



IndioCloud

PRODUCT GUIDE 1.0



sales@indionetworks.com



+91 (20) 6715 7377
+1 888-280-4112



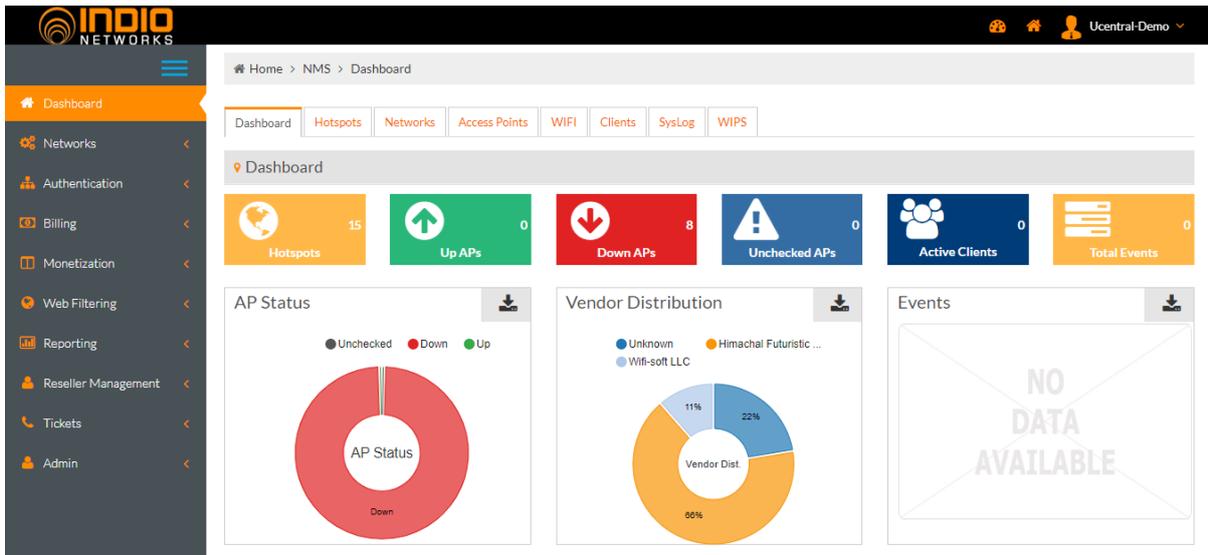
www.indionetworks.com

Table of Contents

1. Dashboard	3
2. Device Configuration	3
2. Access Point Provisioning	14
3. Access Point Command Section	15
4. User Authentication	16
5. External Gateway Configuration	25
6. Heatmap	28
7. 802.1x Authentication	30
8. BYOD (Bring Your Own Device)	31
9. Content Filtering	32
10. WIPS	34
11. SysLog	35
12. Events	35
13. External User Import	36
14. Voucher	37

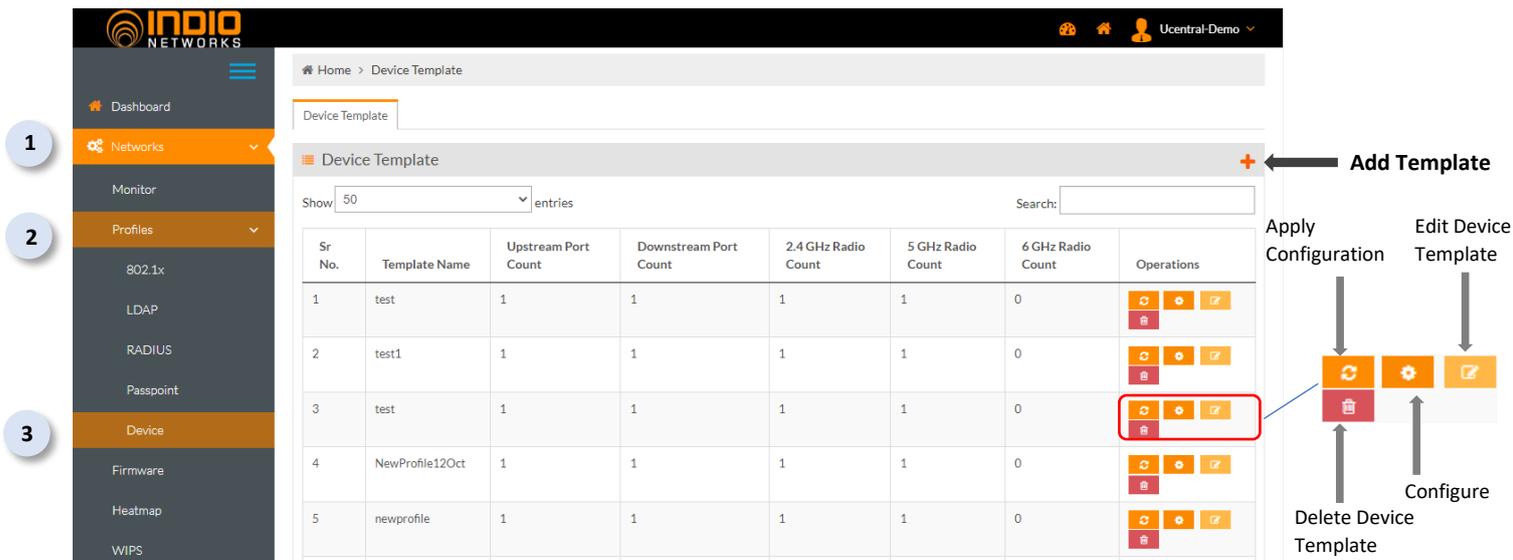
1. Dashboard

The dashboard allows you to view various user activity reports like data usage per device, traffic specific website access, syslog and more.



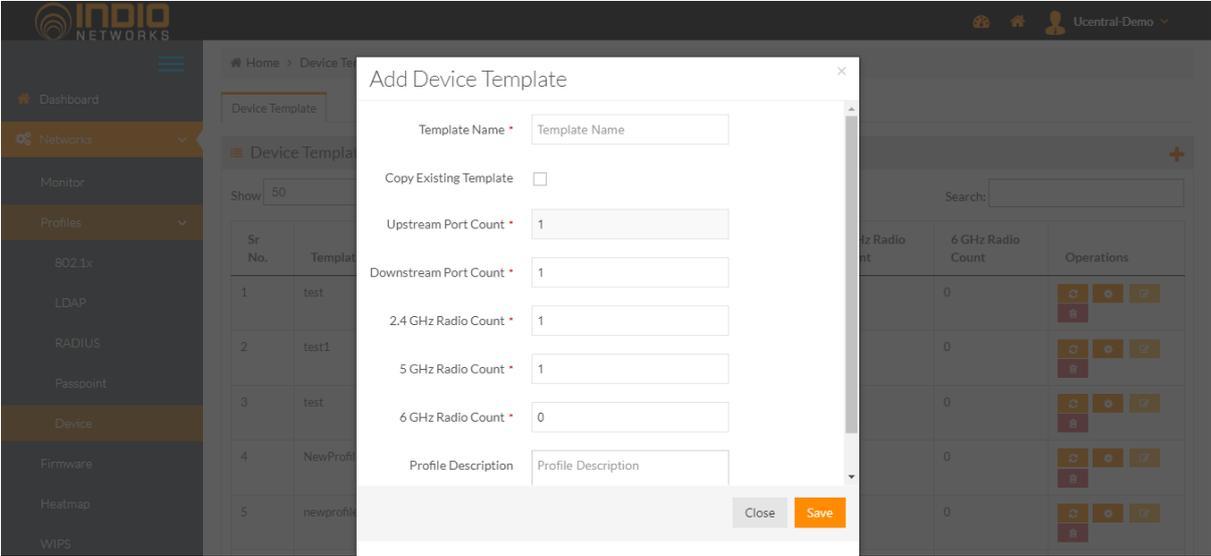
2. Device Configuration

This section deals with the device configuration.

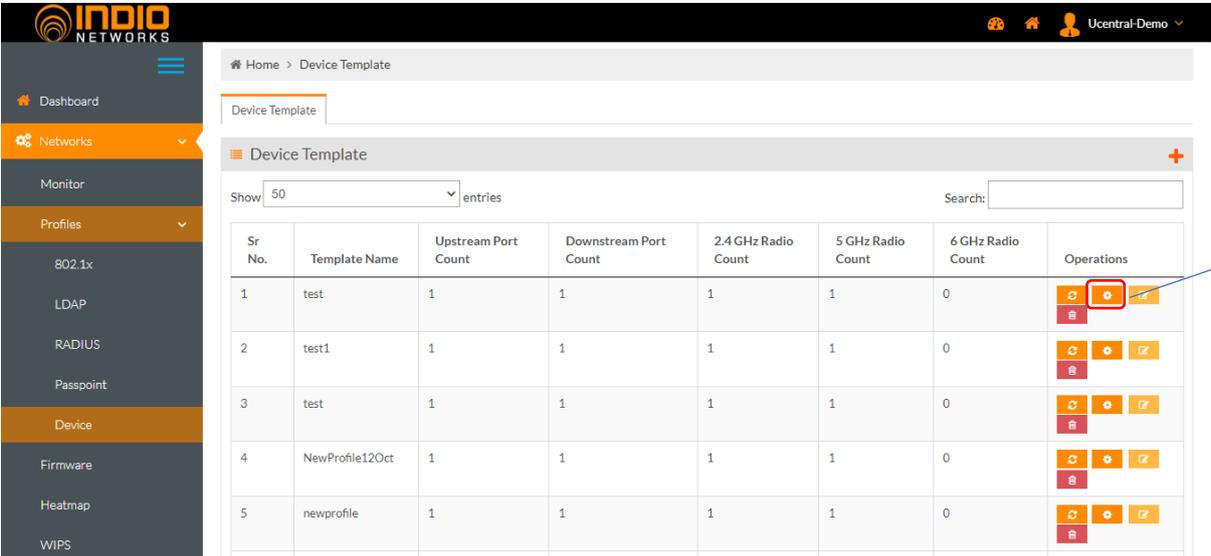


Once you click on the “+” symbol a window will appear, fill in the required details.

Note: Default configuration is already available.



In case you want to make any changes in the configuration, perform the following steps:



Device template configure section allows following changes:

Set **IPv4** and **IPv6** address to be used on a configured upstream (WAN) or downstream (LAN) interface.

IPv4 List

Sr No.	Name	Addressing	Subnet	Gateway IP	DNS	DHCP	Operations
1	Default_Wan1	Dynamic			Disable	Disable	
2	Default_Lan	Static	172.17.0.1/24	172.17.0.1	Disable	Enable	

Showing 1 to 2 of 2 entries

IPv6 List

Sr No.	Name	Addressing	Subnet	Gateway IP	DNS	DHCP	Operations
No data available in table							

Showing 0 to 0 of 0 entries

The **Metrics** section provides a granular configuration. There are several types of metrics that shall be reported in certain intervals.

Home > Device Template > test > List Metrics

IPv4 IPv6 **Metrics** Service Radio Wireless Interface

Metrics List

Show 10 entries Search:

Metrics Name	Status	Actions
Statistics	Enabled	Edit
Health	Enabled	
WiFi Filter	Disabled	
DHCP Snooping	Disabled	

Showing 1 to 4 of 4 entries Previous 1 Next

Apply Configuration

Download Configuration

Statistics	Statistics are traffic counters, neighbour tables
Health	Health check gets executed periodically and will report a health value between 0-100 indicating how healthy the device thinks it is.
WiFi Filter	Defines which types of ieee802.11 management frames shall be sent up to the controller.
DHCP Snooping	Defines which types of ieee802.11 management frames shall be sent up to the controller.

The **Service** section describes all of the services that may be present on the AP. Each service is then referenced via its name inside an interface.

Home > Device Template > test > List Service

IPv4 IPv6 Metrics **Service** Radio Wireless Interface

Service List

Show entries Search:

Service	Status	Operations
LLDP	Enabled	Edit
SSH	Enabled	
NTP	Disabled	
MDNS	Disabled	
RTTY	Disabled	
LOG	Disabled	
HTTP	Disabled	
IGMP	Disabled	
Online Check	Disabled	

Apply Configuration

Download Configuration

LLDP	Link Layer Discovery Protocol describes interfaces and capabilities between directly attached neighbours over Layer 2.
SSH	SSH provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.
NTP	NTP is intended to synchronize all subscribing devices to within a few milliseconds of Coordinated Universal Time (UTC) by querying a master server for the current time and then resetting its own local clock to match.
MDNS	It resolves hostnames to IP addresses within small networks that do not include a local name server.
RTTY	RTTY (Radio TeleType) is a method of using tones to send digital messages between radios in amateur HF bands (and other services). This section can be used to setup a persistent connection to a rTTY server.
HTTP	HTTP functions as a request-response protocol in the client-server computing model. Enables the webserver with the on-boarding webui
IGMP	ICMP creates and sends messages to the source IP address indicating that a gateway to the internet, such as a router, service or host, cannot be reached for packet delivery.
Online Check	This section is used to make end user aware about the backhaul connectivity status either by using LEDs or SSID broadcast. If enabled, AP starts to blink LED or stops broadcasting the SSID if the connectivity to host (Hosts that shall be pinged to find out if we are online) is lost
OpenFlow	OpenFlow specifies the communication between the control plane and the data plane. This protocol allows a server to tell network switches where to send packets.
WiFi Steering	Wifi band steering detects what a wireless device supports and automatically steers it to the best available frequency band when connecting to a Wifi network.
Captive Portal	This section can be used to setup a captive portal on the AP with a click-to-continue splash page.
Content Filtering	Content filtering is a process that manages or screens access to specific emails or webpages, executables and other suspicious items.
Air Time Fairness	This section describes the VLAN behaviour of a logical network interface.

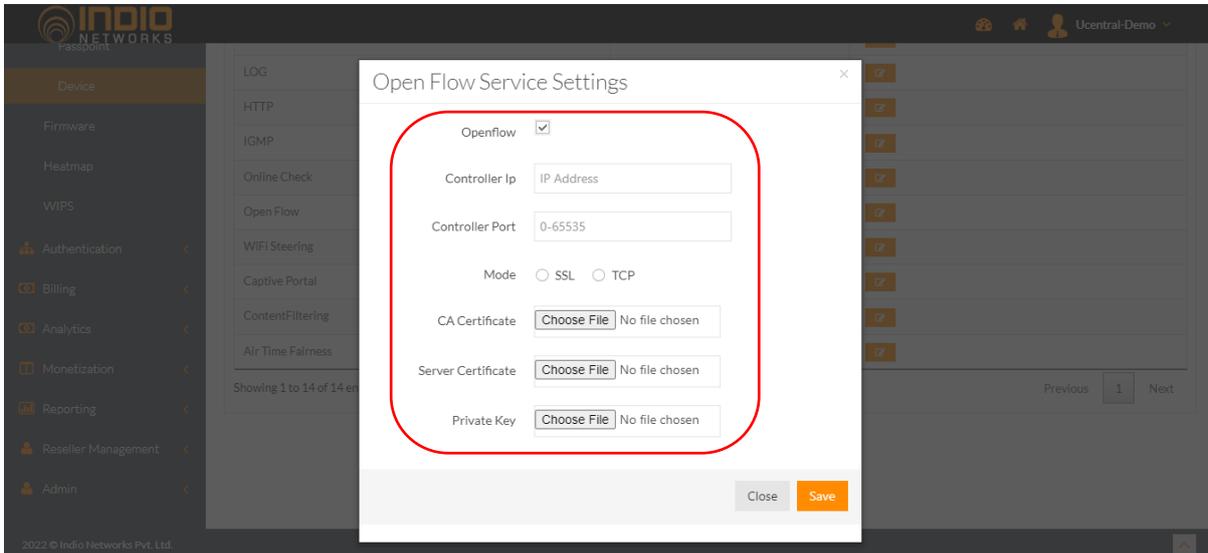
Open Flow Configuration:

The screenshot shows the INDIO Networks management interface. On the left, a sidebar contains navigation options: RADIUS, Passpoint, Device (highlighted with a circled '1'), Firmware, Heatmap, WIPS, Authentication, Billing, Analytics, Monetization, Reporting, and Reseller Management. The main area displays a table of configuration items, all currently 'Disabled'. The 'Open Flow' row is selected, and its edit icon is circled with a '2', with an 'Edit' label next to it. The table includes columns for the feature name, its status, and an edit icon.

NTP	Disabled	
MDNS	Disabled	
RTTY	Disabled	
LOG	Disabled	
HTTP	Disabled	
IGMP	Disabled	
Online Check	Disabled	
Open Flow	Disabled	Edit
WiFi Steering	Disabled	
Captive Portal	Disabled	
ContentFiltering	Disabled	
Air Time Fairness	Disabled	

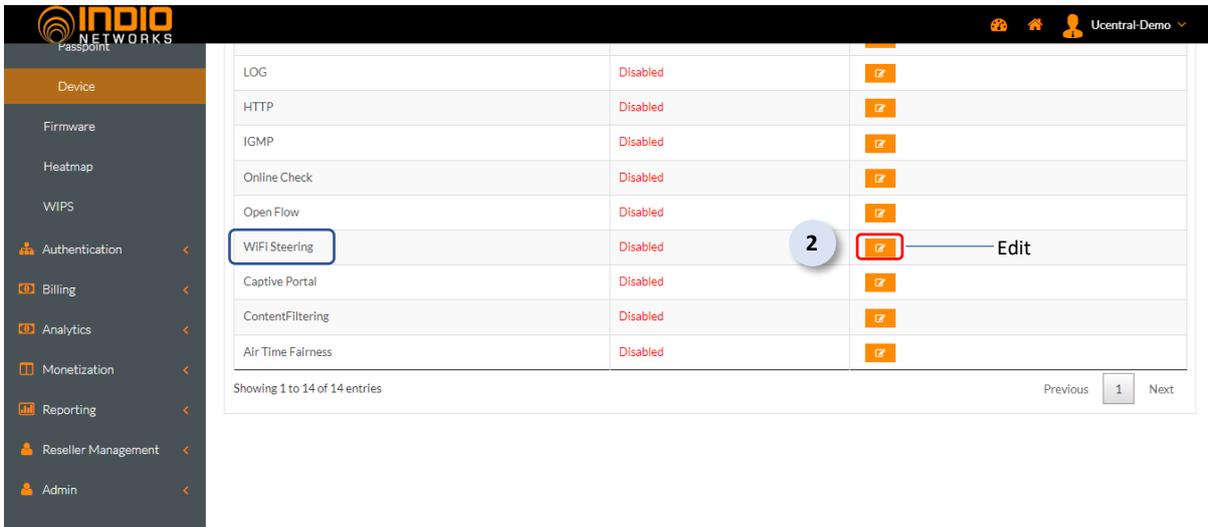
Showing 1 to 14 of 14 entries Previous 1 Next

Fill in the required details:

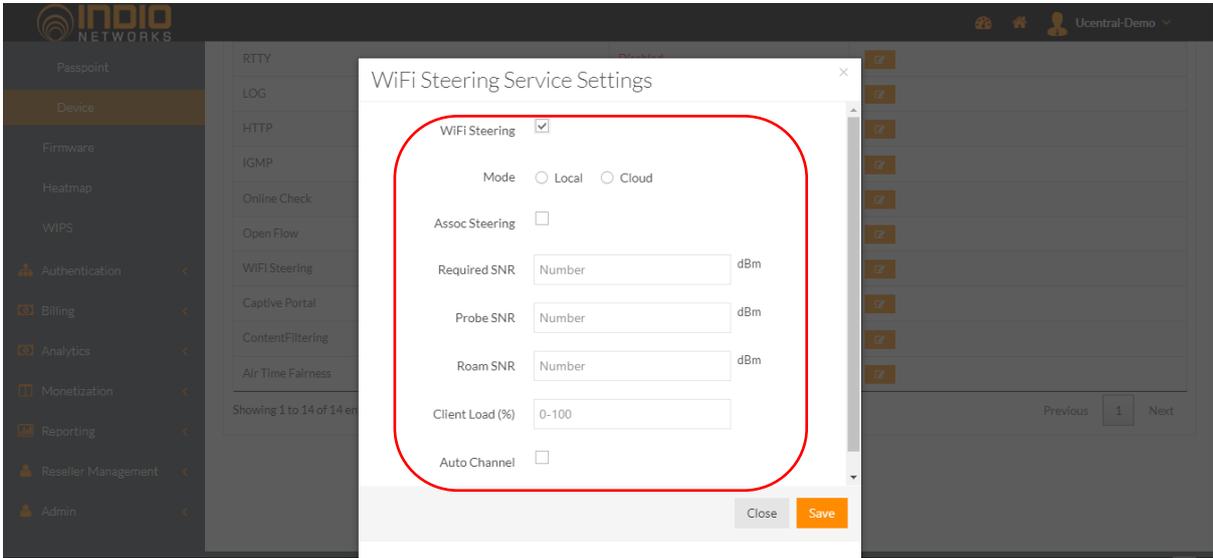


WiFi Steering:

1

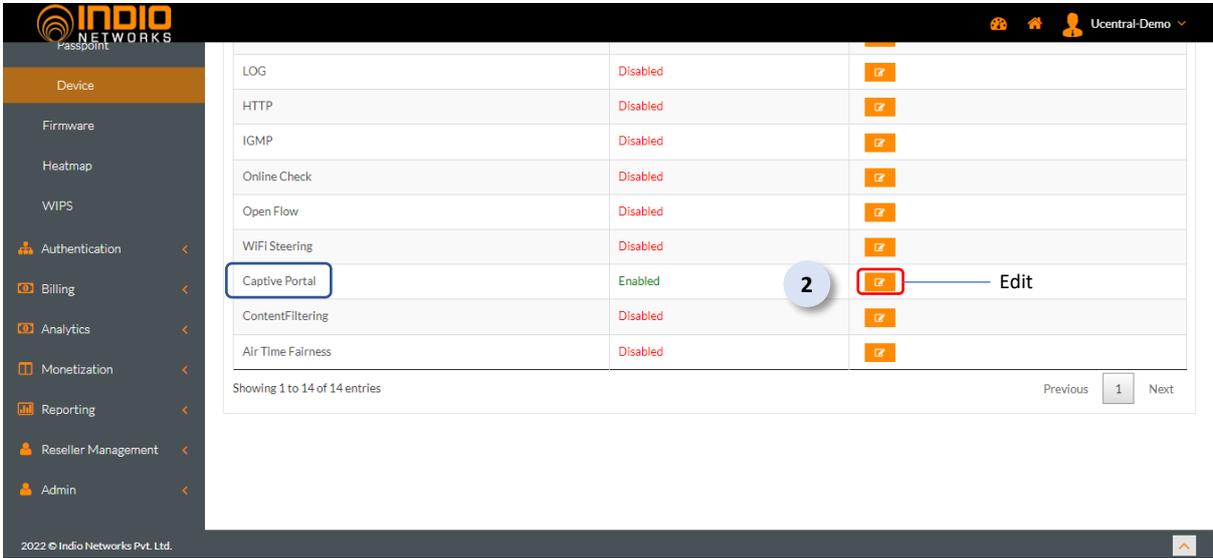


Fill in the required details:

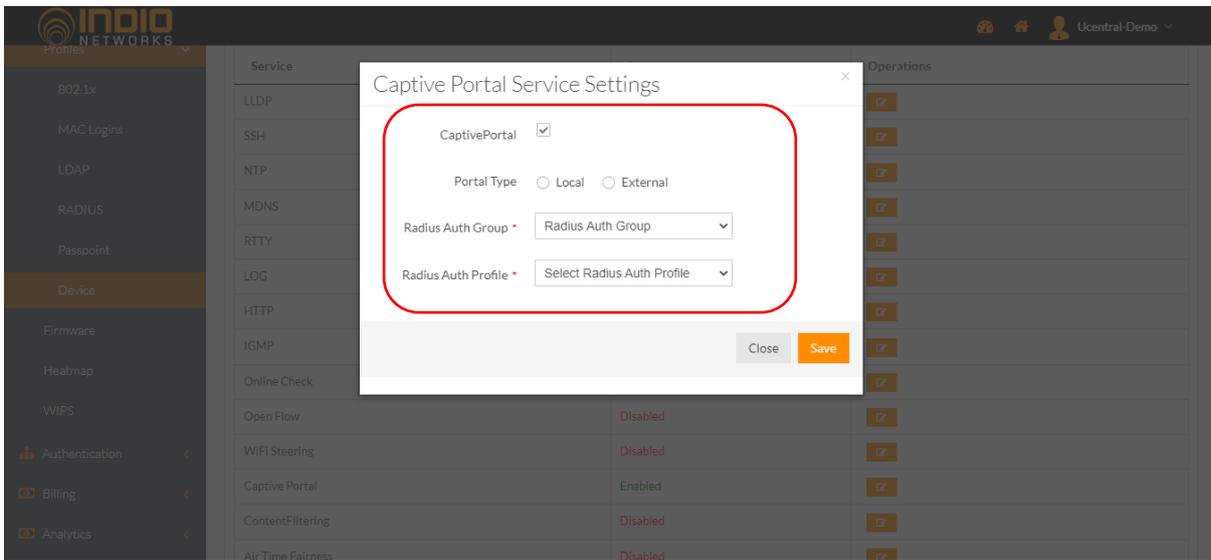


Captive Portal:

1



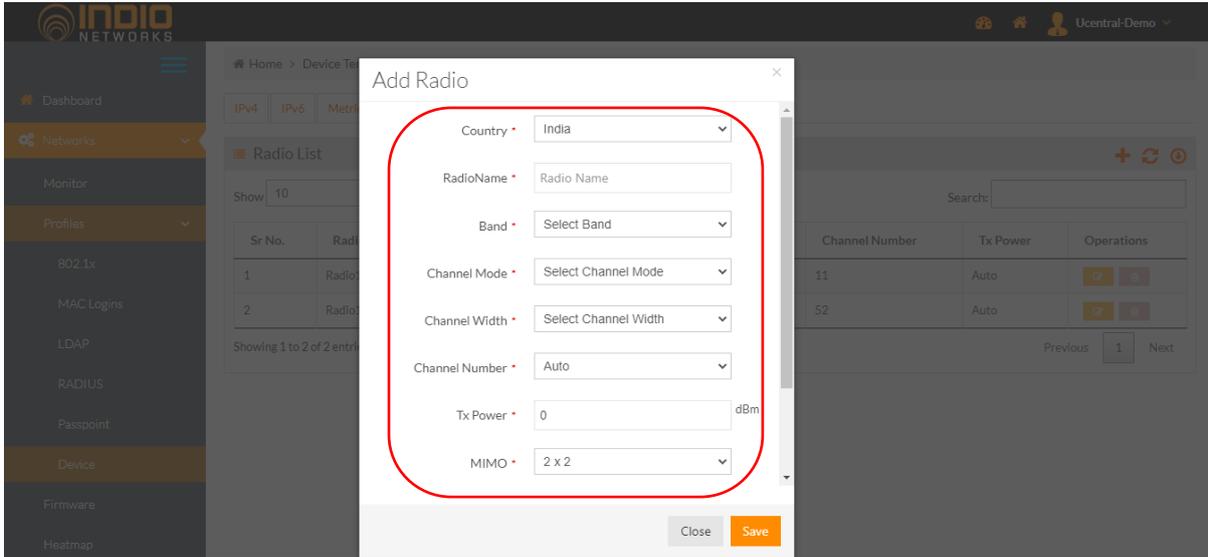
Fill in the required details:



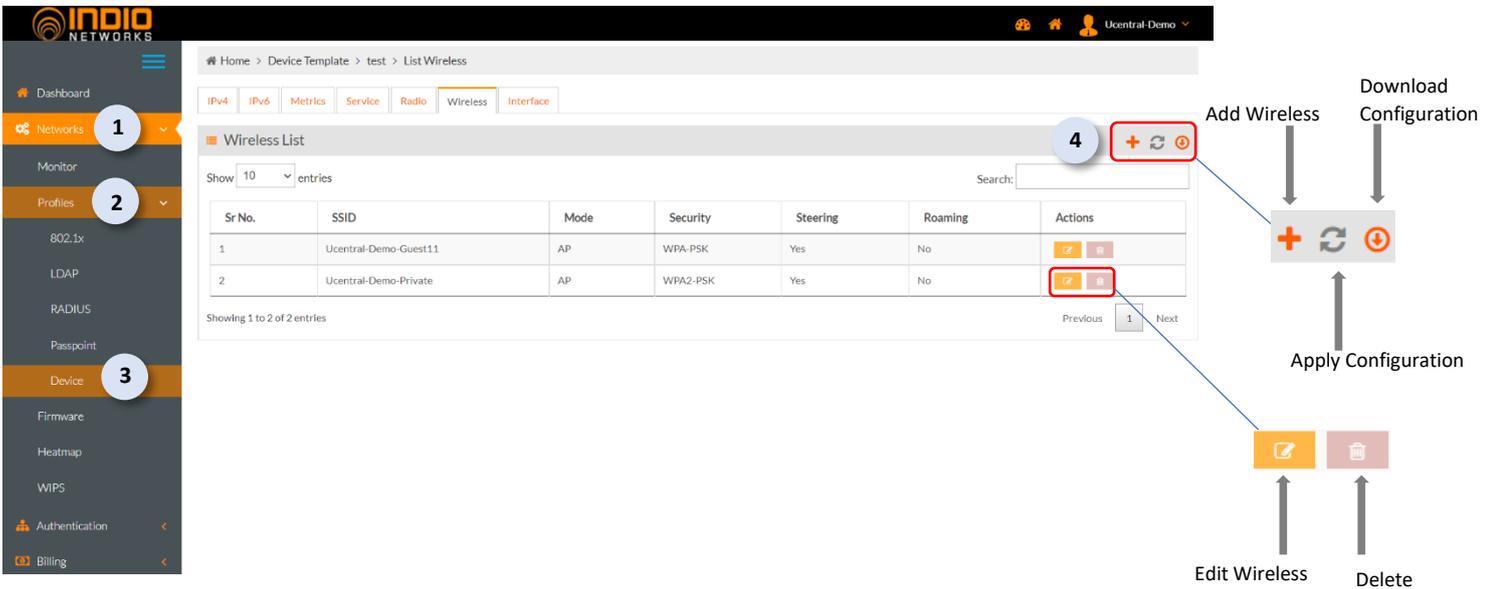
The **Radio** section deals with configuration of radio mode, channel, and power level of an access point, essential functions to consider when setting and deploying networks.

Sr No.	Radio Name	Band	Channel Mode	Channel Width	Channel Number	Tx Power	Operations
1	Radio1_2G Band	2G	11n	20	11	Auto	[Edit] [Delete]
2	Radio1_5G Band	5G	11ac	80	52	Auto	[Edit] [Delete]

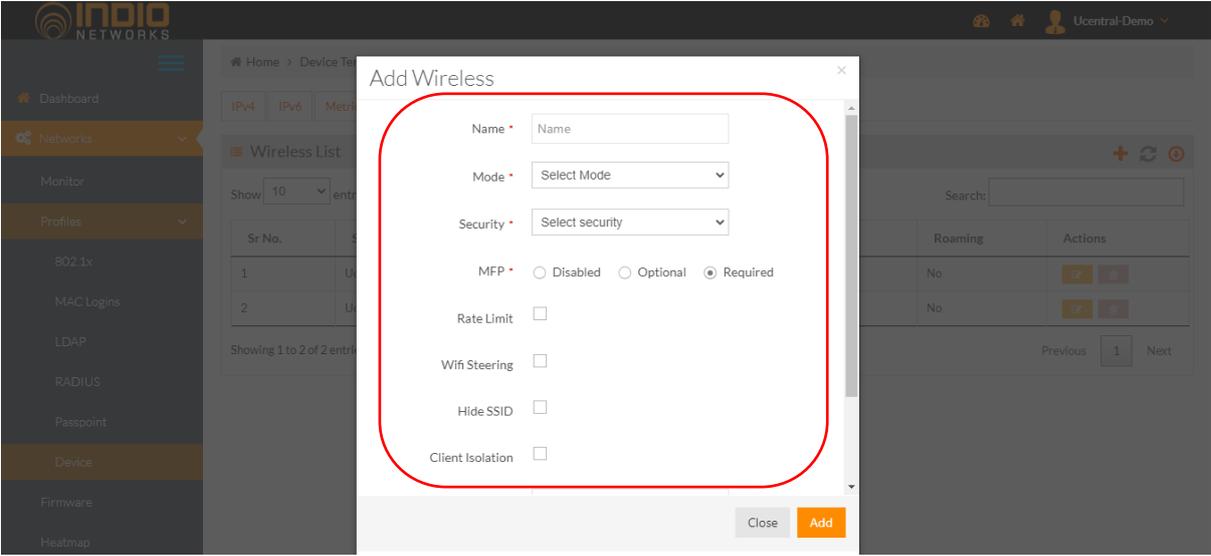
Fill in the required details:



The **Wireless** section is focused on ensuring that your WiFi network is secure and protected from unauthorized access or interference. One of the options available to you is the ability to set a unique SSID (Service Set Identifier) for your network, which is essentially the name that your WiFi network will be identified by.



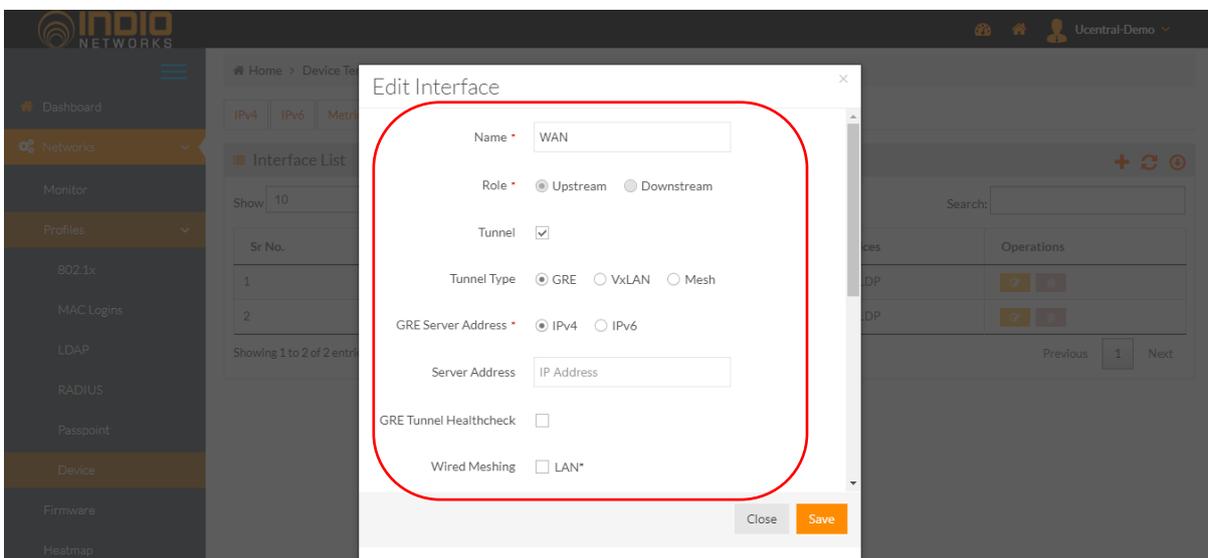
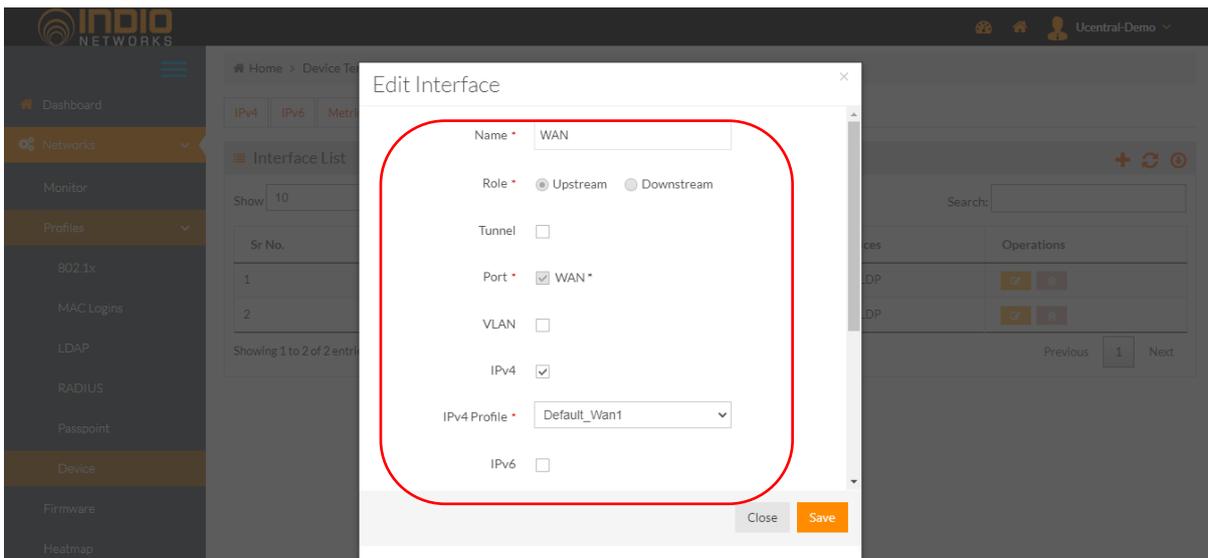
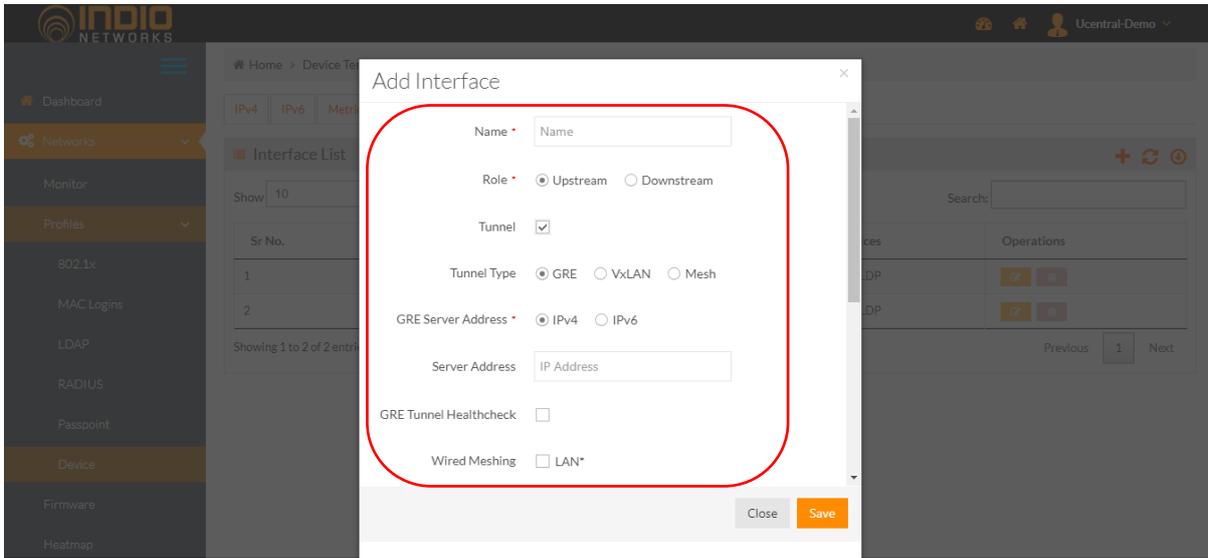
Fill in the required details:



The **Interface** section describes the logical network interfaces of the device. Interfaces as their primary have a role that is upstream, downstream, guest network, etc.

Sr No.	Name	Role	Ports	Services	Operations
1	WAN	upstream	WAN*	SSH, LLDP	[?] [] []
2	LAN	downstream	LAN*	SSH, LLDP	[?] [] []

To add or edit the Interface, fill in the required details:



2. Access Point Provisioning

This section allows you to add an access point in your network.

1

2

3

Sr.No	AP Name	MAC Address	Hotspot	Vendor	Model	Channel	Clients	Lastseen	IP Address	Action
1	72:6D:EC:0A:2E:B9	72:6D:EC:0A:2E:B9	QA_venue1	-	305AC /Indoor	-	-	-	-	[Icons]
2	0006AED32F72	00:06:AE:D3:2F:72	802.1x_Rajendra	Himachal Futuristic Communications Ltd	HFCL ION4	-	-	-	-	[Icons]
3	0006AED3228E	00:06:AE:D3:22:8E	802.1x_Rajendra	Himachal Futuristic Communications Ltd	HFCL ION4	-	-	-	-	[Icons]
4	00:06:AE:7F:FD:C4	00:06:AE:7F:FD:C4		Himachal Futuristic Communications	HFCL ION4	-	-	-	-	[Icons]

Fill in the required details in order to add a new access point.

Home > NMS > New Access Point

Dashboard Hotspot Networks Access Points **New Access Point** Events

New Access Point

Access Point Information

Device Name *

Hotspot * Select Venue

Device Model * Select an Option

MAC Address *
(Mac Address Format: 70:6D:EC:03:06:2B)

Device Profile * Select Device Profile

AP Location Tag *

3. Access Point Command Section

This section defines various commands that can be given to the access points.

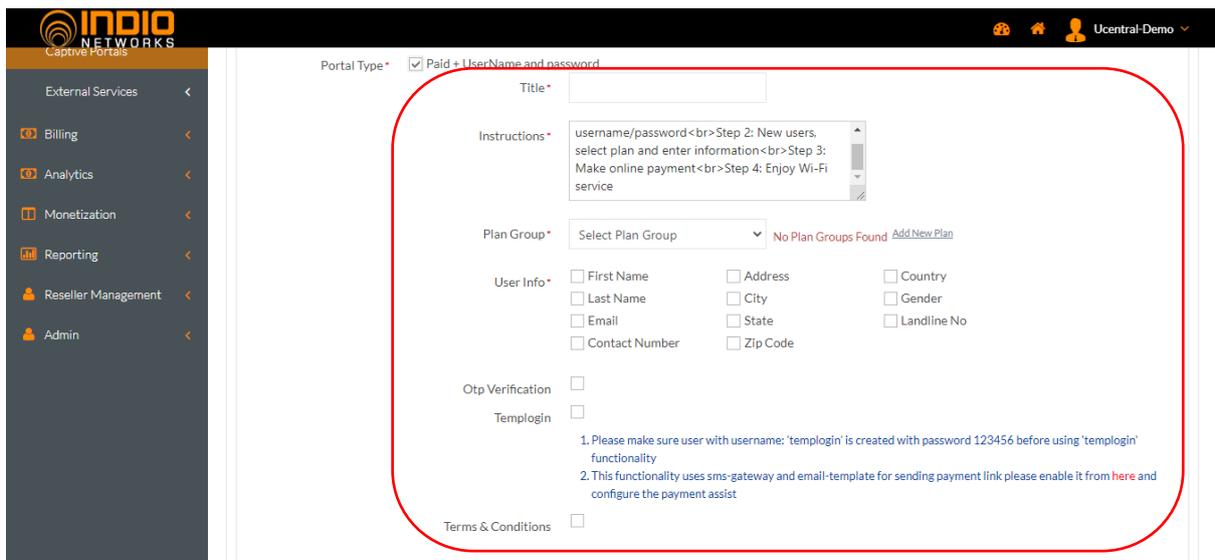
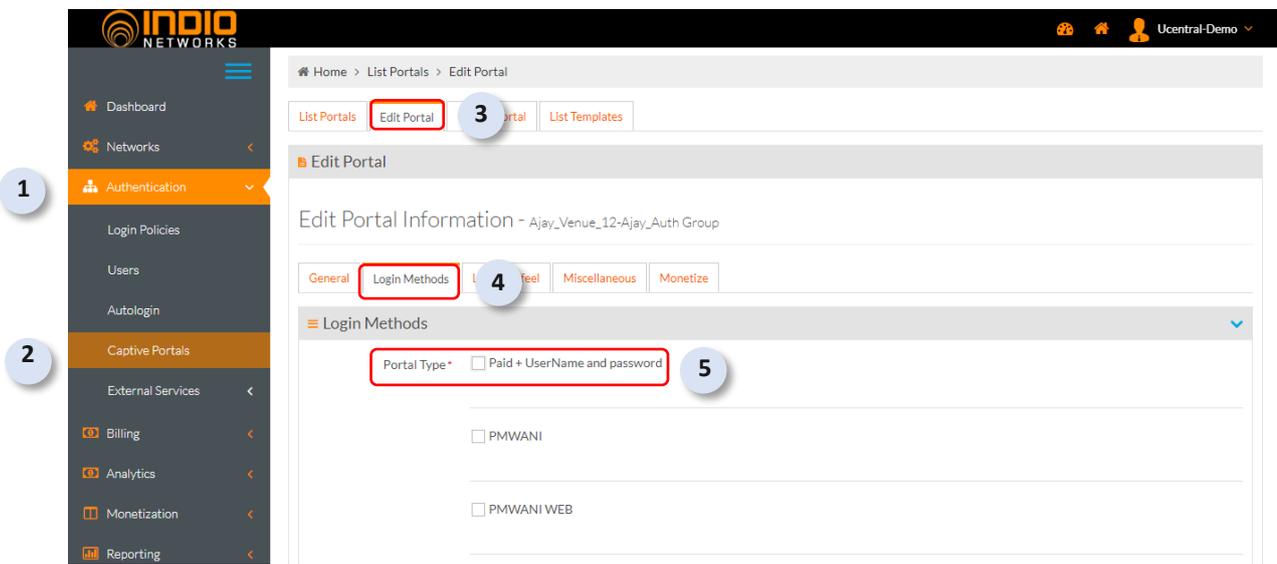
Reboot	Reboot a device
Firmware upgrade	Upgrade a device
Wifi-Scan	Launch a wifi scan for a device
Connect	Get the rtt parameter to initiate a session with AP
Blink	Blink the LEDs on a device
Trace	Launch a trace for a device
Factory Reset	Factory reset a device
Configure	Configure a device by passing a raw json config profile
Telemetry	Request a telemetry stream either on screen using websocket or to backend over kafka

4. User Authentication

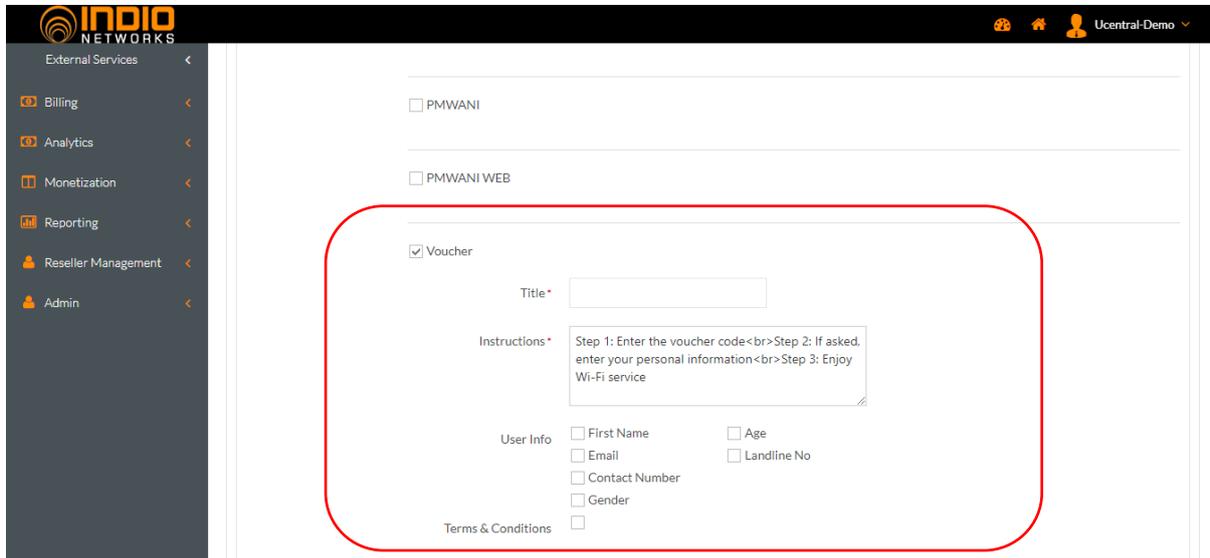
This section includes various methods to authenticate a user. Following are the different methods by which you can authenticate a user:

1. Captive Portal with Username and Password

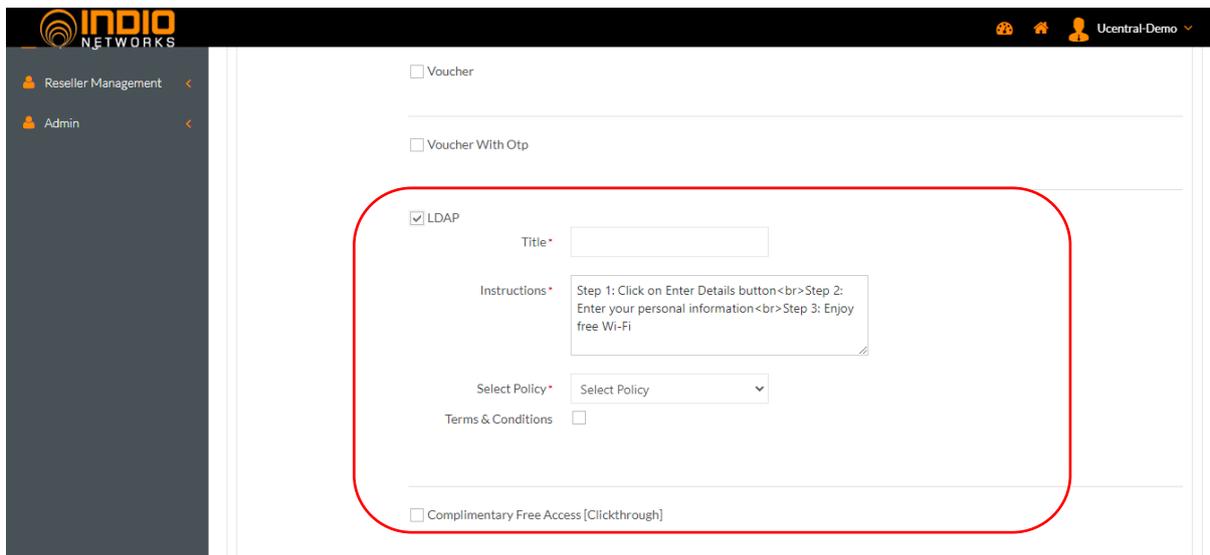
Following steps show the process of setting up a captive portal with username and password:



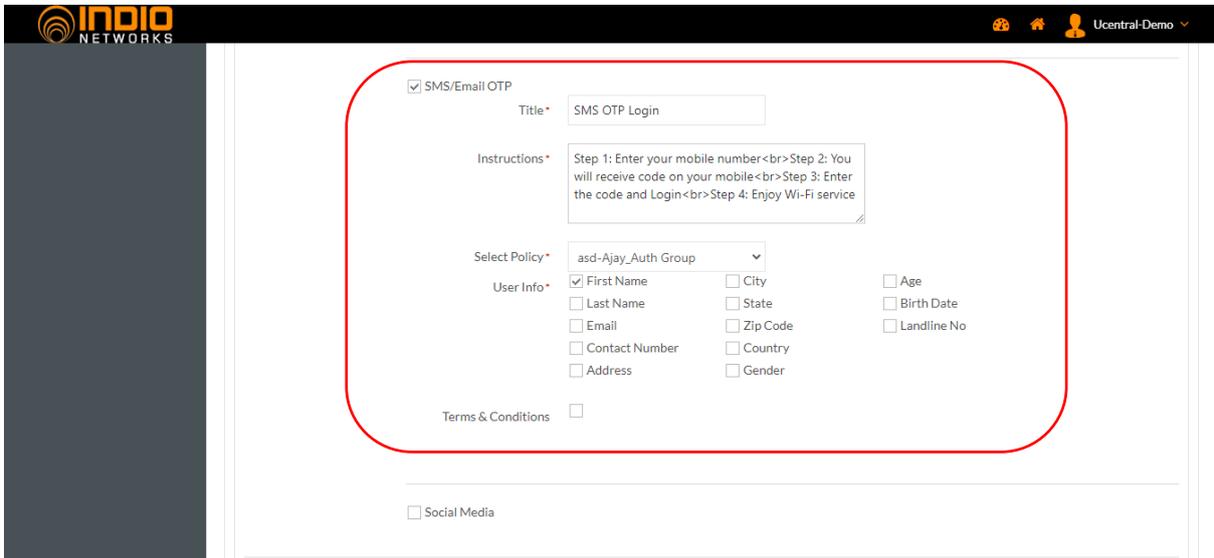
2. Captive Portal with Voucher



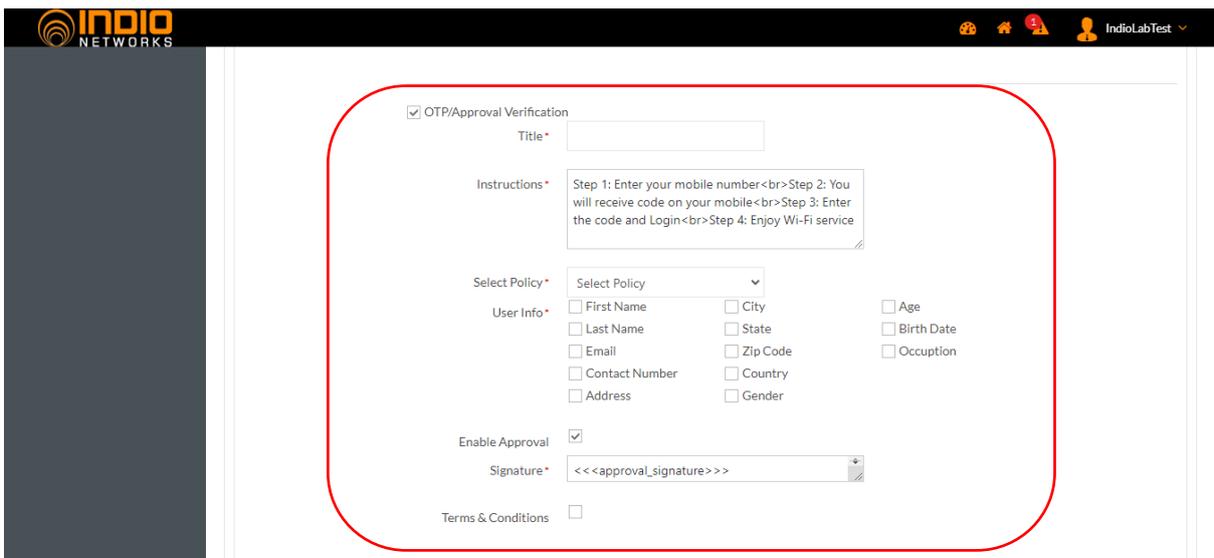
3. Captive Portal with LDAP/AD



4. Captive Portal with SMS/Email OTP



5. Captive Portal with Approval Verification



6. Captive Portal with Social Media

INDIO NETWORKS Ucentral-Demo

Social Media

Title *

Instructions * Step 1: Select social media option
Step 2: Enter social media login credentials
Step 3: Confirm permissions
Step 4: Enjoy Wi-Fi service

Select Policy *

Social Media Type * Facebook LinkedIn Twitter Google Instagram

Terms & Conditions

Captive portal templates

Home > Authentication > Captive Portals > List Portals

List Portals | Create Portal | List Templates

List Portals

Networks: Template Name:

#	Portal URL	Gateway	Network	Created Date	Operations
1	https://uwios-dev-portal.indionetworks.com/portal/default/index.php?n=wios&c=17&l=170	TIP OpenWiFi AP 2.0	Ajay_Venue_12-Ajay_Auth Group	01/11/2022 11:16:41	
2	https://uwios-dev-portal.indionetworks.com/portal/default/index.php?n=wios&c=17&l=286	TIP OpenWiFi AP 2.0	QA_venue1-QA-auth1	27/06/2022 13:09:51	
3	https://uwios-dev-portal.indionetworks.com/portal/default/index.php?n=wios&c=17&l=283	TIP OpenWiFi AP 2.0	QA_venue-QA-auth	22/06/2022 14:42:56	
4	https://uwios-dev-portal.indionetworks.com/portal/default/index.php?n=wios&c=17&l=240	TIP OpenWiFi AP 2.0	802.1x_Rajendra-1xTest_Rajendra	09/06/2022 15:34:13	
5	https://uwios-dev-portal.indionetworks.com/portal/default/index.php?n=wios&c=17&l=199	TIP OpenWiFi	Ax_Demo_Venue-	07/01/2022	

Legend: Preview, Edit, Delete

General settings

The screenshot displays the 'General settings' page in the INDIO NETWORKS interface. The sidebar on the left contains navigation items: Users, Autologin, Captive Portals (highlighted), External Services, Billing, Analytics, Monetization, Reporting, Reseller Management, and Admin. The main content area has tabs for General, Login Methods, Look and feel, Miscellaneous, and Monetize. The 'General' tab is active, showing a checkbox for 'Allow Template To Change Portal Configurations' which is checked. Below this is a 'Gateway' dropdown menu with 'TIP OpenWiFi AP 2.0' selected, accompanied by a note: 'Note: Portal gateway should be the same as network gateway(Device type)'. The 'Language' dropdown menu is set to 'English'. Under 'Language Options', the 'English' checkbox is checked, while French, Swahili, Spanish, and Portuguese are unchecked.

Login Methods

The screenshot shows the 'Edit Portal' page in the INDIO NETWORKS interface. The sidebar on the left has 'Authentication' highlighted, with sub-items: Login Policies, Users, Autologin, Captive Portals (highlighted), External Services, Billing, Analytics, Monetization, Reporting, Reseller Management, and Admin. The main content area is titled 'Edit Portal' and 'Edit Portal Information - Ajay_Venue_12-Ajay_Auth Group'. It features tabs for General, Login Methods, Look and feel, Miscellaneous, and Monetize. The 'Login Methods' tab is active, displaying a 'Portal Type' dropdown menu with the following options: 'Paid + UserName and password', 'PMWANI', 'PMWANI WEB', 'Voucher', and 'M + M + M + M'. All options are currently unchecked.

Look and feel

The screenshot shows the 'Look and feel' configuration page for a captive portal. The left sidebar contains navigation options: Users, Autologin, Captive Portals (selected), External Services, Billing, Analytics, Monetization, Reporting, Reseller Management, and Admin. The main content area has tabs for General, Login Methods, Look and feel (active), Miscellaneous, and Monetize. Under the 'Look and feel' section, there are fields for:

- Logo Image: A preview of the INDIO NETWORKS logo with a 'Change' button. A note specifies: 'NOTE! Max Size: 100 KB. Allowed Extensions: gif, jpg, jpeg, png, x-png. Better logo resolution: 330 X 150.'
- Link on Logo Click: A text input field containing 'http://www.wifi-soft.com' with a note: 'e.g: http://www.demo.com or http://demo.com'
- Location Name: A text input field containing 'Ajay_Venue_12-Ajay_Auth Group'
- Portal frame: A color selection dropdown menu with a note: 'NOTE! This will change portal frame color'
- Portal Enter color: A color selection dropdown menu.

Miscellaneous

The screenshot shows the 'Miscellaneous' configuration page for a captive portal. The left sidebar is expanded to show 'Authentication' options: Networks, Authentication (selected), Login Policies, Users, Autologin, and Captive Portals. The main content area has tabs for General, Login Methods, Look and feel, Miscellaneous (active), and Monetize. Under the 'Miscellaneous' section, there are:

- Terms & Conditions: A text area containing HTML code: '<p>Terms and Conditions of Use <p> By accessing and using Internet Services, you agree that you have read, understand, and accept the Terms and Conditions below for all use. If you do not agree to this policy, it is recommended that you do not use this service. <p> 1. Internet'.
- Footer: A text area containing HTML code: 'Internet Provided by Wifi-Soft'. Below this is a checkbox for 'Support Number' which is currently unchecked.

The screenshot shows the INDIO NETWORKS interface. At the top, there is a header with the logo and a user profile 'Ucentral-Demo'. Below the header, there is a URL 'e.g: http://www.demo.com or http://demo.com'. The main content area contains four rows of configuration options, each with a label and a checkbox:

- Self Care Login Enable Self Care Login
- Restrict users to this network
- Enable End User Ticket
- Captive Portal Bypass

At the bottom of the configuration area, there is a '+ Submit' button.

Monetize

The screenshot shows the INDIO NETWORKS interface with a sidebar menu on the left. The 'Authentication' menu is expanded, showing options like Login Policies, Users, Autologin, Captive Portals, External Services, Billing, Analytics, Monetization, Reporting, and Reseller Management. The main content area is titled 'Edit Portal' and shows 'Edit Portal Information - Ajay_Venue_12-Ajay_Auth Group'. There are tabs for 'General', 'Login Methods', 'Look and feel', 'Miscellaneous', and 'Monetize'. The 'Monetize' tab is selected and expanded, showing the following options:

- Push Notifications Push Notifications
- Ads Enable Ads
- Reviews Enable Reviews
- Survey Enable Survey

User Policies

1
2

#	Policy Name	Date Created	Last Updated	Is Default	Operations
1	Sanity_QA	22/06/2022	22/06/2022	No	
2	asd-Ajay_Auth Group	12/08/2021	12/08/2021	No	

Any change in this policy will affect 1 user's restriction.

Policy Name *

Concurrency Limit

Max Devices Limit

Daily Session Count

Session Timeout Minutes

Idle Timeout Minutes

Daily Time Counts Minutes

INDIO NETWORKS Ucentral-Demo

Reseller Management < Admin <

Daily Time Quota Minutes

Total Time Quota Minutes

Daily Bandwidth Quota MB

Total Bandwidth Quota MB

Download Rate Mbps

Upload Rate Mbps

Validity Interval Days

Auto Renewal * Note : Valid only for free user's validity interval

Is Default this policy is already select as default policy, if you want to change then select checkbox.

Filter ID
* Note : Valid only for vendors like (Meraki etc.)

INDIO NETWORKS Ucentral-Demo

Dashboard Networks Authentication Login Policies Users Autologin Captive Portals External Services Billing Analytics Monetization Reporting Reseller Management

List Policies **New Policy**

New Policy

Add New Login Policy

Policy Name*

Concurrency Limit

Max Devices Limit

Daily Session Count

Session Timeout Minutes

Idle Timeout Minutes

Daily Time Quota Minutes

INDIO NETWORKS Ucentral-Demo

Reseller Management < Admin <

Total Time Quota Minutes

Daily Bandwidth Quota MB

Total Bandwidth Quota MB

Download Rate Mbps

Upload Rate Mbps

Validity Interval Days

Auto Renewal * Note : Valid only for free user's validity interval

Is Default this policy is already select as default policy, if you want to change then select checkbox.

Filter ID
* Note : Valid only for vendors like (Meraki etc.)

+ Submit

5. External Gateway Configuration

The Gateway Configuration options allow you to change the settings of the gateway, which Indio Cloud installs and configures by default.

SMS Gateway Configuration

What is SMS Gateway?

SMS Gateway is convenient when you want to send SMS but not from your phone. Short Message Service (SMS) gateway is a mechanism by which SMS messages are sent and received. SMS gateways facilitate and streamline text messaging processes for organizations, and will often do some of the conversion to different formats.

SMS Gateway in Indio Cloud:

The SMS Gateway feature in **Indio Cloud** facilitates user's mobile number verification with the use of OTP (One Time Password) mechanism. When the user enters their mobile number on the captive portal, they receive an SMS OTP which is used to verify their number.

The various uses of configuring SMS gateway are (following are the templates):

1. User Registration Success
2. User Payment Success
3. User Forgot Password
4. User FUP Alert
5. Login Assist
6. Voucher Alert
7. Subscriber Request
8. Forgot Password
9. Resend Email Template
10. Verification Link Retailer
11. New Distributor Account
12. New Retailer Account
13. Verification Link Distributor
14. New Distributor
15. New Retailer
16. Resend OTP
17. New Retailer Account Through Distributor
18. New Sub Retailer

INDIO NETWORKS Ucentral-Demo

SMS Gateway Information

SMS Gateway: SMSGatewayHub Version 1

API Username: wifisoftservice

API Password: w1f1s0ft@indio

API ID: WIFISS

SMS Attempts: 2

SMS Template: Verification code : <<<VERIFICATION CODE>>> . Some hint here
WIFISOFT SERVICES

Buttons: Test SMS Gateway, Default Template, Restore Template, Get Balance, + Submit

SMS Template: Verification Code = <<<VERIFICATION CODE>>>

Buttons: Test SMS Gateway, Default Template, Restore Template, Get Balance

SMS Template: Verification code : <<<VERIFICATION CODE>>> .
WIFISOFT SERVICES

Buttons: Test SMS Gateway, Default Template, Get Balance

Payment Gateway Configuration

What is Payment Gateway?

A payment gateway is a transaction medium between a merchant and a consumer. This technology is the simplest way to collect payments digitally. There are four parties that involve the payment gateway process: the customer, the merchant, the issuing bank, and the receiving payment or acquiring bank.

Payment Gateway in Indio Cloud:

When the provider configures a paid captive portal as a login method, the payment gateway helps in processing the payments that are received from the end user.

The various payment gateways that are integrated in **Indio Cloud** are as follows:

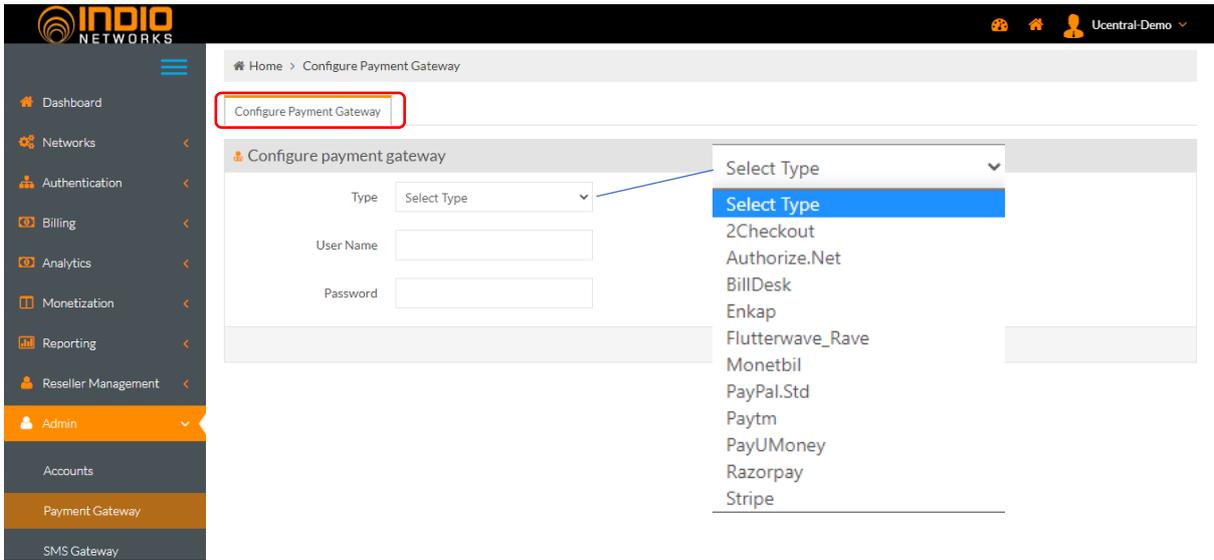
P.S- Payment Gateways can be customized as per requirement.

1. 2Checkout
2. Authorize.Net
3. BillDesk
4. Enkap
5. Flutterwave_Rave
6. Monetbil
7. PayPal.Std
8. Paytm
9. PayUMoney
10. Razorpay
11. Stripe

The screenshot shows the 'Payment Gateway List' interface in the Indio Cloud Admin panel. The table contains one entry:

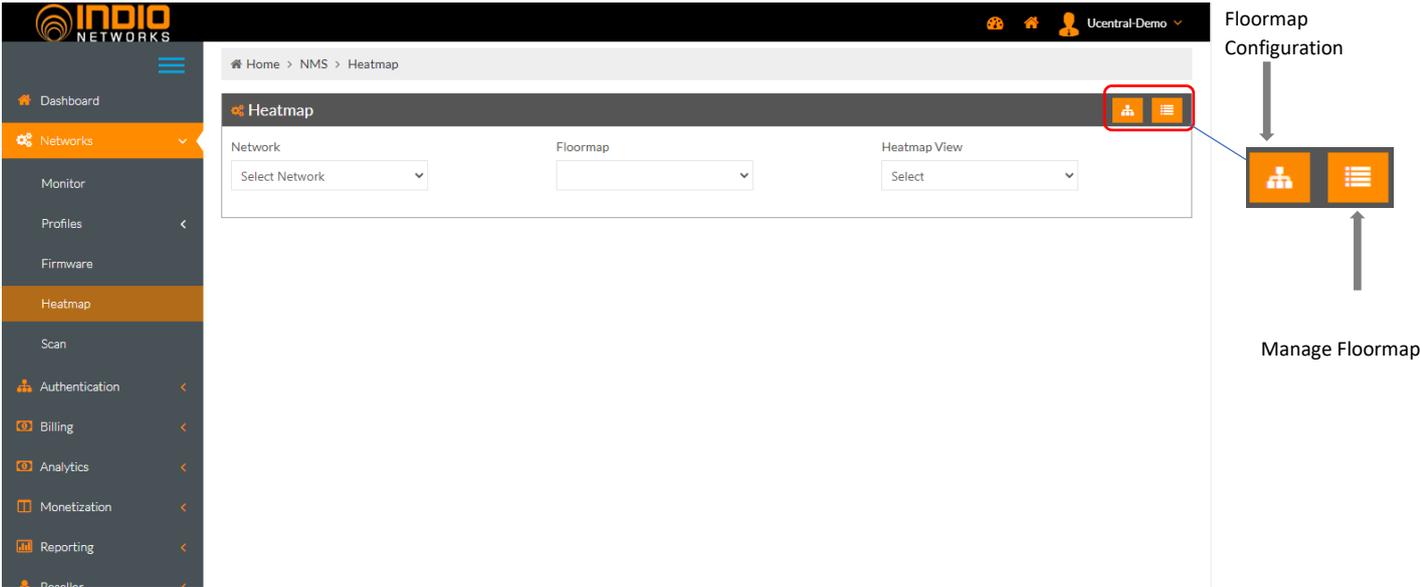
#	Name	Type	Config	Gateway Type	Currency Code	Status	Operations
1	Ucentral-Demo	Customer	Not Configured	-	-	-	<input type="checkbox"/> <input type="checkbox"/>

Annotations in the image include a red circle around the 'Edit' icon in the 'Operations' column of the first row, and arrows pointing to 'Edit' and 'View' labels next to the respective icons.

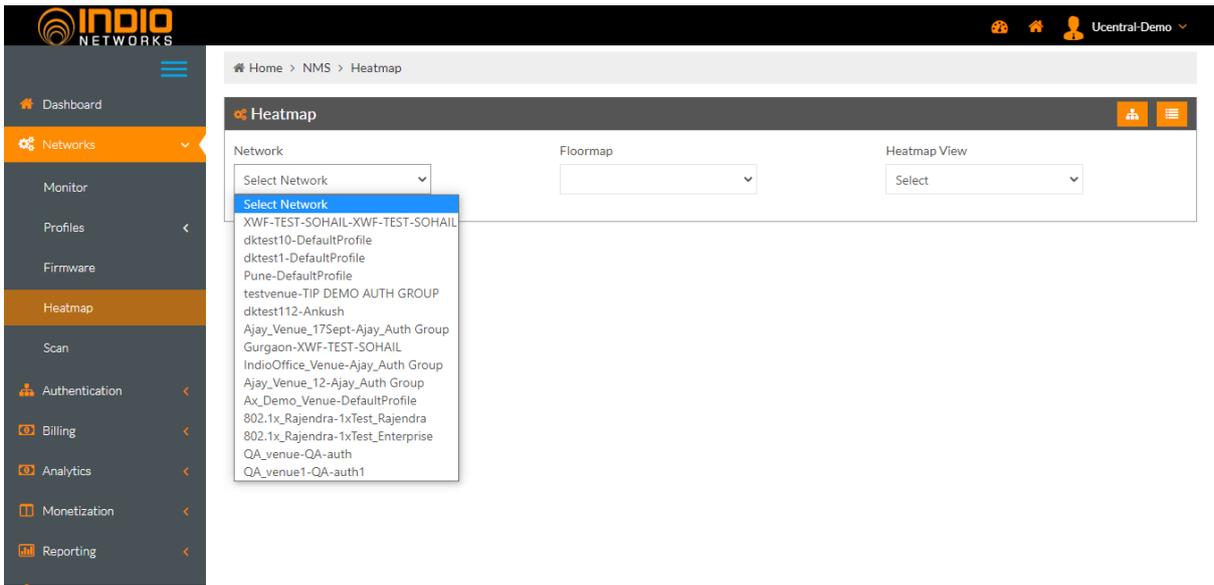


6. Heatmap

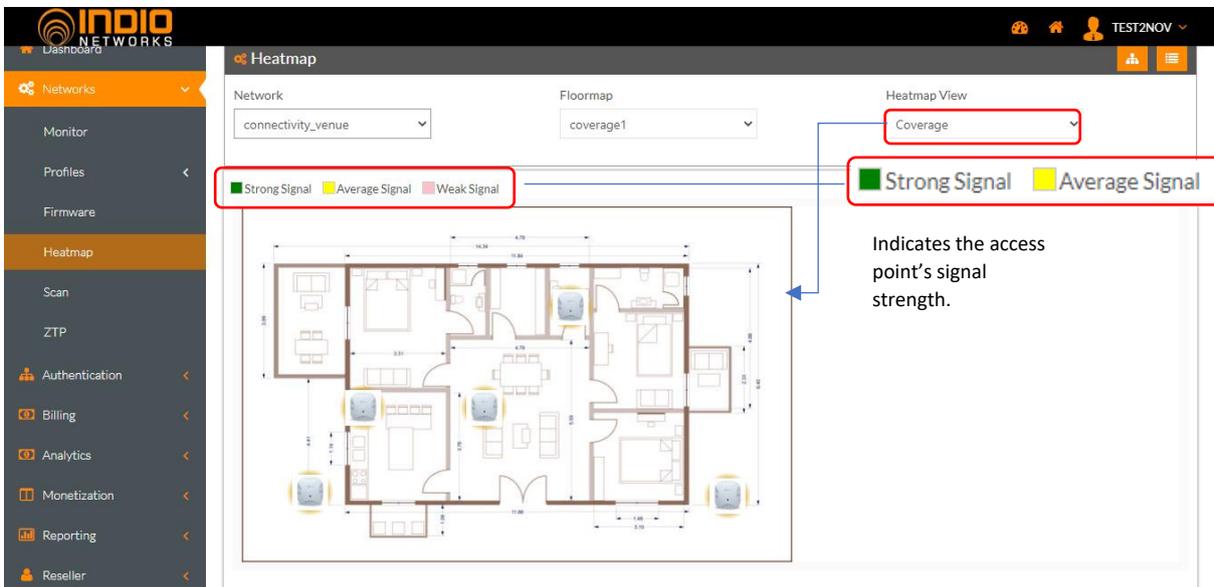
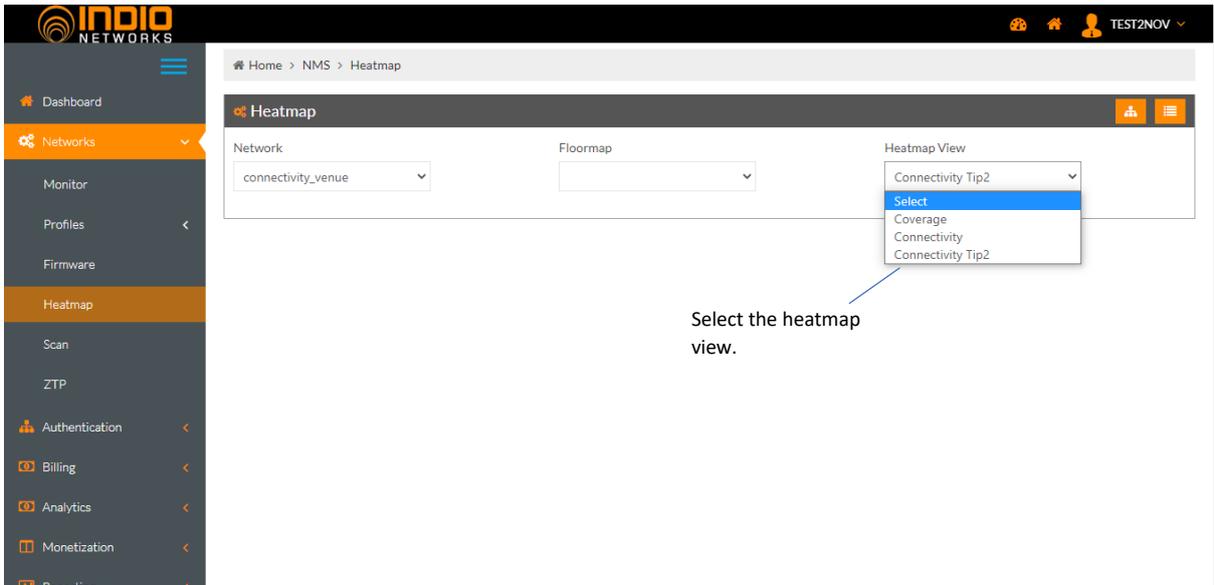
A Wi-Fi heatmap is a visual representation of the wireless signal coverage and strength. It is an L2 topology diagram where you can add access points and optionally the controller to which the access points are associated with. The heatmaps help you visualize wireless signal coverage on a building floor plan.

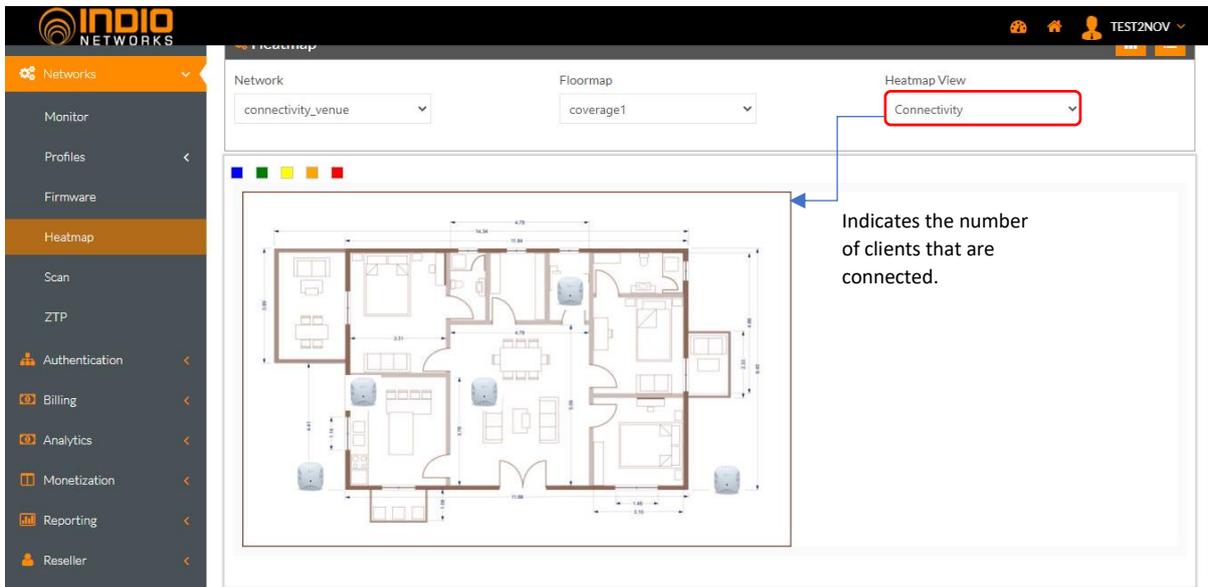


1



2

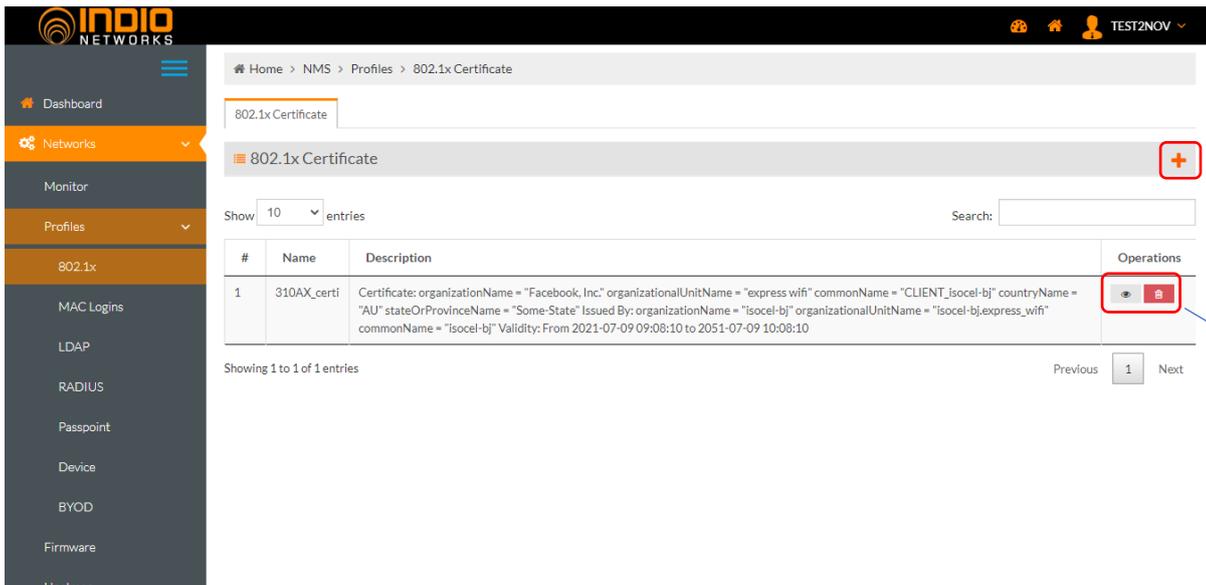




7. 802.1x Authentication

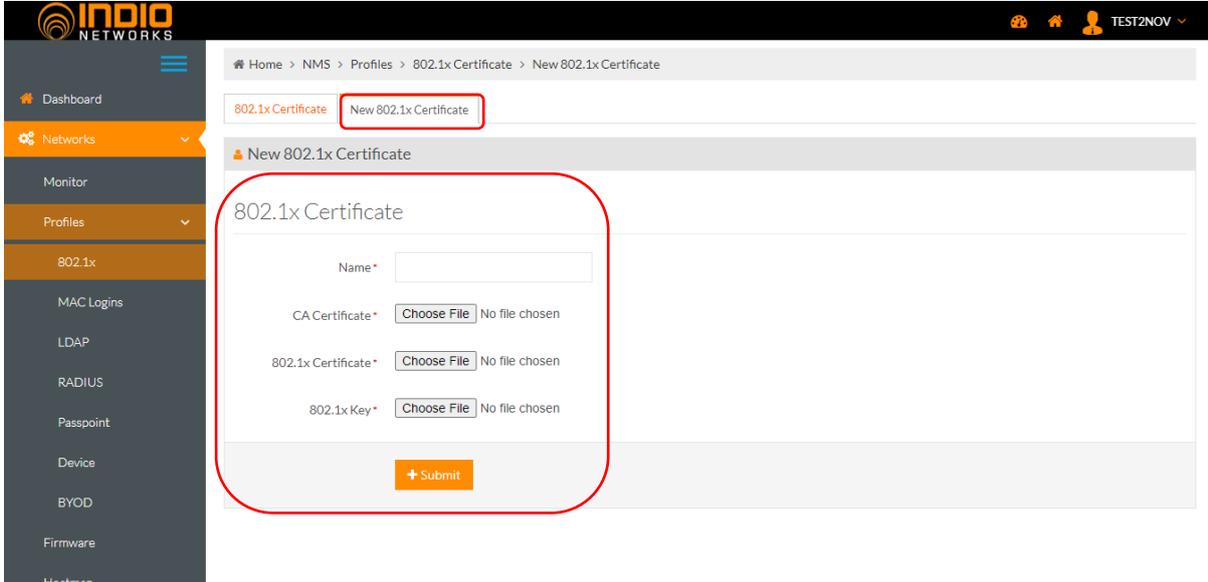
802.1x is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. It allows you to create and enforce policies that can restrict access according to an individual's role or their permissions.

- 1
- 2
- 3



- 4 Add
- View
- Delete

The 802.1x authentication should be attached to the specific device profile. It is essential to upload the certificates related to 802.1x.



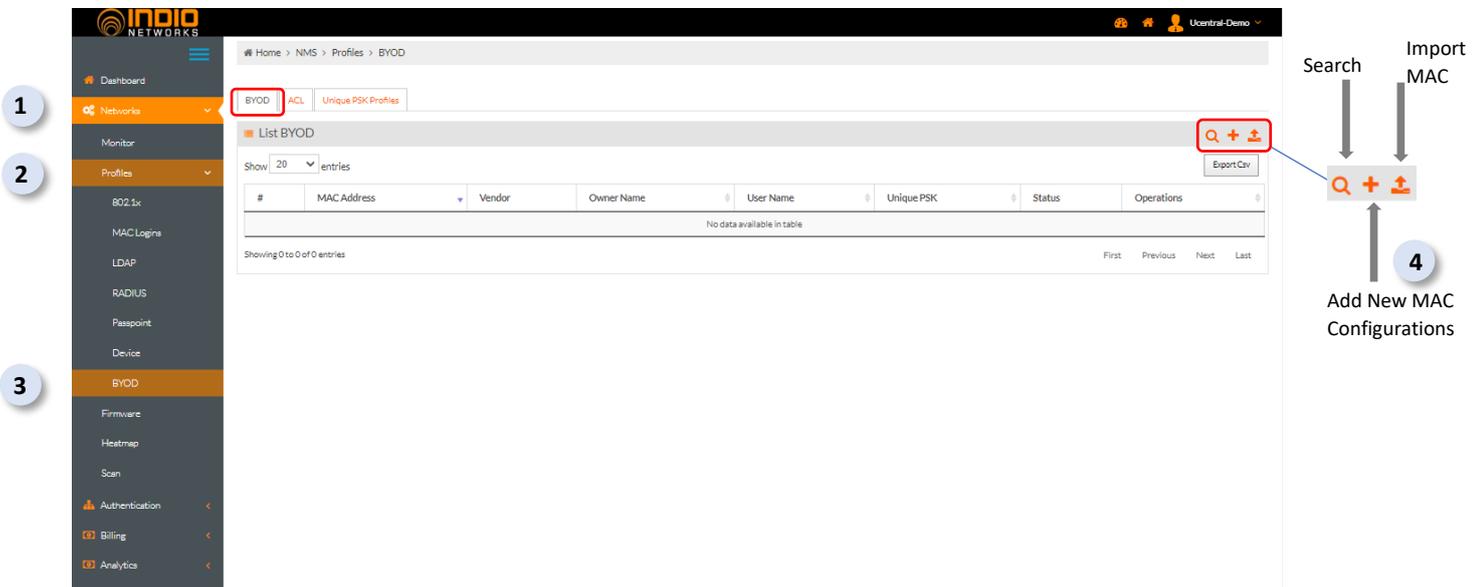
8. BYOD (Bring Your Own Device)

What is BYOD?

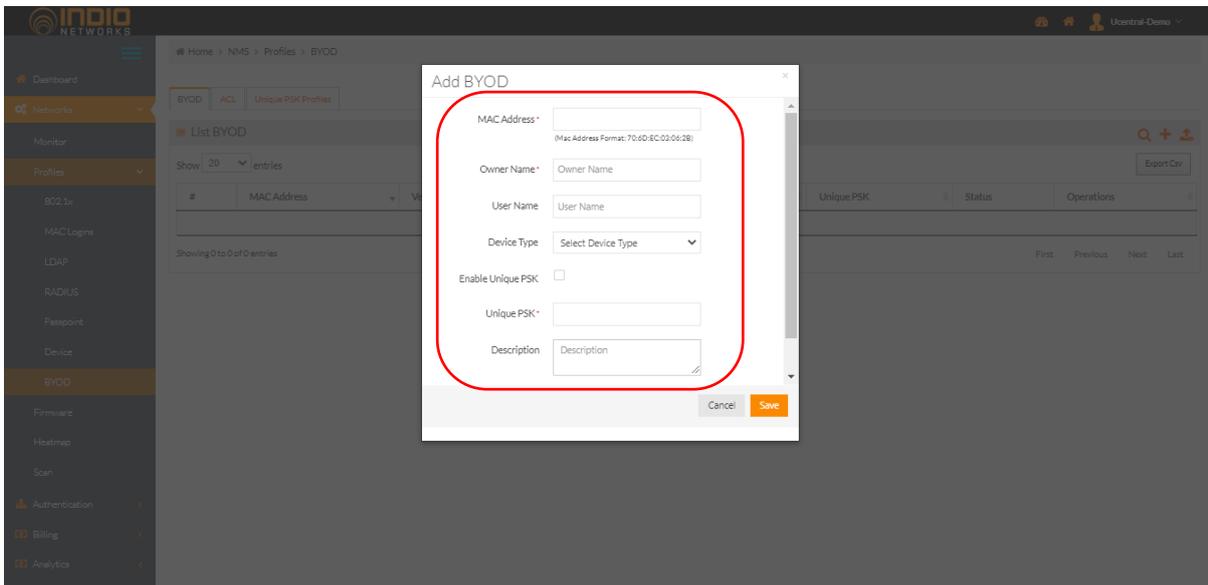
Bring your own device (BYOD) refers to the trend of employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

BYOD in Indio Cloud:

Any user who wants to access the network with their personal devices can be authorized using the BYOD policy.



Fill in the required details.



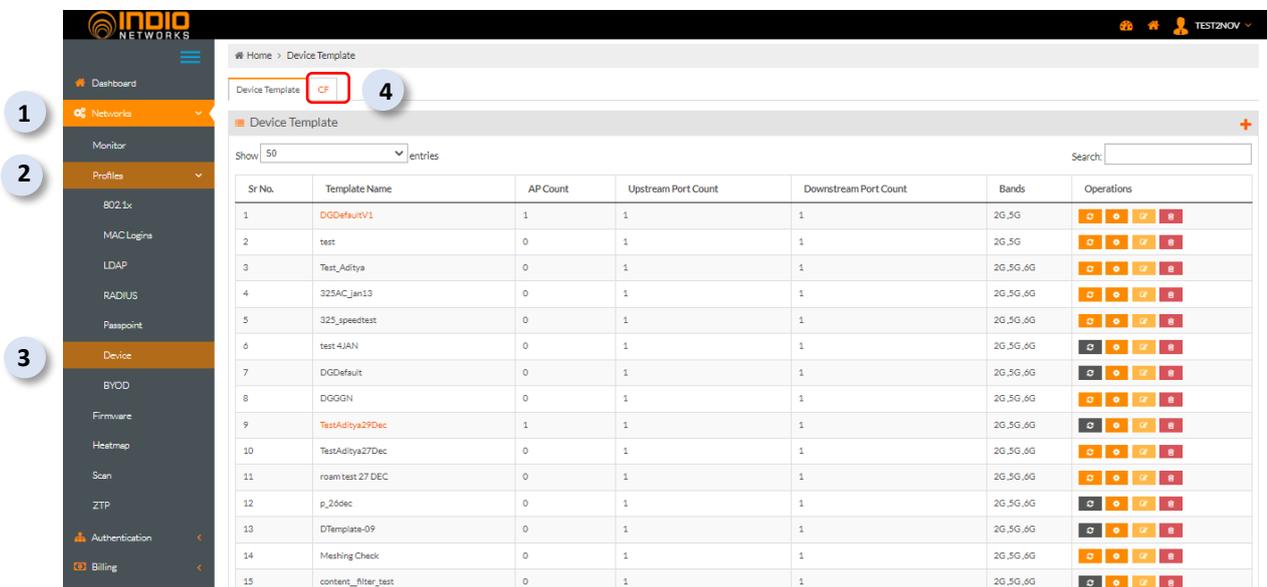
9. Content Filtering

What is Content Filtering?

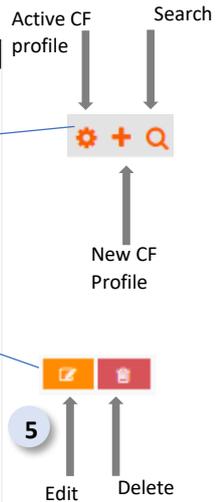
Content filtering is the use of a program to screen and/or exclude access to web pages or email deemed objectionable. Content filtering works by specifying content patterns — such as text strings or objects within images, that, if matched, indicate undesirable content that is to be screened out. A content filter will then block access to this content.

Content Filtering in Indio Cloud:

Content filtering in **Indio Cloud** enables you to block domains, content by different categories or keywords.



#	CF Profile Name	Whitelist Domain	Blacklist Domain	Block Category Count	Active Network Count	Description	Operations
1	AdityaTest	Yes	Yes	0	1	jgugb	[Edit] [Delete]
2	CF TEST	Yes	Yes	2	2	Cg Test	[Edit] [Delete]
3	test20DEC	No	No	4	-	content_filter_test	[Edit] [Delete]
4	TEST7dec	Yes	Yes	1	1	test7dec	[Edit] [Delete]



CF Rule

Name: AdityaTest
Description: jgugb

Custom URL

Whitelist Domain: google.com x e.g. google.co
Blacklist Domain: whatsapp.com x e.g. whatsapp

Exception: Block Except Whitelist Domain

Category

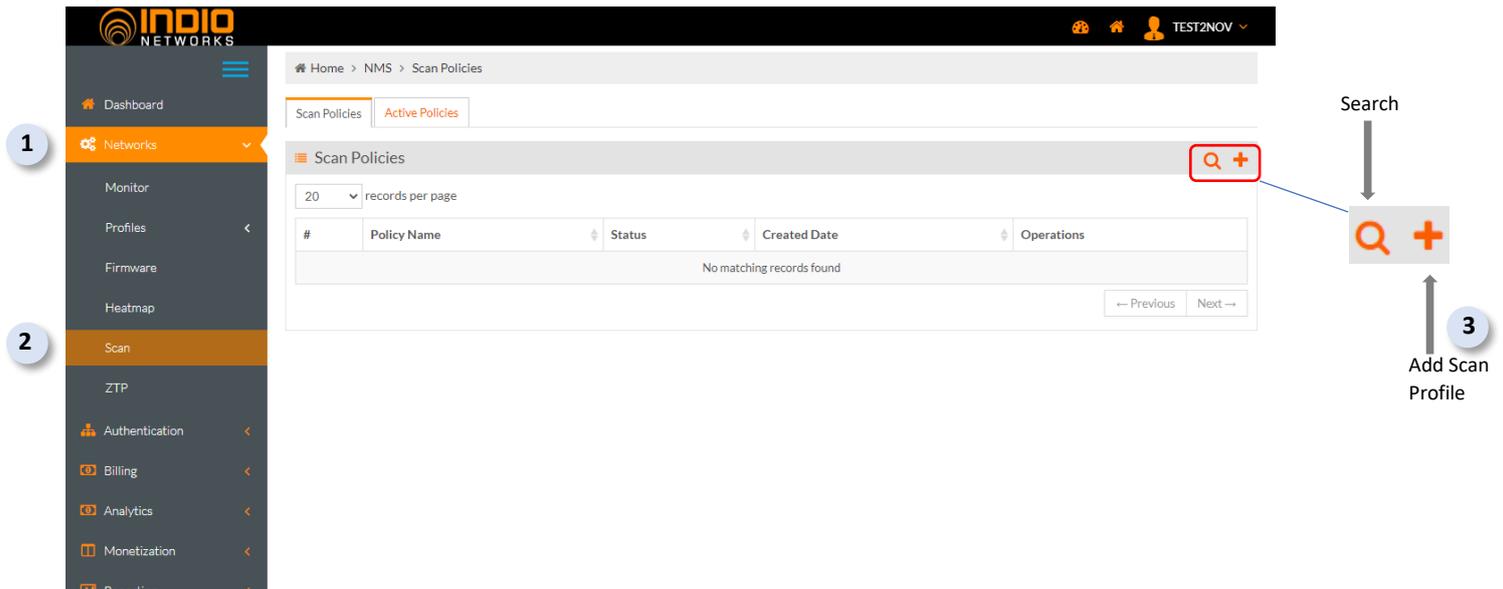
Select All

Block Category

- Abortion
- Alcohol
- Artrudes
- Audio Video
- Automobile Planes
- Beerliquorsale
- Catalogue Blu Toulouse
- Child
- Contraception
- Dare
- Dialer
- Drugs
- Education Schools
- Finance
- Finance Other
- Fortunetelling
- Gambling
- Government
- Hobby Games Misc
- Homerepair
- Hunting
- Instantmessaging
- Kidstimestwasting
- Local
- Manga
- Mixed Adult
- Ads
- Anonvpn
- Associations Religieuses
- Automobile Bikes
- Bank
- Bitcoin
- Celebrity
- Childcare
- Cooking
- Dating
- Dialers
- Dynamic
- Entertainment
- Finance Banking
- Finance Realstate
- Forum
- Games
- Guns
- Hobby Games Online
- Homestyle
- Hygiene
- Isp
- Library
- Magazines
- Marketingware
- Mobile Phone
- Adult
- Antispyware
- Astrology
- Automobile Boats
- Banking
- Blog
- Cellphones
- Cleaning
- Cryptojacking
- Ddos
- Doh
- Ecommerce
- Filehosting
- Finance Insurance
- Finance Trading
- Frencheducation
- Gardening
- Hacking
- Hobby Gardening
- Hospitals
- Imagehosting
- Jewelry
- Lingerie
- Mail
- Medical
- Moviefile
- Aggressive
- Arjel
- Audiovideo
- Automobile Cars
- Beerliquorinfo
- Books
- Chat
- Clothing
- Culinary
- Desktopillies
- Download
- Educational Games
- Filesharing
- Finance Moneylending
- Financial
- Gamble
- Good
- Hobby Cooking
- Hobby Pets
- Humor
- Indisponible
- Jobsearch
- Liste Blanche
- Malware
- Military
- Moviefile

10. WIPS

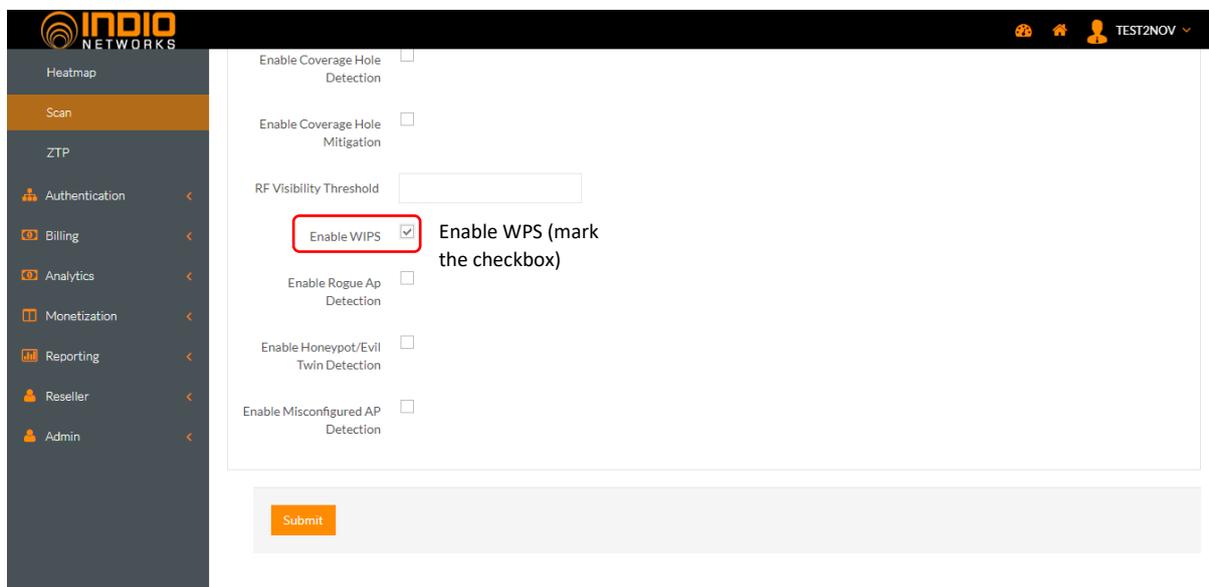
A **Wireless Intrusion Prevention system (WIPS)** operates at the Layer 2 (data link layer) level of the Open Systems Interconnection model. WIPS can detect the presence of rogue or misconfigured devices and can prevent them from operating on wireless enterprise networks by scanning the network's RFs for denial of service and other forms of attack.



1

2

3 Add Scan Profile



Enable Coverage Hole Detection

Enable Coverage Hole Mitigation

RF Visibility Threshold

Enable WIPS Enable WPS (mark the checkbox)

Enable Rogue Ap Detection

Enable Honeypot/Evil Twin Detection

Enable Misconfigured AP Detection

Submit

1. Rogue AP Detection: It helps you to identify an access point which is set to a similar frequency (and channel) as your access point. Once you are notified about the issue, you can then adjust the frequency to a different channel to avoid the conflict.

2. Honeypot/Evil Twin Detection: If an access point is having similar SSID to an existing one, this feature helps in detecting the issue.

3. Misconfigured AP Detection: If an access point fails to apply the configuration, this feature notifies you about it.

11. SysLog

Indio Cloud is responsible for storing the system and user logs in a central repository. The **Indio Cloud** system is integrated with the storage server which will be responsible for storing and archiving user logs, system logs, AP monitoring status, user browsing logs and session statistics. All logs are properly archived and stored for record keeping on the servers. Administrator can easily access the logs when required and provide the information to law enforcement agencies.

12. Events

Indio Cloud provides extensive logs of all the events that take place in your network.

Timestamp	API ID	User	Message
25/01/2023 20:50:02	AP120	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED running on low memory.
25/01/2023 17:05:06	AP117	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Up.
25/01/2023 17:05:06	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.
25/01/2023 13:49:03	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.
25/01/2023 12:50:02	AP120	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED running on low memory.
25/01/2023 12:46:03	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.
25/01/2023 12:23:03	AP116	DeveloperTest1	04:B6:BE:13:9B:E8 : 04:B6:BE:13:9B:E8 status Down.
25/01/2023 12:04:05	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.
25/01/2023 11:34:04	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.
25/01/2023 11:28:04	AP116	DeveloperTestAditya	DGGGN : 70:6D:EC:0A:87:ED status Down.

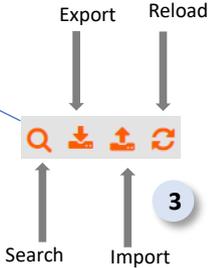
13. External User Import

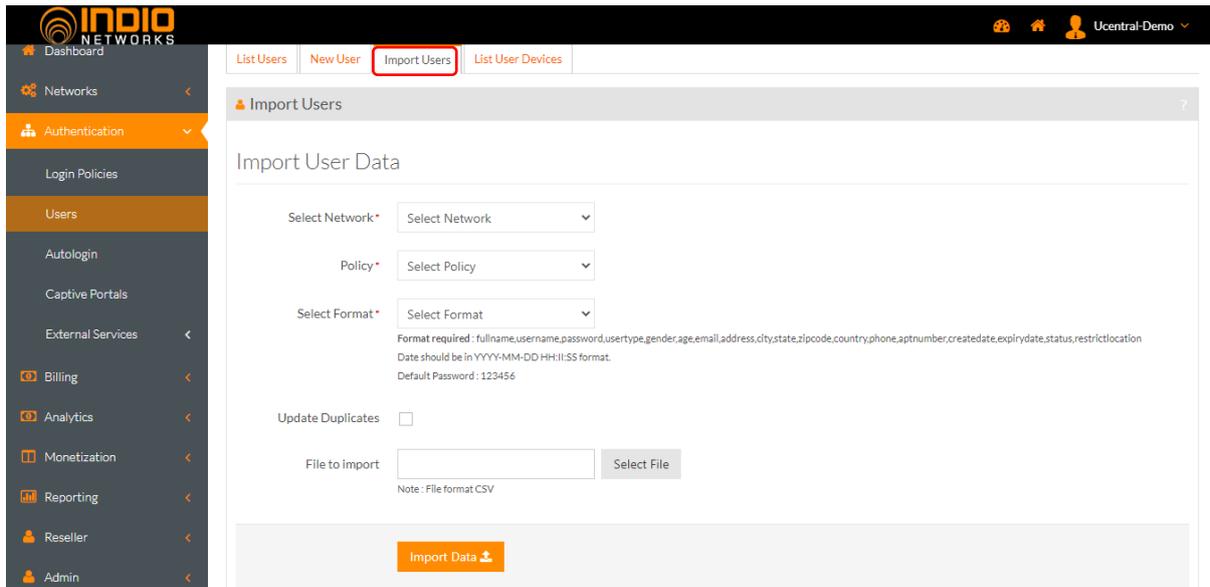
In order to import external users that have not signed up using captive portal sign-up methods, this feature is convenient to use.

1

2

#	Username	User Type	Network	Policy	Created Date	Status	Operations
1	test@test	FREE	Ajay_Venue_12-Ajay_Auth Group	asd-Ajay_Auth Group	16/11/2022 18:13:35	ACTIVE	[Eye] [Export] [Trash]
2	noname170@test	FREE	Ajay_Venue_12-Ajay_Auth Group	asd-Ajay_Auth Group	16/11/2022 8:12:36	ACTIVE	[Eye] [Export] [Trash]
3	917972704763@test	SMS	Ajay_Venue_12-Ajay_Auth Group	asd-Ajay_Auth Group	01/11/2022 1:34:51	ACTIVE	[Eye] [Export] [Trash]
4	919765918841@test	SMS	Ajay_Venue_12-Ajay_Auth Group	asd-Ajay_Auth Group	01/11/2022 1:24:23	ACTIVE	[Eye] [Export] [Trash]
5	noname283@test	FREE	QA_Venue-QA-auth	Sanity_QA	27/06/2022 2:54:29	ACTIVE	[Eye] [Export] [Trash]
6	rajendra@test	ADMIN CREATED	802.1x_Rajendra-1xT est_Enterprise	asd-Ajay_Auth Group	09/06/2022 6:22:48	ACTIVE	[Eye] [Export] [Trash]



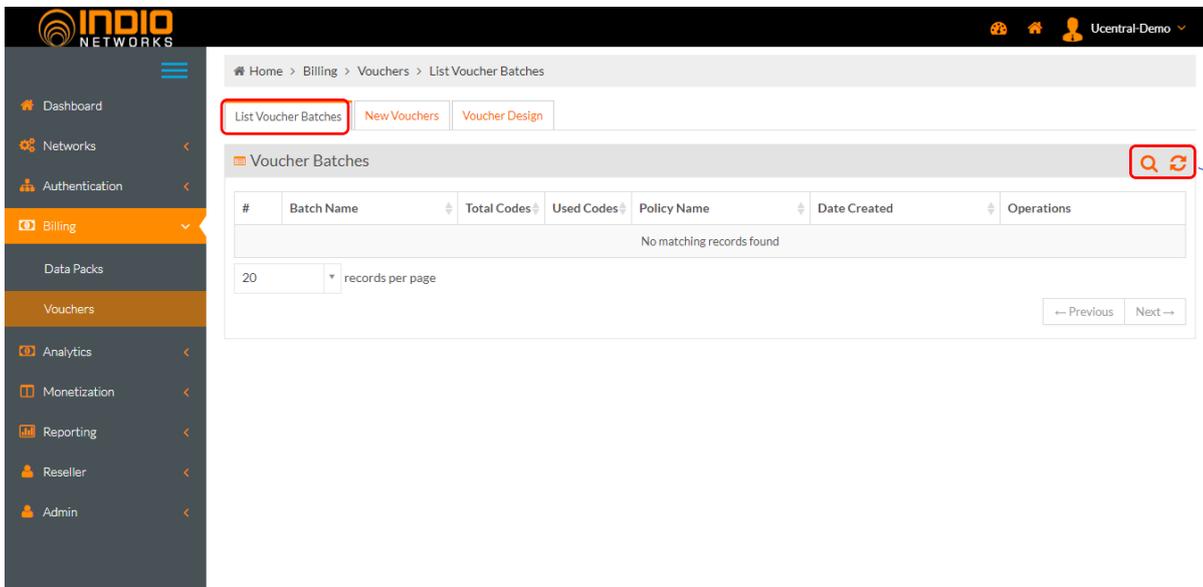


14. Voucher

Users can connect to the internet using vouchers which are created from this section. There are two types of vouchers that can be created, numeric and alphanumeric. Each voucher batch is attached with a login policy (usage quota) which gets applied to the voucher user for browsing the internet

1

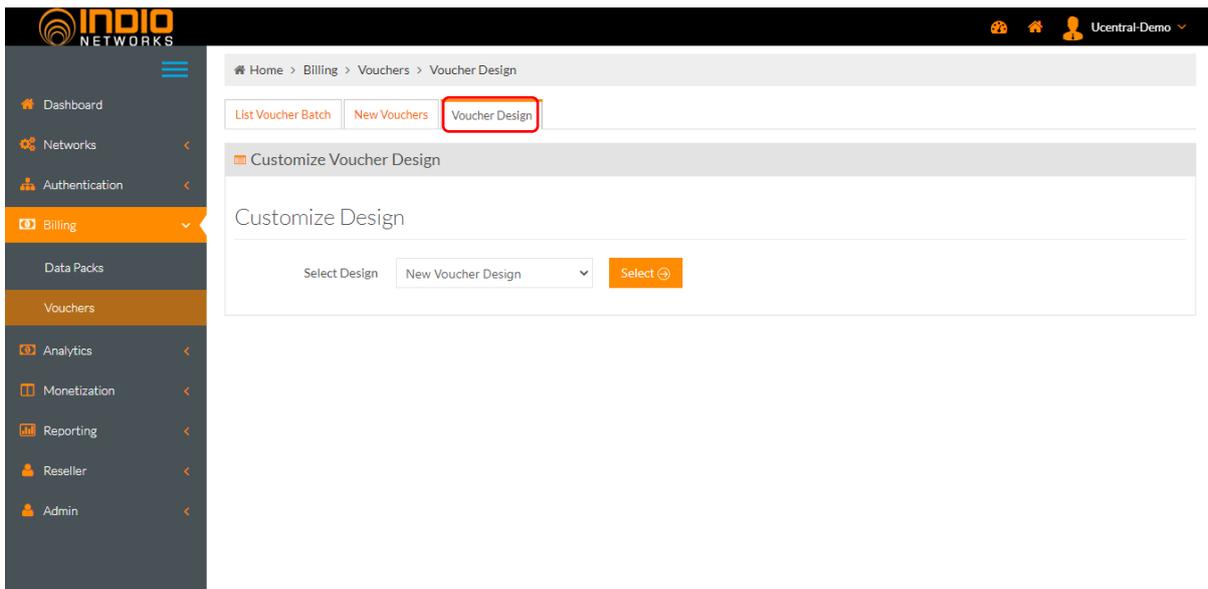
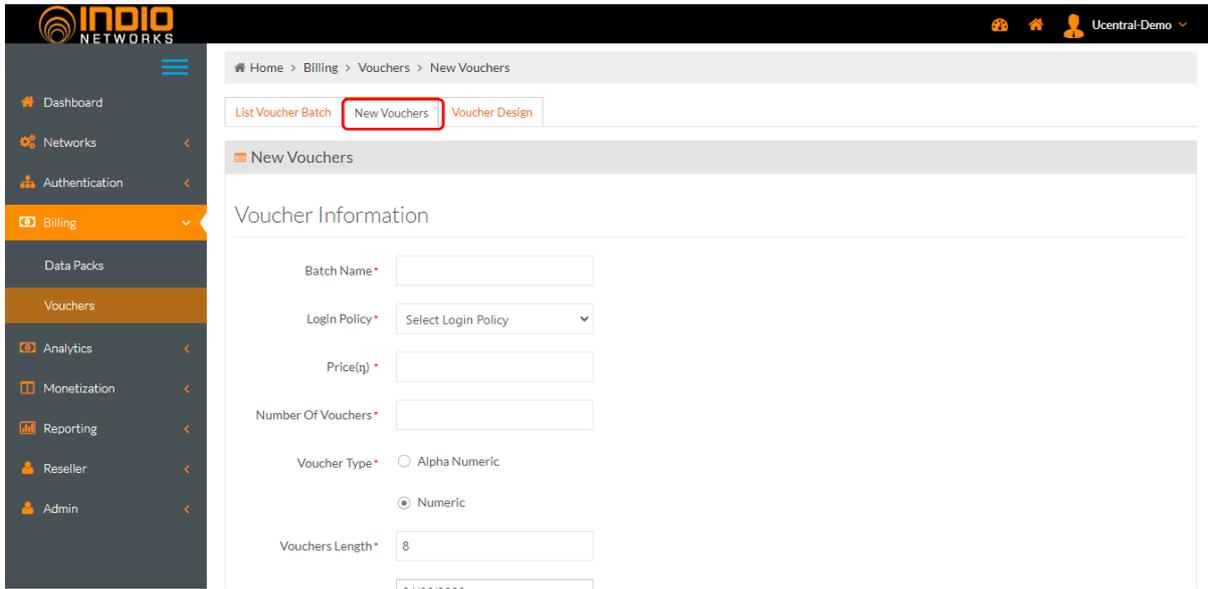
2



Search



Reload



With over two decades of experience, we have worked closely in the wireless space essentially serving over 25+ million users till date. At Indio, we have seen disruptions in the tech sphere and worked alongside them. We solve problems where we see them, we evolve, innovate and adapt. That's why, we constantly craft newer products and solutions to make your life easier. 'Simplifying connectivity' is a principle we hold dear, and we plan on bringing it to everyone, everywhere. With a strong presence in over three important geographies, being Asia, the Middle East and America, we are always available for quick and responsive customer support.

For more information visit- www.indionetworks.com

Indio Networks India, Head Office C-410, Teerth Technospace Baner, Pune -411045, India

#1, Navarathana Gardens, 1st Floor, Sy. No. 68, Kanakapura Main Road, Bengaluru, 560062

Q4-172 SAIF Zone, Sharjah, UAE

815-A Brazos St, Suite 326 Austin, Texas - 78701 U.S.A.

5th Floor Centage Plaza, 14 Allen Ave. Ikeja, Nigeria



sales@indionetworks.com



+91 (20) 6715 7377
+1 888-280-4112



www.indionetworks.com