

Pronto Cloud Controller



User Guide



1. List of Acronym and Abbreviation

The Pronto Cloud Controller is a next generation cloud Wi-Fi network configuration, management and monitoring solution that delivers enterprise class functionality while eliminating upfront costs for on-site setup and maintenance.

The Graphical User Interface is built on the latest technologies with a simple, intuitive, fast and responsive web design. The PCC Software-As-A-Service solution leverages cloud architecture to run multiple instances in the cloud with load balancers that ensures reliability and redundancy.

Acronym	Definition
PCC	Pronto Cloud Controller
API	Application Program Interface
AP	Access Point
SSID	Service Set Identifier
PIAP	Pronto Intelligent Access Point
HB	Heart Beat

2. Product Highlights

An administrator can configure and monitor multiple networks using Pronto Cloud Controller.

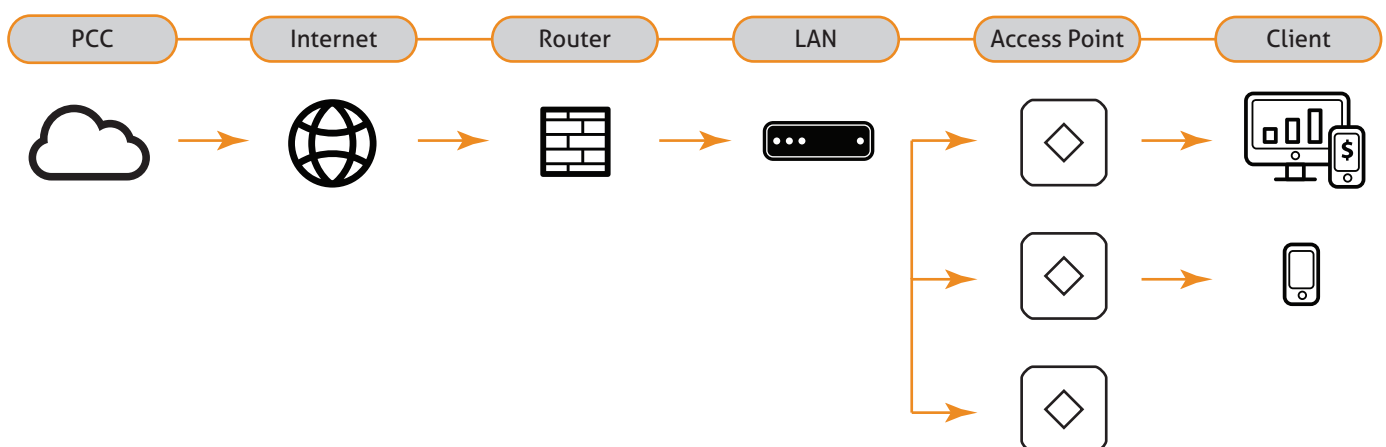
- » Centralized management
 - » Configuration and monitoring of geographically distributed multiple networks.
 - » Secure access to Dashboard via browser.
- » Zero touch Configuration, Provisioning, Bulk Configuration and Upgrade
- » Monitoring
 - » Usage statistics, Connected clients and Device statistics.
 - » Notification, Alerts, Remote troubleshooting and Diagnostics.
 - » Real-time location analytics and Historical monitoring data.
- » Network Performance Management and Optimization
 - » Simplify infrastructure and software management.
 - » Offer continuous and proactive quality assurance and network maintenance.

3. Pronto Cloud Architecture

Traditional access points needed to be configured manually with expertise to use command line interface. Later, the evolution of APs with web based GUI support made the configuration easy. Bulk provisioning of these APs was the biggest operational hurdle faced by the network administrators. Maintenance, monitoring and upgrade also became a nightmare for them. These challenges forced vendors to develop a centralized solution to configure, manage and monitor the access points. This led to the introduction of WLAN controller and thin APs.

WLAN controller is a centralized management unit for configuration of Access Points. Controllers are very expensive hardware. The entire network stops functioning if the controller goes down. This requires a redundant hardware which is an additional cost.

Pronto Cloud Controller has an answer for all these issues. Cloud controller is a single centralized web based solution for managing multi-site networks from a remote location. It has visibility of all network sites, and the same is displayed through Google map support.



4. PCC Account

The initial account on Sign Up is an Admin, who can later create Network admin and Guest account.

Sign Up Instruction. - [Fig 4.1]

- » Launch the browser and type <https://cloud.prontonetworks.com>
- » Click 'Sign Up'.
- » Fill all the mandatory fields: Name, Email, Password, Phone number and Company Name.
- » Click 'Sign Up'.

Congratulation, You have setup your first account.

Didn't receive password instructions? - [Fig 4.2]

- » Launch the browser and type <https://cloud.prontonetworks.com>
- » Click 'Didn't receive password instructions?'.
- » Enter the Email address.
- » Click 'Resend'.

Sign In Instruction.

- » Launch the browser and type <https://cloud.prontonetworks.com>
- » Enter the Email and Password for your PCC account. Click 'Sign in'.

Forgot Password? - [Fig 4.3]

- » Launch the browser and type <https://cloud.prontonetworks.com>
- » Click 'Forgot Password?'.
- » Enter the Email address.
- » Click 'Resend Password'.

Change your account password. - [Fig 4.4 and Fig 4.5]

- » Sign in as Admin
- » Click 'Settings' at the top right hand corner of the screen.
- » Select 'Change Password'.
- » Current password: Enter the existing password.
- » New password: Enter the new password.
- » Confirm password: Confirm the new password.
- » Click 'Change my password' to reset the password.

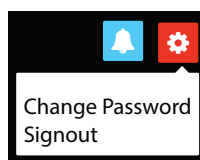


Fig 4.4

Fig 4.5

* To Create a User : - [Fig 4.6]

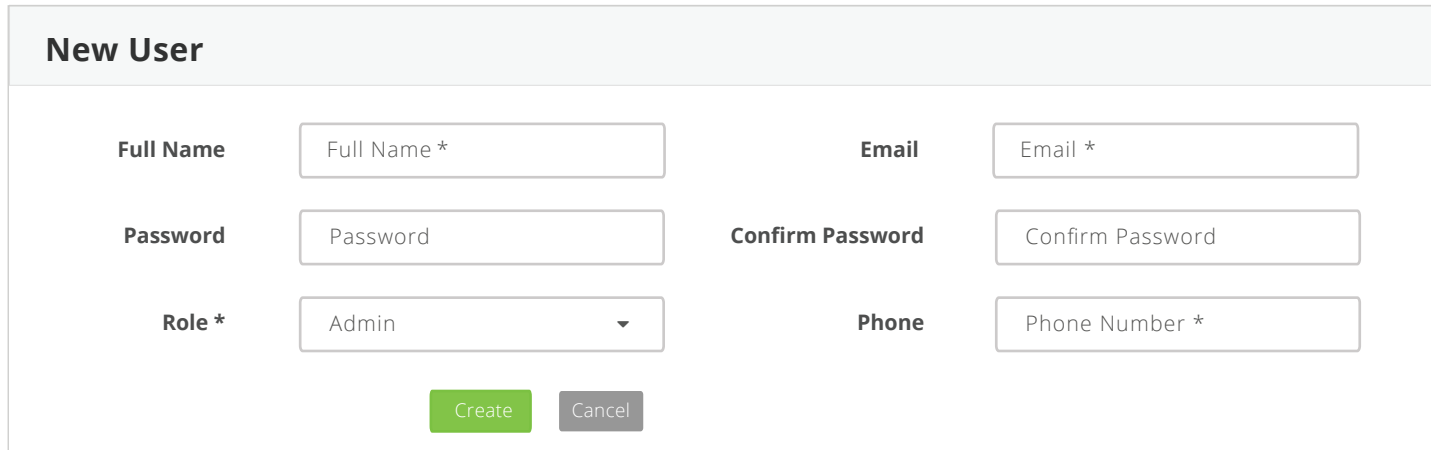
- » Navigate to Organisation → Users on the left pane.
- » Select 'Create Network' from the 'Select Network' drop down list on the right pane.
- » **Full Name** : Name of the User.

Fig 4.1

Fig 4.2

Fig 4.3

- » **Email** : A valid Email address used for PCC Sign In.
- » **Password** : Password for PCC Sign In.
- » **Confirm Password** : Confirm the Sign In password.
- » **Role** : Select Admin, Network admin or Guest based on type of access.
- » **Phone** : Phone number of the user.
- » Click 'Create'.



The 'New User' form is a light gray rectangular box with a title bar at the top. Inside, there are six input fields arranged in two columns. The left column contains 'Full Name' (text input), 'Password' (text input), and 'Role *' (dropdown menu with 'Admin' selected). The right column contains 'Email' (text input), 'Confirm Password' (text input), and 'Phone' (text input). At the bottom center, there are two buttons: a green 'Create' button and a gray 'Cancel' button.

Fig 4.6

Create an account based on different Role.

Apart from Network admin and Guest accounts, PCC enables an Admin to create multiple Admin accounts.

- » Admin account: An administrator account has total control of the PCC accounts, permissions and access rights.
- » Network admin: The user will have a complete access or Read only access to the type of network allowed by the Admin.
- » Guest: The user will have Read only access to the network allowed by the Admin.

5. Create a Network

Network :

Access points in PCC are configured under networks. Each geographical location can have single or multiple networks configured in PCC. Similarly, a network can be associated with a single or multiple geographical locations.

* To Create a Network : - [Fig 5.3]

- » Navigate to Monitor → Dashboard on the left pane. - [Fig 5.1]
- » Select 'Create Network' from the 'Select Network' drop down list on the right pane. - [Fig 5.2]

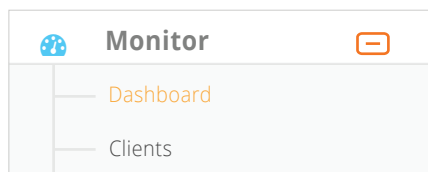


Fig 5.1

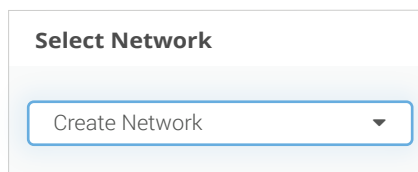


Fig 5.2

Create Network

Network Name

Network Name

Configuration

☒ Default Configuration
 ☐ Clone Configuration

Network Name you have Created will appear

Network TimeZone

(GMT-10:00) New Delhi

Device(s)

Press Enter or Tab for adding Devices

Add one or multiple devices to claim and assign to this network.

Create Network

Cancel

Fig 5.3

- » **Name** : Name of the network.
- » **Configuration** : Helps to configure the APs.
 - » **Default Configuration** : Select this option to setup the APs with a fresh configuration.
 - » **Clone Configuration** : Select this option to copy the configuration of an existing network to a new network.
- » **Network Timezone** : Select the Timezone for the network.
- » **Device(s)** : Enter the Mac Address of the AP. Press Enter or Tab to add multiple APs.
- » Click 'Create Network'.

6. Add Inventory

Inventory :

Pronto Cloud Controller supports complete Pronto PIAP and Mobile Router inventory management. You can explicitly configure access points with enough information to identify them uniquely.

- » Adding and removing the Access Points and Mobile Routers.
- » Managing and Monitoring multiple devices configured across different networks in a PCC account.
- » Moving devices between the network.
- » Adding and Removing Access Points to a Tag.

* To Add Inventory : - [Fig 6.1]

To Add the APs to the network, navigate to Configuration → Inventory.

- » **Device(s)** : Enter the Mac Address of the AP. Press Enter or Tab on the keyboard to add multiple AP's.
- » **Network** : Select the Network under which the APs are to be configured.
- » Click 'Add Many Devices', to add Access Points in bulk.
- » **Upload File** : Sample CSV file in the PCC can be used to add the devices in bulk. Click Browse, Upload the CSV file.
- » Click 'Add Devices'.for the AP.

Add Inventory

Device(s)

Press Enter or Tab for adding Devices

Add one or multiple devices to claim.

Network

Select Network

Add Many Devices.

Add Devices

Cancel

Fig 6.1

7. Edit or Monitor Network

* To Edit or Delete a Network :

- » To either Edit or Delete a Network, navigate again to Monitor → Dashboard on the left pane.
- » Select 'Edit/Delete Network' from the 'Select Network' drop down list on the right pane.

Edit : You can modify the Network Name and Network Timezone.

Delete : Delete the network from the account. This will only delete the network, the AP associated with the network will still be listed in the Inventory.

* To Monitor a Network :

- » Navigate to Monitor → Dashboard on the left pane.
- » Select the network you want to monitor from the 'Select Network' drop down list.

On the right side the Total Access Points and Total Clients on that network are shown. - [Fig 7.1]

- » **Total Access Points :** Displays the total number of Access Points and their status.
- » **Green :** Green indicates the number of APs online.
- » **Red :** Red indicates number of APs offline.
- » **Total Clients :** Displays the number of clients connected to the network.
- » **Total Alerts :** Displays the total number of alerts for a network.



Fig 7.1

Next is a tabbed section which shows the Throughput, Client Graph and Connected Clients details. - [Fig 7.2]

- » **Throughput :** Graphical representation of Real-time and Historical traffic of the network during a specific time period.
- » **Client Graph :** Graphical representation Real-time and Historical data of Downstream and Upstream for all the clients connected to the network.
- » **Connected clients :** Graphical representation of Real-time and Historical network data for the total number of clients and APs, corresponding to a network.

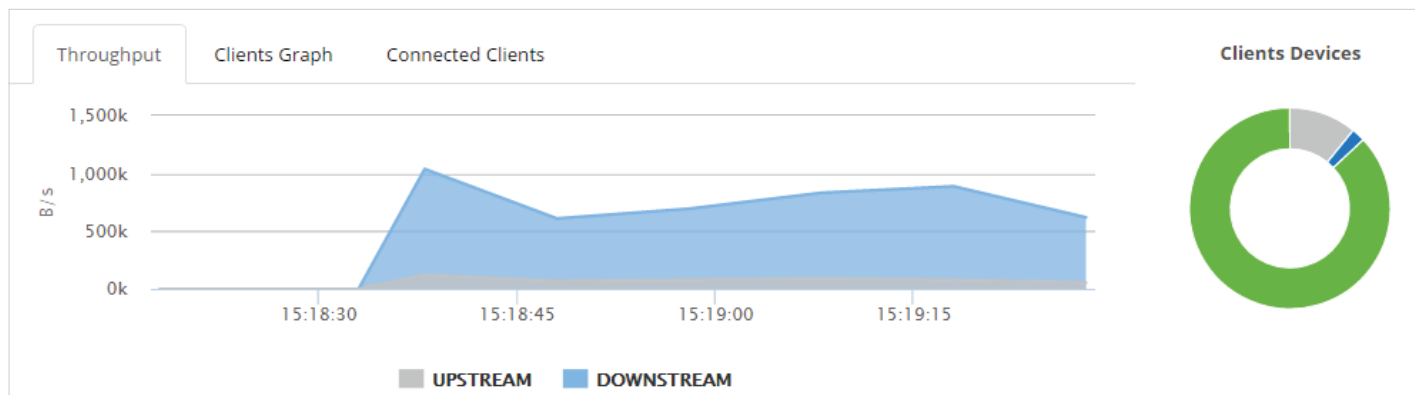


Fig 7.2

- » **Period** : You can filter the statistics for different date and time period.
- » **Client Devices** : Display the type of user devices (Android, IOS, Windows, etc). Each device type is displayed with different color schemes.
- » **Network SSIDs** : Displays all the SSIDs configured on the network. - [Fig 7.3]
 - » **Name** : Displays the name of wireless network.
 - » **Security** : Displays the type of security used.
 - » **Clients** : Displays total number of clients on each wireless network.
- » **Top 5 Access Points by Usage** : Top 5 access points in the network based on the traffic. The section also displays the name of APs. - [Fig 7.3]
- » **Top 5 Clients by Usage** : Top 5 clients based on their usage. This section displays Mac Address of each user. - [Fig 7.3]
- » **Map** : This section conveys complete AP status and Client statistics on the map. - [Fig 7.3]
 - » **Access Points** : In the section, each AP on the network, along with their Name and Mac Address are displayed on a map. Green indicates that the APs are online while the Red indicates that they are offline.
 - » **Clients** : The map shows the number of connected clients on each AP. You can also view the Name and Mac Address of the AP.

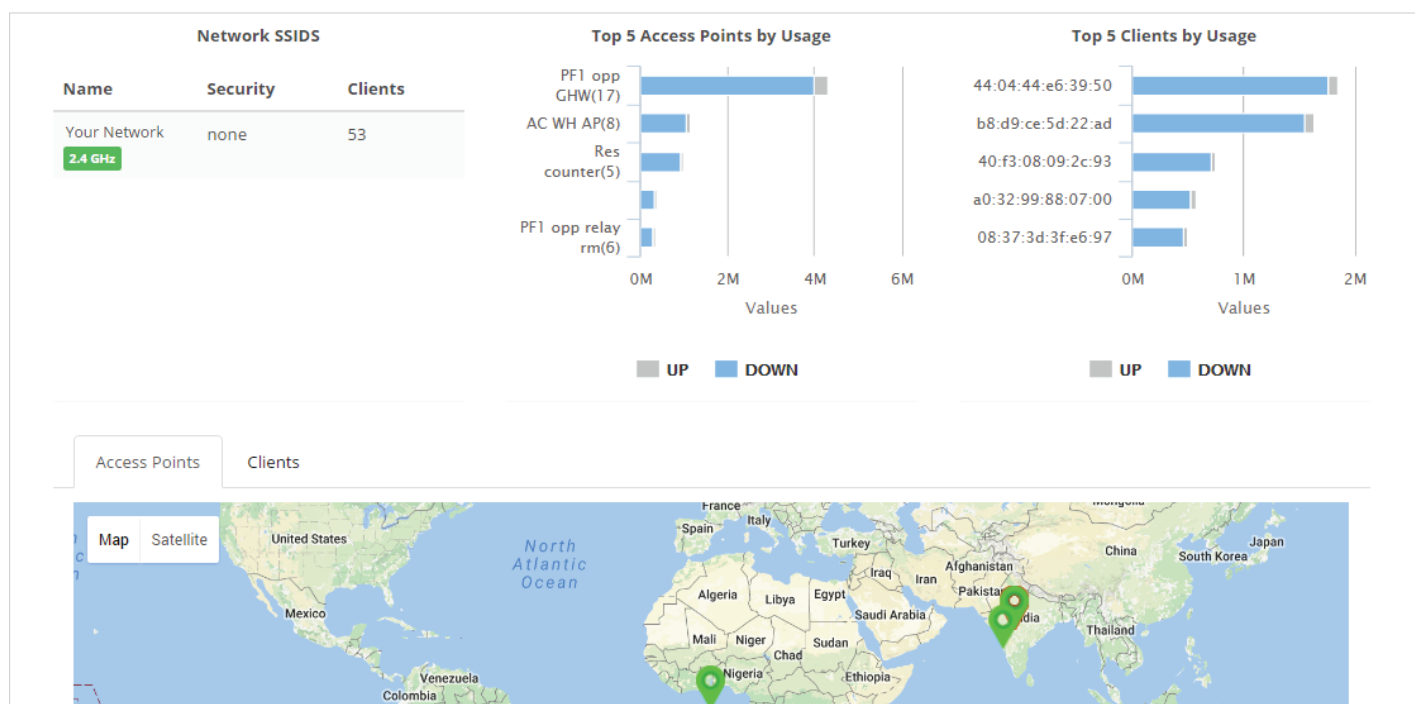


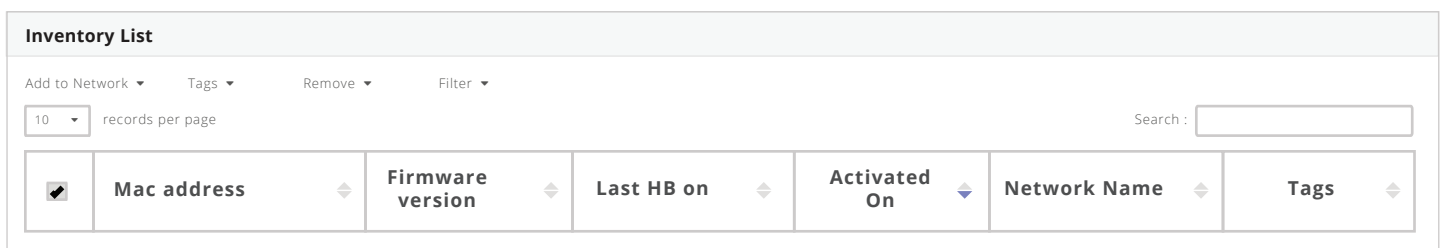
Fig 7.3

8. Edit Inventory

Inventory List :

The Inventory list has 7 sections which gives an overview of each Access Point in the PCC account. - [Fig 8.1]

- » **Check Box** : Check Box can be used to select individual AP or multiple devices using the check box in the first row of the Inventory List section.
- » **MAC Address** : Display the MAC address of the PIAP. A name can be added to identify the Access Point location. The name can be added by clicking the MAC Address. On the Access Point page, Click Edit Configuration, enter the Access Point name under Name section.
- » **Firmware Version** : Displays the Firmware Version of each Access Point.
- » **Last HB on** : Displays the date and time when the Access Point was last seen online.
- » **Activated On** : This shows the date on which the Access Point was configured on the PCC.
- » **Network Name** : The Network which the Access Points belong to.
- » **Tags** : The Tag to which Access Points are associated.



The screenshot shows the 'Inventory List' interface. At the top, there are several dropdown menus: 'Add to Network', 'Tags', 'Remove', and 'Filter'. Below these is a 'records per page' dropdown set to '10' and a search bar labeled 'Search :'. The main part of the interface is a table with the following columns: 'Mac address' (with a checkmark icon), 'Firmware version', 'Last HB on', 'Activated On', 'Network Name', and 'Tags'. Each column header has a small double-headed arrow icon next to it, indicating it can be sorted.

Fig 8.1

* To Edit Inventory List :

There are 3 sections under Inventory List for Adding and Removing APs to and from the Network, Tags and Inventory.

- » **Add to Network** : We can add an individual or multiple APs to an Existing Network or a new Network. - [Fig 8.2]
 - » Select an individual or multiple APs using the check box. Go to 'Add to Network'.
 - » **Existing** : Select this option to add the AP to existing network.
 - » **Create Network** : Select this option to create a new Network. Enter the name of the Network. Select Default Configuration from the drop down list to setup the APs with fresh configuration. Select one of the network names from the drop down list to copy the configuration of an existing network to a new network.
 - » Click 'Add to Network'.
- » **Tags** : We can add or remove an individual or multiple APs to and from the Tag. - [Fig 8.3]
 - » Select an individual or multiple APs using the check box. Go to Tags.
 - » **Add** : Enter the name of the Tag to which the AP needs to be added. Click 'Add'.
 - » **Remove** : Enter the name of the Tag from which the AP has to be disassociated. Click 'Remove'.
- » **Remove** : This allows removing the AP from the Network or Inventory. Removing the AP from the network will not delete it from the Inventory. - [Fig 8.4]
 - » Select an individual or multiple APs using the check box. Go to 'Remove'.
 - » **Network** : Select this option to remove the AP from the network.
 - » **Inventory** : Select this option to remove the AP from the Inventory.
 - » Click 'Remove'.
- » **Filter** : This will give the status of all APs in the PCC account. - [Fig 8.5]
 - » **All** : This will give the up/down information of all APs.

Add to Network ▼

Tags ▼

Remove ▼

Filter ▼

☒ Existing

RailWire SBC ▼

☐ Create New

Add to Network

Add:

Remove:

Add

Remove

☒ From Network
☐ From Inventory

Show:
All | Up | Down

Remove

Fig 8.2

Fig 8.3

Fig 8.4

Fig 8.5

- » **Up** : Status of APs currently online.
- » **Down** : Status of all Offline APs.
- » **Search** : Enter the MAC address of an AP, and get the status and information.

9. Access Point Monitoring

Access Point :

Access Point has two sections, one for monitoring, and other for configuration and management.

Monitoring :

* Multiple Access Point Overview :

To get the overview of all Access Points, navigate to Monitor → Access Points. This section shows the Firmware Version, Last HB date, Activate date, Channels, and Connected client on each channel - [Fig 9.1].

- » **MAC Address** : Displays the MAC address of the PIAP.
- » **Firmware Version** : Shows the Firmware Version of each Access Point.
- » **Last HB on** : Displays the date and time when the Access Point was last seen online.
- » **Activated On** : This shows the date on which the Access Point was configured on the PCC.
- » **Channel** : Provides the channel for each AP on 2.4GHz and 5GHz radio band.
- » **Connected Clients** : Displays the clients connected on 2.4GHz and 5GHz radio bands.
- » **Tags** : We can add or remove an individual or multiple APs to and from the Tag.
- » **Filter** : Refer to 'Filter' section on page ___for information.

Inventory List									
Filter ▼		Show: All Up Down		Search :					
Mac address	Firmware version	Last HB on	Activated On	Channel		Connected Clients		Tags	
				2.4 GHz	5 GHz	2.4 GHz	5 GHz		

Fig 9.1

* Individual Access Point Monitoring :

To view the configuration of individual Access Point, navigate to Configuration → Inventory, Click on the AP MAC Address Or go to Monitor → Access Points, Click the on the AP MAC Address.

- » **Access Point** : Shows the MAC address of the AP and the time when it was seen online.

- » **Configuration** : Edit the Configuration of the Access Point. Details are provided in the Access Point Configuration section.
 - » **MAC Address** : MAC Address of the Access Point.
 - » **Address** : Location where the access point is deployed.
 - » **Tags** : Name of the tag to which the Access Point is associated. This section will be displayed when a Tag is assigned to an AP.
 - » **Channel** : Displays the Channel on which the signal is transmitted. This can be set to Auto or a channel can be configured manually. Refer to 'Radio Profile' section for setting up the channel.
 - » **Power** : Transmission power set for the AP.
 - » **Enable L2oGRE** : Shows the status of L2oGRE.
 - » **Enable DHCP** : Displays the status of DHCP Relay on LAN.
 - » **Uplink IP** : Shows the internet Backhaul IP. This can be either a Private or a Public IP.
 - » **Latitude** : Drag the mark on the Map to set the Latitude of a specific location.
 - » **Longitude** : Drag the mark on the Map to set the Longitude of a specific location.
 - » **SSID** : Displays total number of SSIDs enabled and disabled on the AP.
 - » **Uplink** : Shows the number of Uplinks configured for AP.
 - » **Wired** : Displays the Wired WAN connection information.
 - » **IP Type** : Shows the Internet Connection Type: DHCP or Static.
 - » **IP** : Shows the Uplink IP.
 - » **Mobile Broadband** : Displays the Mobile Router connection information.
 - » **Service** : The value will always be '1'.
 - » **APN** : Each service provider will have different APN. A few APNs for few service providers are listed below:
 - » **Airtel** : airtelgprs.com.
 - » **Vodafone** : www.
 - » **Reliance** : jionet.
- » **Status** : - [Fig 9.2].
 - » **Public IP** : Displays the Pubic IP of the AP.
 - » **CPU Idle Time** : CPU idle time without any processing.
 - » **Uptime** : Uptime of the AP.
- » **System Information** : - [Fig 9.2].
 - » **Public IP** : Shows the Firmware Version of the AP.
 - » **Kernel Version** : Kernel Version of the AP.
 - » **HW Part no** : Shows the Hardware Part number of the AP.

Status	System Information	Memory Information
Public IP : 112.133.248.101	Firmware Version : 2.0.2.18	Total : 61996kB
CPU Idle Time : 2hr 38m 10s	Kernel Version : 3.10.49	Free : 26004kB
Uptime : 3hr 15m	HW Part no : PIAP-11N-S-48C	Buffers : 3388kB
		Cached : 12696kB

Fig 9.2

- » **Memory Information in KB** : - [Fig 9.2].
 - » **Total** : Shows the Total Memory Information.
 - » **Free** : Displays the free memory space.
 - » **Buffers** : Displays the space utilized in the Buffer.
 - » **Cached** : Shows the cached memory.
 - » **Throughput** : Graphical and Quantitative data of Real-time and Historical traffic of the AP during the selected time period. - [Fig 9.3].
- » **Quantitative Data** : - [Fig 9.3].
 - » **Upload in KB/s** : Total Uploaded data.
 - » **Download in KB/s** : Total Downloaded data.
 - » **Total in KB/s** : Total Downloaded and Uploaded data.
 - » **Graphical Representation** : Graphical representation of Real-time and Historical, Downstream and Upstream data usage on the AP. The data is showed for both Wired and 4G/3G interfaces.
- » **Connected Clients** : - [Fig 9.3].
 - » **Total Clients** : Total number of clients connected in real-time to the Wireless interface of the AP.
 - » **Client** : MAC Id of each client connected to the AP.
 - » **Host Name** : Hostname of the user device.
 - » **Device Type** : Type of user devices (Android, IOS, etc).
 - » **SSID** : SSID to which user is connected.
 - » **Signal** : Signal level seen by each user device.
 - » **Usage (Up/Down)** : Real-time Upload and Download data usage for each user.

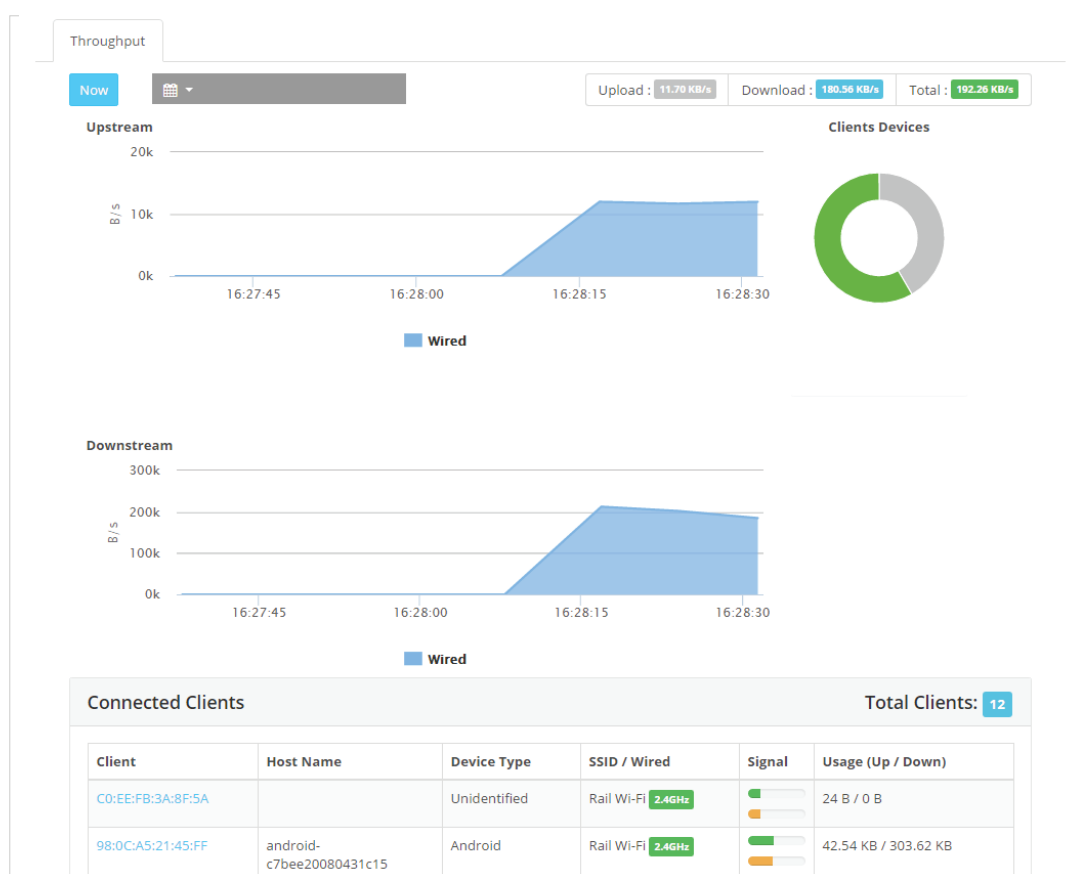


Fig 9.3

10. Access Point Configuration

Access Point Configuration :

* To Configure Access Points :

Access Point configuration screen can be accessed by going to either Inventory or Access Point section.

- » To access from the Inventory, go to Configuration → Inventory and click on the AP MAC Address.
- » To access from Access Points section, go to Monitor → Access Points and click the on the AP MAC Address. - [Fig 10.1].
- » Click 'Edit Configuration'.
 - » **Name** : Name of the Access Point
 - » **Channel** : The Channel selection for the PIAP and Routers are limited only for a few hardwares. For other devices, the Channel can be set from the Radio Profile section.
 - » **L2oGRE on LAN** : Pronto PIAP supports a variety of encapsulation methods between the AP and the remote gateway. The solution enables the AP to bridge the LAN traffic from the end host and terminate on a remote gateway.
 - » Enable the feature and specify the IP address of the remote gateway.
 - » **DHCP Relay on LAN** : Enable this option to use a DHCP server on the network for serving the IP address.
 - » **Power** : The Power selection for the PIAP and Routers are limited only for a few hardwares. For other devices, the Channel can be set from the Radio Profile section.
 - » **Uplink Configuration** : The Uplink Configuration is enabled only for Mobile Broadband Router or devices that can configure with more than one Uplink Type. For all other PIAPs, the Uplink Type will be wired by default, and Add Uplink will not be enabled.
 - » **Uplink Type** : There are two Uplinks allowed, Wired and Mobile Broadband. The Mobile Broadband is only used for Routers that uses a 4G SIM as a backhaul.
 - » **IP Type** : Displays the internet connection type : DHCP or Static.
 - » **Primary** : Use the check box to select the Primary Uplink. The device will try to come online with the selected Uplink Type. Upon failure, AP will try to initialize with the Secondary Uplink.
 - » **Actions** : The section allows one to add Uplink and Connection type.
 - » Click the Add Uplink to configure the type of Uplink.
 - » **Uplink Name** : Name of the Uplink.
 - » **Uplink Type** : Wired or Mobile Broadband.
 - » **Wired** : Enter the Uplink Name, select the Uplink Type as Wired and choose the IP Type as DHCP or Static as needed. Click Save.
 - » **Mobile Broadband** : To configure Mobile Broadband, enter the Uplink Name, select the Uplink Type as Mobile Broadband, choose the service as UMTS and enter the service provider APN. Click Save. Refer 'Mobile Broadband' section on page ___ for APN list.
 - » Click Save on the Access Point configuration screen.
- » **Enable LB** : Select "Yes" or "No" to enable Load balancer for the Router.
- » **Notes** : Under this section one can update important information about the Location, Network or AP. This will allow anyone having access to the AP configuration screen to know about the AP without the help of Admin.
- » **Address** : The location Address, Latitude and Longitude can be set manually or automatically by dragging the marker on the map.
- » Please refer to 'Individual Access Point Monitoring' section on Page __ for information about Status, System Information, Memory Information, Throughput and Connected Clients.

Access Point
00:0C:66:10:3A:18
(Last Seen: 29/09/2016 16:02:45 +05:30)
Reboot

Configuration
Edit configuration

Name
PF1-Pno33

Channel
11

L2oGRE on LAN
☐ Enable

DHCP Relay on LAN
☐ Enable

IP Address

IP Address

Power(dbm)
20

Uplink Type	IP Type	Primary	Actions
Wired	dhcp	<input checked="" type="checkbox"/>	

Notes
Notes

Tags
PF1

Note:Below details can be set automatically by dragging marker on map.

Address Line1
Bangalore City

Address Line2
Address2

City
City

Country
India

State / Province
-- Select state --

Zipcode
Zipcode

Latitude
20

Longitude
77

Save

Cancel

Note: By dragging marker you can set new location for your device.

Map
Satellite

Fig 10.1

11. Configuring and Editing SSID

SSID is the name of a wireless network that a client “discovers” when it probes for available wireless networks in the surrounding. PCC allows multiple SSIDs on a network.

* To configure an SSID for the network :

» Select the Network and navigate to Configuration → Network → Add SSID. - [Fig 11.1] and [Fig 11.2].

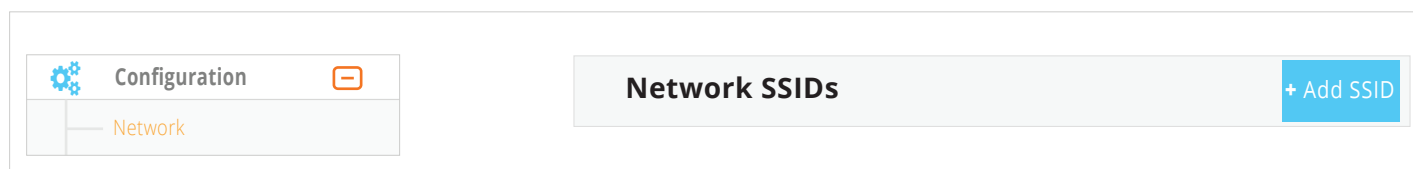


Fig 11.1

- » **APs/AP Tags** : APs/AP Tags : We can specify Network name, AP Mac Address or Tag name.
- » **Network name** : The SSID configuration will be applied to all APs in the network.
- » **Mac Address** : The configuration will be applied to individual APs.
- » **Tag name** : The configuration will be applied to a group of APs associated with Tag.

Note : Tag is a label used to organize APs, and separate them from one another based on different profiles. Each AP can have multiple Tags. Refer to "Inventory and Access Point" on page 13 for steps to create Tags.

- » **SSID Name** : Enter the wireless name (SSID).
- » **SSID Status** : SSID is enabled by default. All wireless devices within a range are able to see the SSID when they scan for available networks. Select Disable to stop broadcasting.
- » **SSID Hidden** : The option is disabled by default. Enabling this option will prevent the Access Points from broadcasting the SSID. Choosing not to broadcast the SSID of a wireless network does not make it undetectable.
- » **SSID Isolate** : The option is disabled by default. It prevents devices connected to different SSIDs from seeing each other.
- » **SSID Radio Band** : This will allow an SSID to broadcast on either 2.4GHz or 5GHz band. To broadcast both 2.4GHz and 5GHz with same wireless name (SSID), one has to create two SSIDs: one for 2.4GHz and another one for 5GHz radio band.
- » **Apply SSID QoS** : The option is disabled by default. Enable Quality of Service (QoS) to prioritize the traffic and ensure adequate bandwidth on the SSID.
 - » **SSID QoS in kbps** : Select the Custom check box to set the QoS manually.

Create SSID

APs / AP Tags	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">x Network Name</div>	
SSID Name	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">New SSID</div>	
SSID Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
SSID Hidden	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID Isolate	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID Radio Band	<input type="radio"/> 5 Ghz	<input checked="" type="radio"/> 2.4 Ghz
Apply SSID QoS	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID QoS	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;">0 Kbps</div> <div style="flex-grow: 1; border: 1px solid #ccc; position: relative;"> <div style="background-color: #007bff; width: 10%; height: 10px; position: absolute; bottom: 0; left: 0;"></div> </div> <div style="margin-left: 10px;"> <input checked="" type="checkbox"/> Custom <div style="border: 1px solid #ccc; padding: 2px; margin-left: 5px; width: 50px; text-align: center;">0</div> Kbps </div> </div>	

Fig 11.2

- » **Policies** : MAC address filtering allows you to define a list of devices and only allow those devices on your Wi-Fi network. Enable Policies to allow or deny access to the SSID by the MAC Address of the requesting devices. -[Fig 11.3]

» **MAC ACL Policy :**

- » **Allow :** Select the option and add the MAC Addresses under Allowed MAC Address to permit access to the listed devices. The devices not added to the list will be denied access to the network.
- » **Deny :** Select the option and add the MAC Addresses under Denied MAC Address List to block access to the listed devices. Remaining all devices will be allowed access to the Wi-Fi network.

- » **SSID WDS :** WDS allows you to connect multiple access points. With WDS, APs simplify the network infrastructure by reducing the amount of cable required. Select the option to Enable or Disable the WDS link.

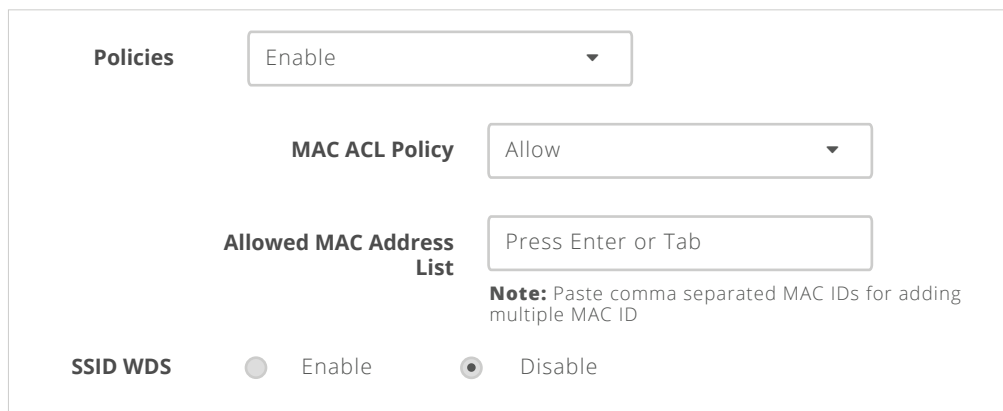


Fig 11.3

- » **Mode :** APs can be configured in either Bridge or Router mode as needed by the network.

- » **Bridge mode :** In this mode, NAT is disabled, and the wireless clients get IP address from the Router or External DHCP server.
 - » **VLAN :** To use the VLAN, select the VLAN profile from the drop down list. Refer to “VLAN” section on page 19 for steps to create VLAN profile.
In Bridge mode configure a VLAN tag to the SSID. Wireless traffic (Data) on the SSID will be tagged between the AP and the wired infrastructure.
 - » **Association :** An administrator can configure the parameters required for the client to associate successfully with the Wireless network. PCC supports a wide variety of encryption and authentication methods.
 - » **Open/None :** This mode is enabled by default. Any station that knows the SSID can join as the security features are disabled.

- » Click Update SSID.

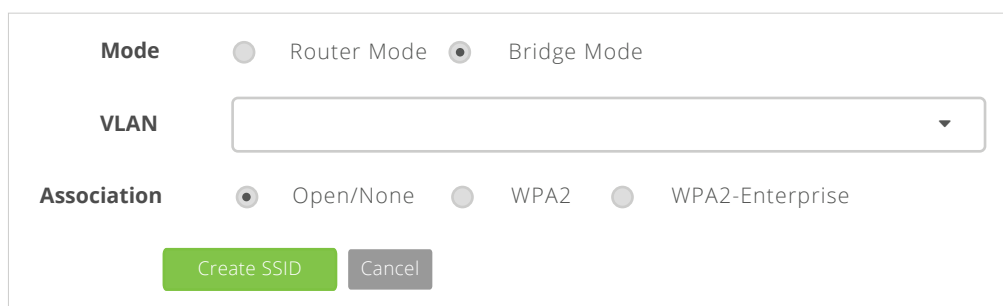


Fig 11.4

- » **WPA2 :** WPA2 requires a Pre-shared key to connect to the wireless network.

- » **Encryption Algorithm** : TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) are two different types of encryption that can be used by a Wi-Fi network. Select the relevant encryption from the drop down menu.
- » **Authentication Key** : Set the Key for Authentication to wireless network.

The screenshot shows a configuration window for creating an SSID. It includes the following elements:

- Mode:** Radio buttons for Router Mode and Bridge Mode (selected).
- VLAN:** A dropdown menu.
- Association:** Radio buttons for Open/None, WPA2 (selected), and WPA2-Enterprise.
- Encryption Algorithm:** A dropdown menu showing TKIP.
- Authentication Key:** A text input field with a 'show' button next to it.
- Buttons:** 'Create SSID' (green) and 'Cancel' (grey) at the bottom.

Fig 11.5

- » **WPA2-Enterprise** : This mode supports 802.1x RADIUS authentication and is appropriate in the cases where a RADIUS server is deployed.
 - » **Radius Authentication Server** : Select the Radius Server authentication Profile against which the users on the wireless network have to authenticate.
 - » **Radius Accounting Server** : This is optional. When enabled, the "Start" and "Stop" accounting messages are sent by AP to the Radius accounting server. Select the appropriate Radius Accounting Profile of the Radius Authentication server.

» Click Update SSID.

This screenshot shows the same configuration window as Fig 11.5, but with additional RADIUS settings visible:

- Mode:** Bridge Mode (selected).
- Association:** WPA2 (selected).
- RADIUS Authentication Server:** A dropdown menu.
- RADIUS Accounting Enabled:** A dropdown menu showing 'Enable'.
- RADIUS Accounting Server:** A dropdown menu.
- Buttons:** 'Create SSID' (green) and 'Cancel' (grey) at the bottom.

Fig 11.6

- » **Router mode** : In this mode, NAT is enabled. The PIAP can serve the IP address to the client or support DHCP relay.

Note : SSID WDS should always be disabled in Router mode.

- » **NAT** : Enable NAT.

» **Association** : Association in Route mode.

» **Open / None or WPA2** : As compared to Bridge mode, AP can be configured with following additional options in Router mode.tagged between the AP and the wired infrastructure.

- » **Captive Portal** : Captive Portal allows administrators to block internet access for users until they complete a defined process. The user is redirected to a landing page which may require authentication, payment or other valid credentials before the user is granted access.
- » **Radius Authentication and Accounting** : Refer to “WPA2-Enterprise” section on page 18 for information on Radius Authentication and Accounting.
- » **Splash URL** : Specify the URL of the web server where the Splash page is hosted.

NAT	<input type="radio"/> Enable <input type="radio"/> Disable
Association	<input checked="" type="radio"/> Open/None <input type="radio"/> WPA2 <input type="radio"/> WPA2-Enterprise
Captive Portal	<input type="text" value="Enable"/>
RADIUS Authentication Server	<input type="text" value="RADIUS Authentication Server Name"/>
RADIUS Accounting Enabled	<input type="text" value="Enable"/>
RADIUS Accounting Server	<input type="text" value="RADIUS Accounting Server Name"/>
Splash URL	<input type="text" value="Splash URL"/>

Fig 11.7

- » **Default Interim Update Time** : ‘Interim Accounting Message’ is an accounting message that is sent in order to periodically update the RADIUS server with information pertaining to a specific session. The ‘Interim Update Time’ value has to be provided in seconds.
- » **Default Idle Timeout** : When these settings are configured, the connection will automatically terminate after a specified period of inactivity. The idle timeout value has to be provided in seconds.
- » **Walled Garden** : Walled Garden Sites (a.k.a. white listed sites) are the sites that do not require any authentication for the end user. In effect, the walled garden directs the user's navigation within particular areas, to allow access to a selection of material or prevent access to other material.

Walled Garden	<input type="text" value="Enable"/>
	Walled Garden Range
	<input type="text" value="Walled Garden Domains"/>
Where should users go after the splash page?	<input type="radio"/> The URL they were trying to fetch <input checked="" type="radio"/> A different URL:
	<input type="text" value="URL"/>

Fig 11.8

- » **Per User QoS** : Per User QoS provides different levels of prioritization and guarantees dedicated bandwidth for each user connected to the wireless network.
- » **Where should users go after the splash page** : Success page; User redirection on successful authentication.
- » **WPA2-Enterprise** : The AP can be configured as a DHCP server or DHCP Relay. Other configurations are similar to Bridge mode. Refer to “WPA2-Enterprise” section on page 8 for information about the configuration.
- » **SSID IP Configuration (Open/None, WPA2, WPA2-Enterprise)** : The IP Configuration is similar for Open/None, WPA2, WPA2-Enterprise methods.
 - » **IP Address** : IP address for the interface.
 - » **Netmask** : Enter the Subnet mask for the network.
 - » **DNS mode** : Select the DNS server.
 - » **Use ISP (Default)** : Primary and Secondary DNS server IP address of the ISP.
 - » **Custom** : By selecting this option, enter the Primary and Secondary IP address of the Domain name.
 - » **Relay Server** : Enable this option to use an External DHCP server on the network.
 - » **DHCP Range Start** : Start IP address of the DHCP range.
 - » **DHCP Range End** : End IP address of the DHCP range.
 - » **Lease Times(s)** : Minimum amount of time that an IP address acquired by DHCP is to be retained before expiring on inactivity.

SSID IP Configuration

IP Address

Netmask

DNS Mode

Use ISP(default)
▼

Relay Server

Disable
▼

DHCP Range Start

DHCP Range End

Lease Time(s)

Create SSID

Cancel

Fig 11.9

* To Edit SSID Configuration :

To Edit an SSID for the network, select the Network, navigate to Configuration → Network, click Edit on the appropriate SSID to modify the configuration. - [Fig 11.10]

Edit SSID

APs / AP Tags	<input type="text" value="x Network Name"/>	
SSID Name	<input type="text" value="New SSID"/>	
SSID Status	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID Hidden	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID Isolate	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
SSID Radio Band	<input type="radio"/> 5 Ghz	<input checked="" type="radio"/> 2.4 Ghz
Apply SSID QoS	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Policies	<input type="text" value="Disable"/>	
SSID WDS	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Mode	<input type="radio"/> Router Mode	<input checked="" type="radio"/> Bridge Mode
VLAN	<input type="text"/>	
Association	<input checked="" type="radio"/> Open/None <input type="radio"/> WPA2 <input type="radio"/> WPA2-Enterprise	
<div><input type="button" value="Update SSID"/> <input type="button" value="Cancel"/></div>		

Fig 11.10

Switch Configuration :

To configure the LAN interface for the network, select the Network, navigate to Configuration → Network → Add Switch Configuration. - [Fig 11.11]

- » **Name** : Enter the name of the Switch Configuration.
- » **APs/AP Networks** : We can specify Network name, AP Mac Address.
- » **Apply Wired QoS** : The option is disabled by default. Enable Quality of Service (QoS) to prioritize the traffic and ensure adequate bandwidth on the LAN.
- » **Wired QoS in kbps** : Select the "Custom" check box to set the QoS manually.

Wired Configuration			+ Add Wired Configuration
Name	Captive Portal	Network / AP / Ap tags	Delete

Fig 11.11

12. Policy and Profile Management

RADIUS CONFIGURATION

The Remote Authentication Dial-In User Service(RADIUS) server configuration is required for WPA2-Enterprise based SSID association or when Captive Portal is enabled for Open/None and WPA2 association. It facilitates the administrators to configure RADIUS Authentication and Accounting servers.

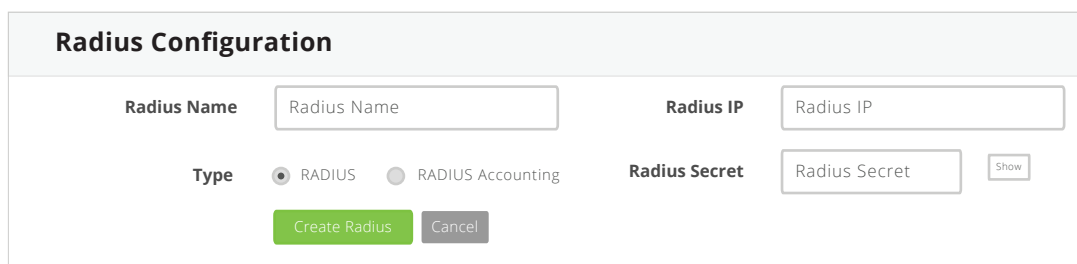
* To Configure Radius Profile :

» Navigate to Organization → Radius Configuration. - [Fig 12.1]

» **Radius Authentication Server :**

- » **RADIUS Name :** The name of the RADIUS Authentication profile.
- » **RADIUS IP :** The IP address of the RADIUS Authentication server.
- » **RADIUS Port :** Enter the port number.
- » **RADIUS Secret :** Enter secret passkey required to access the RADIUS server.
- » **Type :** Select the type as RADIUS.
- » Click 'CREATE RADIUS'.

» **Radius Accounting Server :** Refer 'Radius Authentication Server' section for configuration information. Select the type as 'RADIUS Accounting' and click CREATE RADIUS.



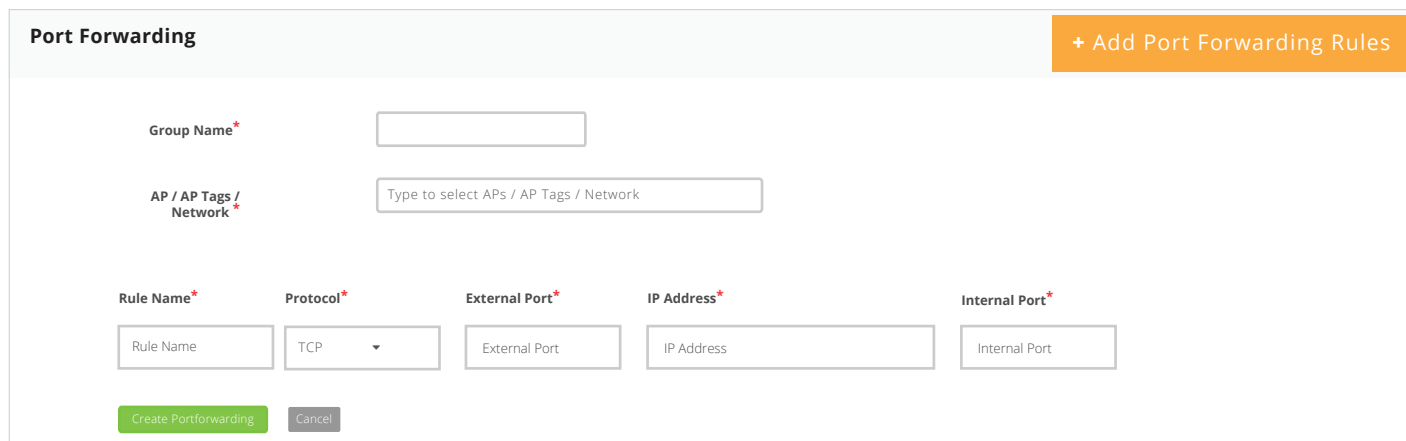
The 'Radius Configuration' form contains the following fields and controls:

- Radius Name:** A text input field with the placeholder 'Radius Name'.
- Radius IP:** A text input field with the placeholder 'Radius IP'.
- Type:** Two radio buttons: 'RADIUS' (selected) and 'RADIUS Accounting'.
- Radius Secret:** A text input field with the placeholder 'Radius Secret' and a 'Show' button to toggle visibility.
- Buttons:** 'Create Radius' (green) and 'Cancel' (grey).

Fig 12.1

» **Port Forwarding :** This allows remote services on the Internet to connect to a specific device within a private LAN. - [Fig 12.2]

- » To configure Port Forwarding, navigate to Organization → Port Forwarding.
- » **Group Name :** Define a name for the rule.

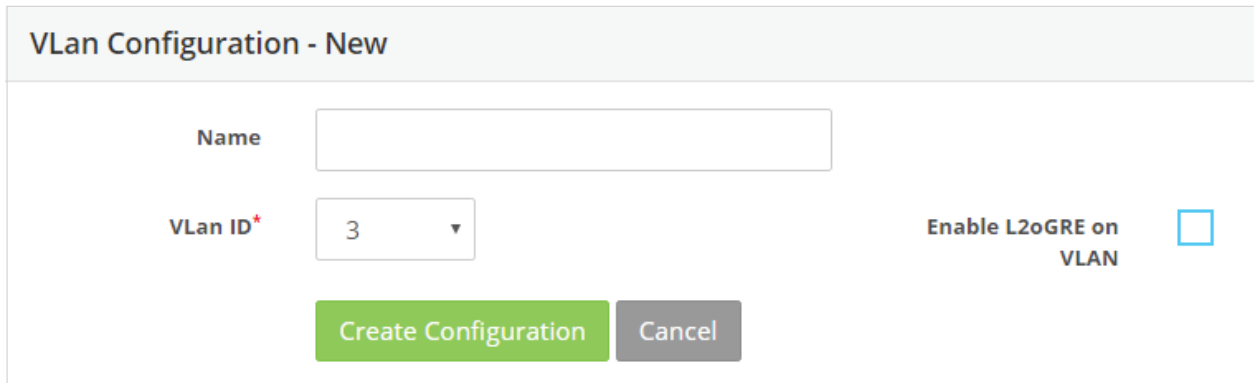


The 'Port Forwarding' form contains the following fields and controls:

- Group Name*:** A text input field.
- AP / AP Tags / Network*:** A text input field with the placeholder 'Type to select APs / AP Tags / Network'.
- Rule Name*:** A text input field with the placeholder 'Rule Name'.
- Protocol*:** A dropdown menu currently showing 'TCP'.
- External Port*:** A text input field with the placeholder 'External Port'.
- IP Address*:** A text input field with the placeholder 'IP Address'.
- Internal Port*:** A text input field with the placeholder 'Internal Port'.
- Buttons:** 'Create Portforwarding' (green) and 'Cancel' (grey).
- Header:** 'Port Forwarding' title and '+ Add Port Forwarding Rules' button.

Fig 12.2

- » **AP / AP Tags / Network** : Select the AP or AP Tags or Network on which the Port Forwarding rules need to be implemented.
 - » **Rule Name** : Name of the rule.
 - » **Protocol** : Select either TCP or UDP.
 - » **External Port** : Indicates the port number of the PIAP that receives information from the external network and forwards it to the devices on the internal network.
 - » **IP Address** : IP address of the device in the internal network.
 - » **Internal Port** : Indicates the port number of the actual device on the internal network.
 - » Click 'Create Port forwarding'.
- » **VLANs**
- » To configure VLAN, navigate to Organization → VLANs. - [Fig 12.3]
 - » **Name** : Provide the name for the VLAN.
 - » **VLAN ID** : Select VLAN identifier, which should be a unique number, ranging between 3 and 4096.
 - » **Enable L2oGRE on VLAN** : Enable this feature to tunnel LAN traffic to a remote endpoint, over GRE protocol. By default, it is disabled.
 - » Click 'Create Configuration' button. The VLAN configuration can be associated with a particular SSID on the SSID Configuration screen.



Vlan Configuration - New

Name

Vlan ID*

Enable L2oGRE on VLAN ☐

Create Configuration **Cancel**

Fig 12.3

» ACL Groups

This feature helps as a filter to allow/deny access to connected devices located on LAN or WLAN network from the WAN network.

- » To create ACL group, navigate to Organization → ACL Groups → + Create New ACL. - [Fig 12.4]
- » **Group Name** : Define a group name for the ACL.
- » **AP / AP Tags / Network** : Select the AP or AP Tags or Network on which the rules need to be implemented.
- » **Policy** : Select Accept or Deny, to allow or restrict access to a particular IP, Network or Port.
- » **Protocol** : Select either TCP or UDP
- » **Source IP** : The IP address of the source device. Only the device with the specific IP address is allowed to access any target device.
- » **Source Bitmask** : It is the number of netmask bits used for IP subnet masking of the source server. This will allow the access control to both the host as well as the network addresses. The default subnet mask bit value is 32.
- » **Source Port** : Port number or range of port numbers for the source is specified. The start and end range is separated by a colon.

- » **Destination IP Address** : If the IP addresses of the targets are also specified, then this device will be allowed access through those specific IP addresses.
- » **Destination Bitmask** : It is the number of netmask bits used for IP subnet masking of the destination server. This will allow the access control to both the host as well as the network addresses. The default subnet mask bit value is 32.
- » **Destination Port** : Port number or range of port numbers for the source is specified. The start and end range is separated by a colon.
- » To add more ACL Rules, click '+ Add ACL.'
- » Click Create ACL group.
- » The configured ACL group with the rules will reflect in the 'ACL List' table. To create more ACL Group click '+ Create New ACL'.

ACL Group

Group Name*

AP / AP Tags / Network*

+ Add ACL

Policy	Protocol	Source IP	Source Bitmask	Source Port	Destination IP	Destination Bitmask	Destination Port
Acce ▼	TCP ▼	Source IP	Source Bitm	Source Port	Destination	Destination	Destination

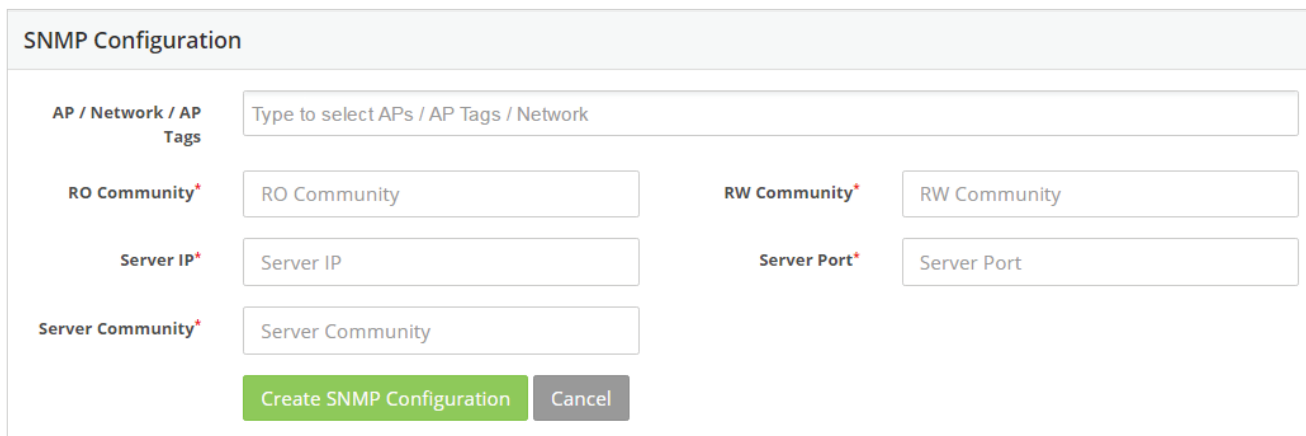
Create ACL group
Cancel

Fig 12.4

» SNMP Configurations

SNMP (Simple Network Management Protocol) is a set of standards for communication with devices connected to a TCP/IP network. SNMP provides a standardized framework and a common language used for the monitoring and management of devices on a network.

- » To configure SNMP, navigate to Organization → SNMP Configuration. - [Fig 12.5]
- » **AP / AP Tags / Network** : Select the AP or AP Tags or Network to which the SNMP Configuration is needed.
- » **RO Community** : Community string for read only Access. An empty string indicates that the operation is disabled.
- » **RW Community** : Community string for Write Access. An empty string indicates that the operation is disabled.
- » **Server IP** : It should be either a fully qualified domain name or IP Address of the NMS Server. Empty value implies no traps are issued.
- » **Server Port** : It is the port on which NMS server will listen for SNMP Traps. The default value for port number is 162.
- » **Server Community** : It is a string used for authentication to decide whether to accept or discard SNMP trap information received.
- » Click 'Create SNMP Configuration'.



SNMP Configuration

AP / Network / AP Tags:

RO Community*: RW Community*:

Server IP*: Server Port*:

Server Community*:

Fig 12.5

» Radio Profiles.

The Radio profiles are created to provide real-time RF management of the wireless network.

» To create a Radio Profiles, Navigate to Organization → Radio Profiles → + Add Radio Profile. -[Fig 12.6]

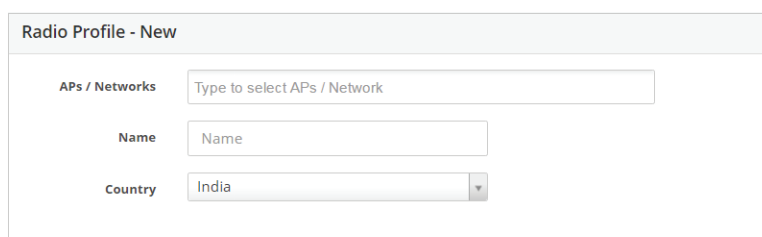
» Radio Profile New:

» **Aps/Networks** : Add the Mac Address of the AP or the whole network.

Note : If you create a Radio profile '1' by adding the whole network, and create another profile '2' and add the AP Mac Address from the same network, the profile '2' will be updated to the AP as the priority would be given to the profile with AP Mac Address over the profile with network.

» **Name** : Name of the Radio Profile.

» **Country** : Select the country for Channel and Power selection.



Radio Profile - New

Aps / Networks:

Name:

Country:

Fig 12.6

» Radio Settings: -[Fig 12.7]

» **Band** : 2.4Ghz.

» Disable/Enable based on preferences.

» Disable/Enable the 'Country IE' option based on preferences.

» Select the channel number or keep default, Auto

» The default is Auto. Set the Power from the 'Power(dbm)' drop down list

» **Band** : 5Ghz

» Disable/Enable based on preferences.

» Disable/Enable the 'Country IE' option based on preferences.

» Select the channel number or keep default, Auto.

» The default is Auto. Set the Power from the 'Power(dbm)' drop down list

» Click Create

Band	Disabled	Country IE	Channel	Power(dbm)
2.4 Ghz	<input type="checkbox"/> NO	Enable ▼	Auto ▼	Auto ▼
5 Ghz	<input type="checkbox"/> NO	Enable ▼	Auto ▼	Auto ▼

Create Cancel

Fig 12.7

13. Alerts

Alert helps real-time monitoring and notifications when certain network or device event occurs. Alerts are sent to the administrators email address.

* To Configure an Alert :

- » Navigate to Configuration → Alerts. - [Fig 13.1]
- » **Alert name** : Enter a suitable Alert name. The Alert name should highlight the nature of the alert. For example, 'Access Point Down' is an appropriate Alert name, indicating that a particular access point is offline.
- » **Message** : The section contains the alert message that needs to be sent in the email.
Use the {} tag to access the device or network details. The possible details are listed below:
 {ap_mac} = MAC address of the device.
 {client_mac} = MAC address of the client.
 {value} = Value for the Alert criteria.
 {ssid} = The name of the SSID.
 {uplink_name} = The name of the Uplink.
 {network_name} = The name of the Network.
- » **Category** : There are 3 categories – Device Alert, Client Alert, and Network Alert.
 - » **Device Alert** : The alert is configured to generate the AP behavioral notification.
 - » **Client Alert** : This is configured to generate alert pertaining to the client.
 - » **Network Alert** : The alert will give notification specific to the network.
- » **Select Color** : Select the appropriate color to indicate the criticality of the alert.
- » **Select Tags** : The tag selection is optional.
- » **Rules** : The rules will help to generate and send the notification on matching certain criteria.
- » **Device** : The option is selected for Up/Down alert of the AP. The time to generate an alert is configured in seconds.
- » **Ethernet throughput in KB** : The alert is generated when Ethernet throughput reaches the limit based on the set criteria. The options are Below, Above or Equal to.
- » **SSID throughput in KB** : The alert is generated when SSID throughput reaches the limit based on the set criteria. The options are Below, Above or Equal to.
- » **Free memory in KB** : To configure the Free memory limit of the AP notification. The options are Below, Above or Equal to.

- » **Load average** : Load average limit for the AP on which the alert needs to be generated. The options are Below, Above or Equal to.
- » **Client throughput in KB** : When Client throughput reaches the threshold value. The options are Below Above or Equal to.
- » **Client**
- » **Connected client count** : The notification for connected client count for AP or Network. The options are Below, Above or Equal to.
- » **Captive portal**
- » **Network uplink**
- » **Select Actions** : Mode of sending the alert to the Administrator. It will be either Email or SMS.

Alert - New

Alert name

Message

Note: Use {} tag for access device data. Possible data are listed here:
 {ap_mac} = Device MAC address
 {client_mac} = Client MAC address
 {value} = Value from alert criteria
 {ssid} = SSID name
 {uplink_name} = Uplink Name
 {network_name} = Network Name

Category

Select Color ☒ ☐ ☐ ☐

Select Tags

Rules ☒ Match All ☐ Match Any + Add Rule + Add Group

Automation Rules are retroactive and affect all prospects that meet the selected criteria.

Criteria	Operator	Unit
<input type="text" value="Device"/>	<input type="text" value="Above"/>	<input type="text" value="in seconds"/>

Select Actions

Create Alert

Fig 13.1

Few alert configuration scenarios :

- » **AP down Alert** : Alert is generated when AP is offline.
 - » **Alert name** : 'Access Point Down'.
 - » **Message** : Access Point with MAC Address {ap_mac} is down!
 - » **Category** : Select Device alert.
 - » **Color** : Select the Red color, denoting the failure case.
 - » **Rules** : Select 'Device' from the first section, 'Down' from the second drop down list, and assign an integer value (threshold value in seconds) in the third column for sending the alert.
- » **AP up alert** : Alert is generated when AP is back online.
 - » **Alert name** : 'Access Point Up'.

- » **Message** : 'Access Point with MAC Address {ap_mac} is up!'.
- » **Category** : Select Device alert
- » **Color** : Select the Green color, denoting the success case.
- » **Rules** : Select 'Device' from the first section, and 'Up' from the second drop down list, and assign an integer value (threshold value in seconds) in the third column for sending the alert.
- » **Ethernet throughput** : Generation of alert when the throughput is equal to the value configured.
 - » **Alert name** : 'Ethernet throughput'.
 - » **Message** : Ethernet throughput for the AP with MAC Address {ap_mac} has reached the threshold {value}'.
 - » **Color** : Select Blue color.
 - » **Rules** → Choose 'Ethernet throughput' from the first drop down list, 'Equal to' from the second drop down list, and assign the threshold value (in KB) in the third column for sending the alert.

14. Reports

The report provides a variety of statistics relating to usage of AP, SSID, and information pertaining to clients.

* To Generate Reports :

- » Navigate to Monitor → Report. Under Reports, select the appropriate section for viewing the statistics.
- » **Top 5 APs by usage** : Lists the top 5 APs in the network based on their usage during a specific time period. The report section includes AP's MAC ID, Usage (Download and Upload) and Total Usage.
- » **Top 5 Clients by usage** : Lists the top 5 Clients based on usage during a specific time period. The report section includes Client's MAC ID, Usage (Download and Upload) and Total Usage.
- » **Usage per SSID** : Provides the usage per SSID on network for a given time period. The report section includes SSID Name, Down Stream, Up Stream and Total Usage.
- » **Number of connected Clients** : Total number of clients connected to the network for a given time period.
- » **Number of connected Clients per SSID** : Total number of clients per SSID on a network. The report section will show SSID Name, Client Count and % value for clients on each SSID for the network.
- » **AP List** : Total number of APs in the network with their MAC ID and Firmware Version.
- » **AP Down time** : Lists the total number of APs and number of Non-functional APs during a given period of time. The report includes AP's MAC ID, Tags, Downtime Period and Total Downtime.
- » Select a time range.
- » Click Generate

The report generated can be either downloaded as a PDF or sent to the administrator email address using the Actions section.

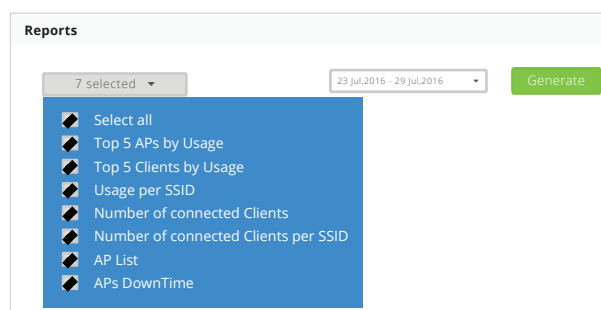


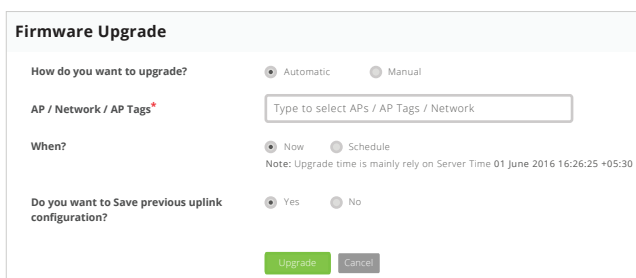
Fig 14.1

15. Firmware Upgrade

Pronto cloud controller minimizes the administrative overhead by centrally managing the firmware upgrade process for its Access Points and Routers. Administrator can schedule or perform the upgrade manually using the same Dashboard.

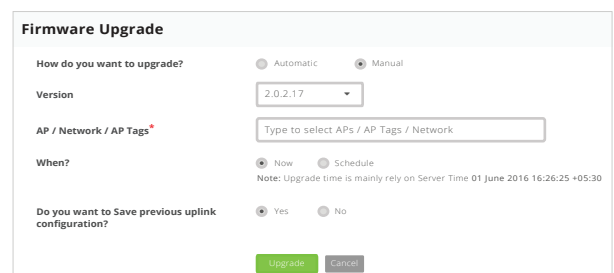
* To Upgrade the firmware :

- » Navigate to Configuration → Upgrade.
 - » **How do you want to upgrade?**
 - » **Automatic** : On selecting the mode, firmware will be automatically upgraded. Administrator can plan and schedule the Date and Time for the upgrade. The configured device will be automatically recognized and appropriate firmware will be updated to the AP or Router.
 - » **Manual** : In this mode, user has to select the firmware version.
 - » **Version** : The latest and old firmware versions are listed. This option is only available for manual upgrade.
 - » **AP / Network / AP Tags** : The firmware upgrade can be done on individual AP, AP Tags or the whole network.
 - » **When?** :
 - » **Now** : Select this option to upgrade the image immediately to a newer version.
 - » **Schedule** : Set the date and time for the upgrade.
 - » Do you want to save previous uplink configuration?
 - » **Yes** : Selecting this option will save the following configurations of the AP or CPE during the upgrade.
 - » Static IP of the AP/CPE.
 - » Wireless bridge configuration.
 - » **No** : Selecting this option will not save the above configurations.
 - » Click Upgrade.



The screenshot shows the 'Firmware Upgrade' dashboard. Under 'How do you want to upgrade?', the 'Automatic' radio button is selected. The 'AP / Network / AP Tags' field has a text input box with the placeholder 'Type to select APs / AP Tags / Network'. Under 'When?', the 'Now' radio button is selected. A note states: 'Note: Upgrade time is mainly rely on Server Time 01 June 2016 16:26:25 +05:30'. At the bottom, there are 'Upgrade' and 'Cancel' buttons.

Fig 15.1



The screenshot shows the 'Firmware Upgrade' dashboard. Under 'How do you want to upgrade?', the 'Manual' radio button is selected. The 'Version' dropdown menu is set to '2.0.2.17'. The 'AP / Network / AP Tags' field has a text input box with the placeholder 'Type to select APs / AP Tags / Network'. Under 'When?', the 'Now' radio button is selected. A note states: 'Note: Upgrade time is mainly rely on Server Time 01 June 2016 16:26:25 +05:30'. At the bottom, there are 'Upgrade' and 'Cancel' buttons.

Fig 15.2

16. Logging

An event log is a basic resource that helps provide information about network traffic, usage and other conditions. It stores these data for retrieval by security professionals or automated security systems to help network administrators manage various aspects such as security, performance and transparency.

* For Logging :

- » Navigate to Configuration → Logging.
- » Select the network from the drop down list.

- » **Logging Name** : Provide a suitable logging name. -[Fig 16.1]
- » **Logging Type** : In case of 'Event Logging', provide a suitable logging name and choose 'Event Logging' from the drop down list. Please note, only a single instance of Event Logging can be created.
- » **For CALEA configuration :**
 - » **Logging Name** : Provide a suitable logging name.
 - » **Logging Type** : Choose 'CALEA' from the drop down list.
 - » **Upload File** : Select 'FTP' from the drop down list.
 - » **Upload URL** : Provide the URL of the location where the log file needs to be uploaded.
 - » **AP/AP Tags/Network** : Add MAC addresses of the APs for which the log file needs to be created.
 - » **Upload User & Password** : Provide a username and password to upload the log file.
 - » Click 'Create Logging' to add the configuration to the logging list.

The 'Logging List' contains the list of the created configurations.

Fig 16.1

* Event Logging :

- » Navigate to Monitor → Event Logging.
- » Select the network from the drop down list.

'Event Logging List' contains a details list of the logging events based on live and historical data. The list can be filtered based on several parameters such as 'Access Points' and 'Clients'.

* Live Data :

This feature helps to monitor live logs of the current scenario.

- » **Authentication** : The devices that have successfully been authenticated
- » **Association** : The devices that are connected to the SSID
- » **Disassociation** : The devices that are authenticated but not connected to the network

The 'Live Data' can be filtered based on the above mentioned criteria and the result can be viewed in the table below.
Access Point: Provide the MAC addresses of the APs to monitor their activities live.

* History Data :

Get details of event logs for a specified time frame. Choose the desired option from the 'Event Range' drop down list to view data for the specified time frame. The below table shows the details of the search.

- » **Time Stamp** : The devices that have successfully been authenticated
- » **AP** : MAC address of the AP
- » **TYPE** : The nature of event i.e. association, authentication or disassociation
- » **Client MAC** : MAC address of the device associated with the event
- » **Description** : Detailed description of the event

17. Tools

- » **Ping:** Add the MAC address of the AP
 - » **IP Address/Host:** Provide the address of the Host for which the reachability needs to be tested. Ping is used diagnostically to ensure that a host computer that a user is trying to reach is actually working.
 - » **TRACE ROUTE:** It is a tool for displaying the route through which the connection between the host and the user is established. It will list all the routers it passes through until the connection is established.
- » **DNS Routing:**
 - » **Select AP:** Add the MAC address of the AP
 - » **Host:** Provide the address of the Host for which the reachability needs to be tested.
 - » **NS Lookup:** A program that lets any computer user enter a host name and find out the corresponding IP address.

18. VPN Configuration

A virtual private network is a network technology that creates a secure network connection over a public network.

- » **Connection Name:** Provide a suitable name for the connection - [Fig 18.1]
- » **Enable:** Select 'Yes' to enable the VPN connection
- » **AP :** Add MAC address of the AP
- » **Local Subnet Mask:** Provide the subnet mask of the local network
- » **Enable Server-Client:** By default, the connection is set as site to site. By enabling this option, you can choose between a client and the server
- » **Remote Peer IP :** Add the IP address of the peer machine
- » **Remote Network:**
 - » **Remote Network IP :** Provide the IP address of the remote network
 - » **Remote Subnet Mask:** Provide the subnet mask of the remote network
- » **Authentication:**
 - » **Method :** Choose the authentication method as PSK
 - » **Pre-shared Key :** Provide a pass key for establishing the VPN connection
 - » **IKE Version:** Internet Key Exchange version 2 is selected by default
- » **Phase 1 Selector (IKE):**
 - » **Encryption:** Select the desired encryption type from the drop down list
 - » **Authentication:** Select the desired authentication type from the drop down list
 - » **Diffie-Hellman Group:** Select the type of algorithm to be used to generate a shared secret key to encrypt further IKE communications
 - » **Key Lifetime:** Provide the value for which the pass key will be active. The input should be given in minutes
- » **Phase 2 Selector (ESP):**
 - » **Encryption :** Select the desired encryption type from the drop down list
 - » **Authentication:** Select the desired authentication type from the drop down list

'Create VPN' to save the configurations

VPN

Connection Name

Enable

NO

AP

00:0C:66:10:74:F0

Local Network Subnet

Enable Server-Client

NO

Note: By default it will be site to site

Remote Peer IP

Remote Network

Remote Network

Remote Network Subnet

Authentication

Method

PSK

Pre-shared Key

show

IKE Version

2

Phase 1 Selector(IKE)

Encryption

3DES

Authentication

MD5

Diffie-Hellman Group

MODP768

Key Lifetime (M)

Phase 2 Selectors(ESP)

Encryption

3DES

Authentication

MD5

Create VPN

Cancel

VPN Configuration List

10 records per page

Search:

Name	AP	Enable/Disable	Remote IP	Remote Network IP	Remote Network Subnet	Local Subnet	IKE Time	IKE	ESP	Action
No data available in table										

Showing 0 to 0 of 0 entries

Previous

Next

Fig 18.1

Contact Us

Call us or write to us at the below contacts for any assistance required.

Email : support@prontonetworks.com

Phone : +91-080-44469494 / +01-866-809-2323

HQ Address : Pronto Networks Inc, 955 Pleasant Hill Road, Lafayette, CA 94549.