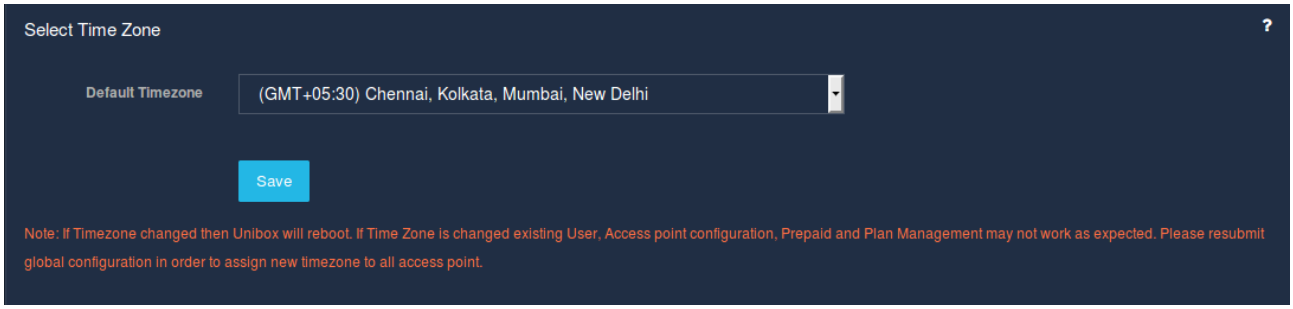
Once sure, click on the 'Delete' button.

9.6 Time

9.6.1 Timezone

This section helps you to set or change the timezone settings of Unibox. Select the timezone setting for Unibox. The timezone will be used to display reports, usage statistics and other time related information to the administrator. Unibox doesn't support daylight savings time in this version.

Timezone changes take effect for all the activities, hence forth. Previous logs are unchanged.



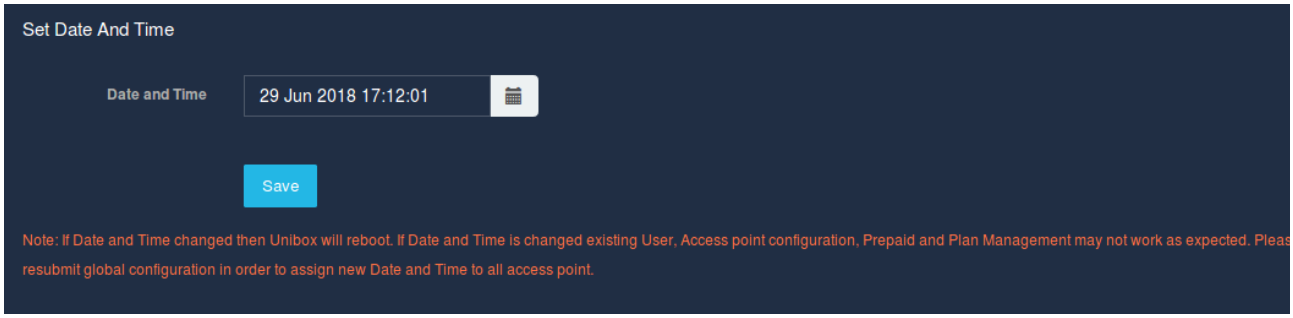
Fig

Click on the 'Save' button to save the new timezone.

9.6.2 Date & Time

This page will display the current date and time of Unibox.

This page allows an administrator to define or set the current date and time for Unibox. Please note that the date and time on old records will not adjust whenever date and time is changed. The change will take effect for all the new activities in Unibox.



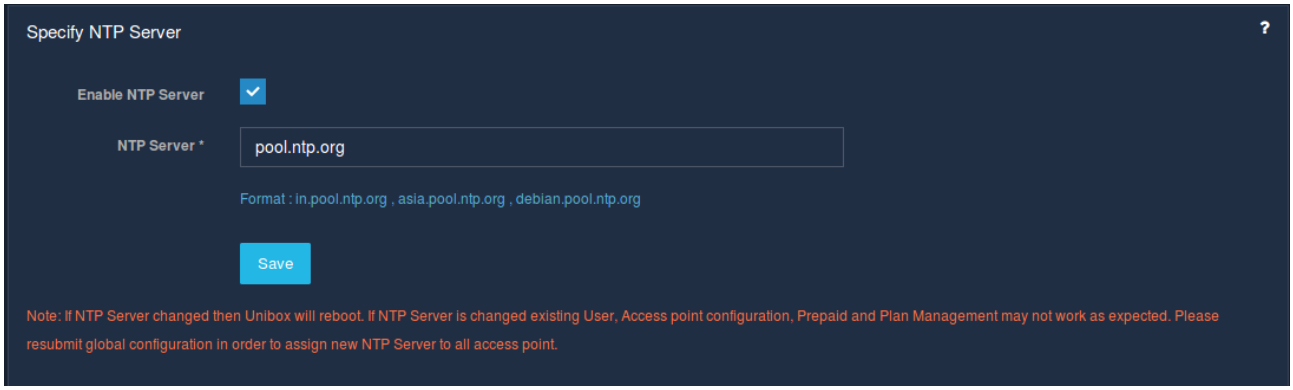
Fig

Click on the 'Save' button to save the new date and time.

9.6.3 NTP Server

This section allows you to change the NTP server settings.

The administrator can change the NTP server address on this page. Please ensure that the specified NTP server is responding before you save the configuration.



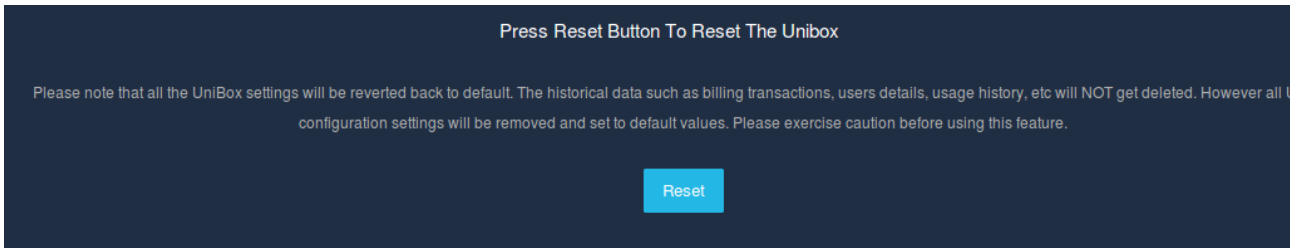
Fig

9.7 Reset

This section allows the administrator to RESET Unibox to factory defaults settings from Unibox User Interface using administrator's credentials.

Please note that all the Unibox settings will be reverted back to default. The historical data such as billing transactions, users details, usage history, etc will NOT get deleted.

However all Unibox configuration settings will be removed and set to default values.



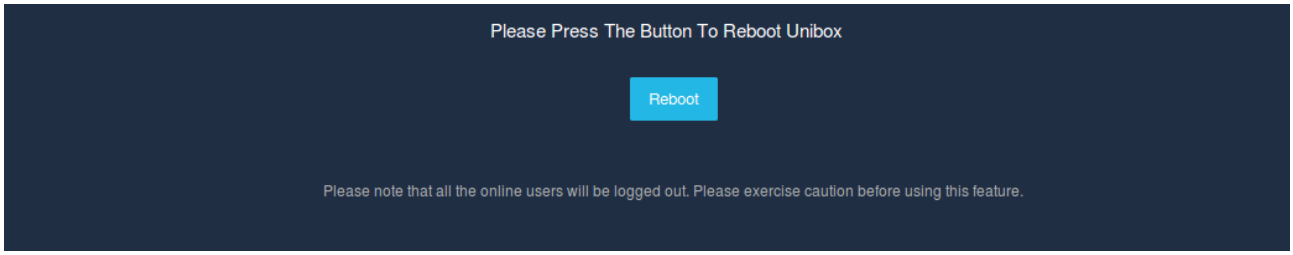
Fig

In order to reset Unibox ,click on the 'Reset' button. A confirmation message pops up to confirm the reset action. Once sure, click on the 'Reset' button.

9.8 Reboot

This section allows the administrators to reboot Unibox from the user interface. On confirming, Unibox will perform a graceful shutdown and will close all user sessions, active connections and will restart the system.

To reboot a Unibox , click on the 'Reboot' button. A confirmation message pops up to confirm the reboot action. Once sure, click on the 'Reboot' button.

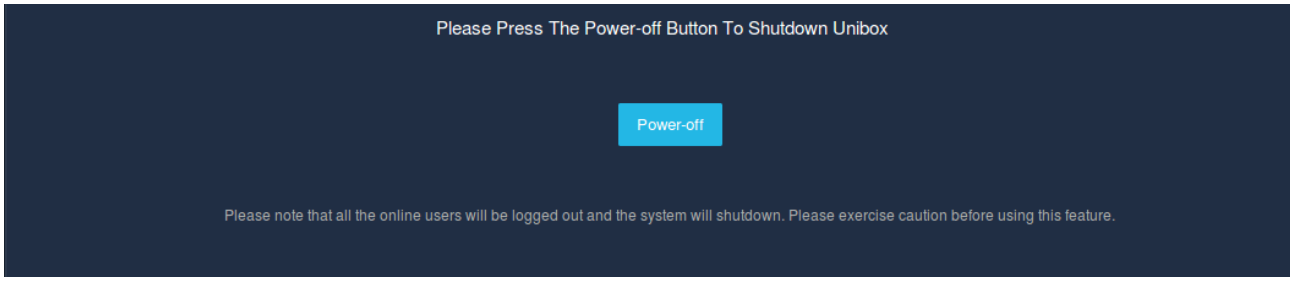


Fig

9.9 Power-off

This section allows administrators to shutdown the machine. On confirming, Unibox will perform a graceful shutdown and will close all user sessions, active connections. One should remember that the power off action would log out all the online users and further shut down the system.

To perform the power-off action,click on the Power-off button. A confirmation message pops up to confirm the power-off action. Once sure, click on the 'power-off' button.



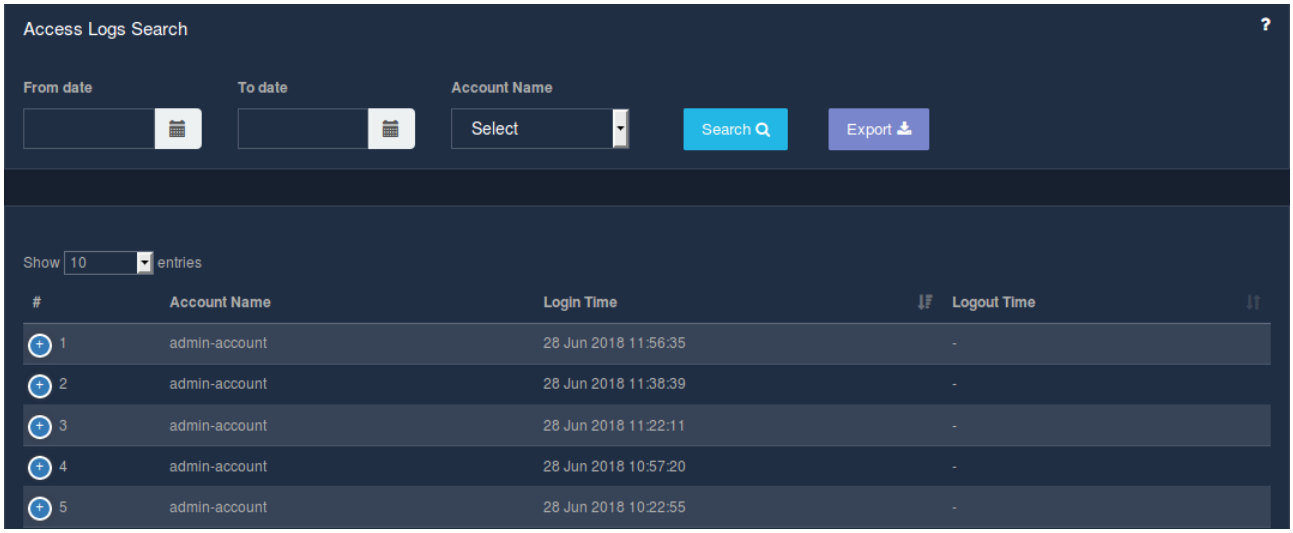
Fig

9.10 Logs

9.10.1 Access Logs

9.10.1.1 List Access Logs

This page displays the access logs of all administrative accounts in reverse chronological order. The history will allow the main administrator to view or search the date and time when administrator access Unibox. Also the list can be sorted in ascending or descending order by using the icon on each column header.



Fig

Fields	***Description***
Account Name	This field displays the account name of the user.
Login Time	This field displays the login time of the user.
Logout Time	This field displays the logout time of the user.
Remote IP Address	This field displays the IP address of the device which took access from Unibox.

Table

9.10.2 Export Access Logs

This section allows an administrator to export the access log information. To export an access log list,click on the 'Export' button.These logs are then downloaded to the local machine of the user.The logs generated are in the csv file having the format :

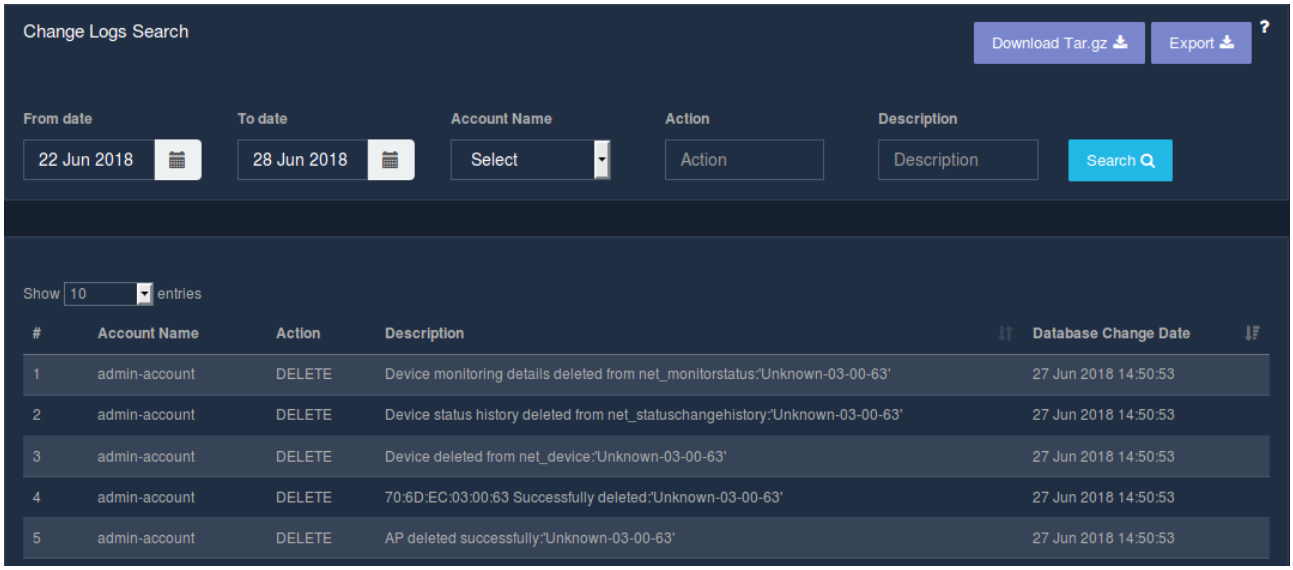
- Account Name
- Login Time
- Logout Time
- Remote IP Address

9.11 Change Logs

9.11.1 List Change Logs

This section displays the changes done to the Unibox configuration from the user interface. This allows administrator to track changes done in the past and keep an audit trail of the changes. All the database changes, including the insertion, deletion, modification, change password and so on. All are being recorded and listed in the change logs.

The administrator can search for the changes using the search fields. Also the list displayed can be sorted in ascending or descending order by using the icon on each column header.



Fig

Fields	***Description***
Account Name	**Account Name** field displays the account name of the administrator account.
Action	**Action** field displays the action done by the administrator.
Description	**Description** field displays the short description for the change log.
Account Change Date	**Account Change Date** field displays the date on which the action from administrator was performed.

Table

9.11.2 Export Change Logs

This section allows the administrator to export the database change logs information. On click of the 'Export' button,a CSV file containing the change logs is generated having the format:

- Account Name
- Action
- Description
- Database Change Date

9.11.3 Download Tar.gz

This page allows admin to download the archived change logs. UniBox automatically archives the old change logs and stores them in zip format. Admin can download these logs for audits and record keeping.

To click the Download Tar.gz file, click on the "Download Tar.gz" button. It would then prompt you to select the specific year and month. Based on the search criteria, the result would be generated.