

*mimosa*TM



A5-360 14, A5-360 18 User Guide

A5-360 Installation Instructions



NOTE: Installations instructions are included on the product packaging

1. Unlock



IMPORTANT

An unlock key must be obtained online before installing the product.

2. Mount



Using the included pole mount clamps, tightly attach the bracket to the top section of your mounting pole with a flathead screwdriver.

3. Ground



Use minimum 10 AWG (5.26 mm²) ground wire, less than 1 m in length.

4. Connect



Use only shielded CAT 6 cabling and seal the system with the IP67 gland as shown.

Table of Contents

Access Points	1
User Guide	1
Overview	1
Accessing the Interface	1
Logging In	2
User Interface Overview	3
Dashboard	5
Dashboard Overview	5
Performance	6
Device Details	7
Connected Clients	8
Wireless	9
Clients	9
Client List	9
SSID	11
SSID Management	11
Site Survey	14
Survey Results	14
Channel & Power	15
Spectrum Analyzer	15
Channel & Power Settings	16
Exclusions & Restrictions	18
Location	19
Local Satellite Signals	19
Satellite Information	20
Location Data	21
Traffic	22
Access Control Lists	22
Traffic Shaping Plans	23
Preferences	25
General	25
Naming	25
Set Password	26
Management	27
Management IP	27
VLAN Management	28
Firmware & Reset	29
Device Firmware	29
Reset & Reboot	30
Backup & Restore	31
Backup & Restore	31

Diagnostics	32
Logs	32
Log Overview	32
Tests	33
Tests	33
Ping	34
Traceroute	35
SNMP Interface	36
SNMP OID Reference Tables	36

Accessing the Graphical User Interface

Accessing the graphical user interface (GUI) requires that the radio first be connected to power. The Power over Ethernet (PoE) connection process describes the steps to do this. Note that the GUI will be available approximately one minute after applying power.

The GUI can be accessed in three ways to facilitate set-up and management.

1. Locally through the built-in 2.4 GHz wireless management network (A5 Only)
2. Through the local Ethernet interface (LAN)
3. Remotely through the 5 GHz wireless link

Via 2.4 GHz Management Network

On any device with 2.4 GHz 802.11n capability, go to the wireless network listing and connect to the Local Network Management wireless network (SSID): "mimosaMXXX". The default passphrase for the 2.4 GHz connection is "mimosanetworks". Once connected, type 192.168.25.1 into your browser. Please note that both the Local Network Management SSID and passphrase are configurable by the user, so their values could be different from the default values.

Via Ethernet interface or in-band over the 5 GHz Wireless link

By default, the device IP address is 192.168.1.20 and can be accessed via the Ethernet port using this IP address in any standard Web browser. To access the device via a locally connected computer initially (on the same LAN or directly to the Ethernet port), the computer's IP address must be on the same subnet as the above address. Once you have modified the IP address (static or is DHCP) of the device for remote management purposes (in-band over wireless or over the Ethernet interface), the new specified IP address must be used to access the device. This is important to do in order to avoid IP address conflicts with other devices on the network. Current IP addresses of different Mimosa devices on the network can be identified using terminal-based discovery. It is highly recommended to change the default password to a unique and secured password.

Logging In

After connecting via one of the three access methods, the GUI will prompt you to log-in with a password. The default password is "mimosa", and should be changed immediately after login to protect your network since it gives the user read / write privileges. The password can be changed within the Preferences > General > Set Password panel of the GUI.



If you are looking for the Mimosa Cloud Log In process, please see [Manage User Guide: Logging In](#).

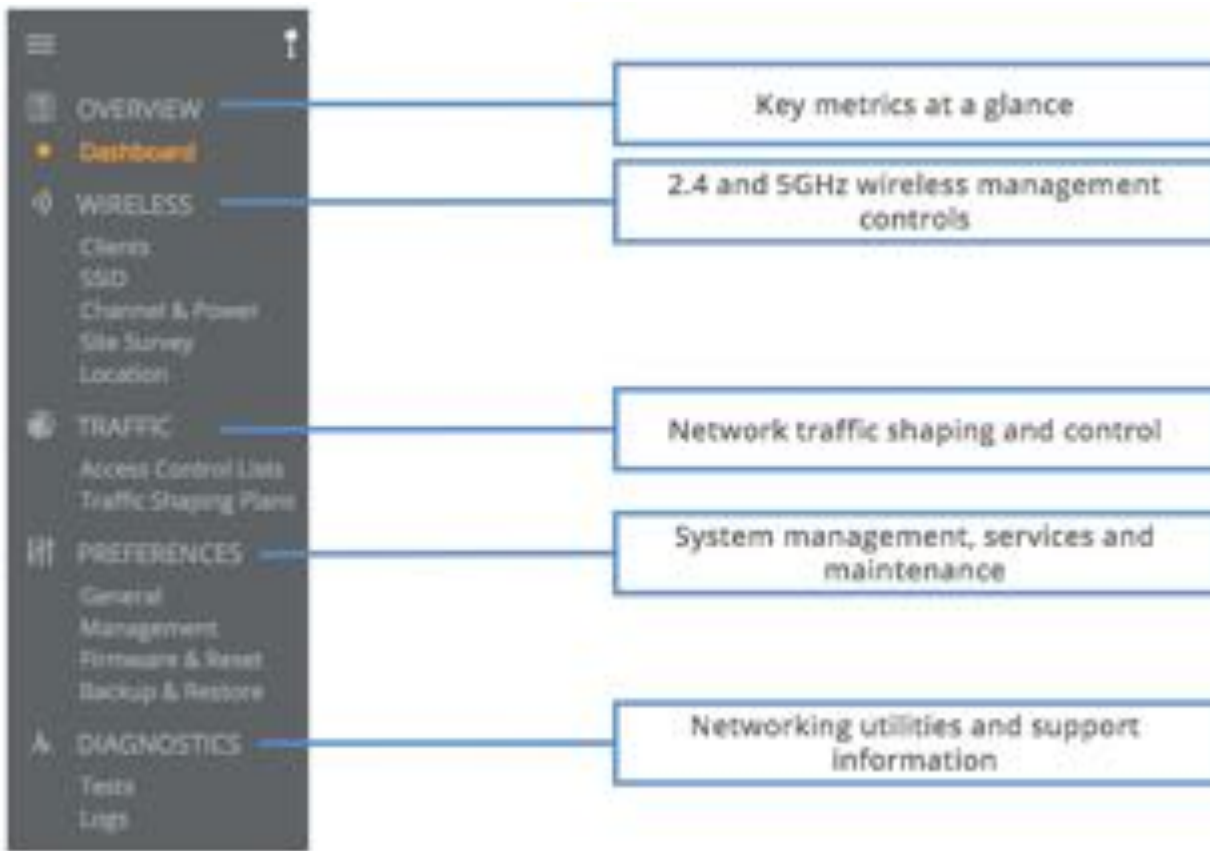
User Interface Overview

When you first log in, you'll notice that there is a title bar with the device name shown in the top-right corner, a navigation pane on the left, and a large content pane on the right. The default page shown in the content pane is the Dashboard, which shows a summary of overall performance at a glance, and highlights both radio and link parameters that affect link health.



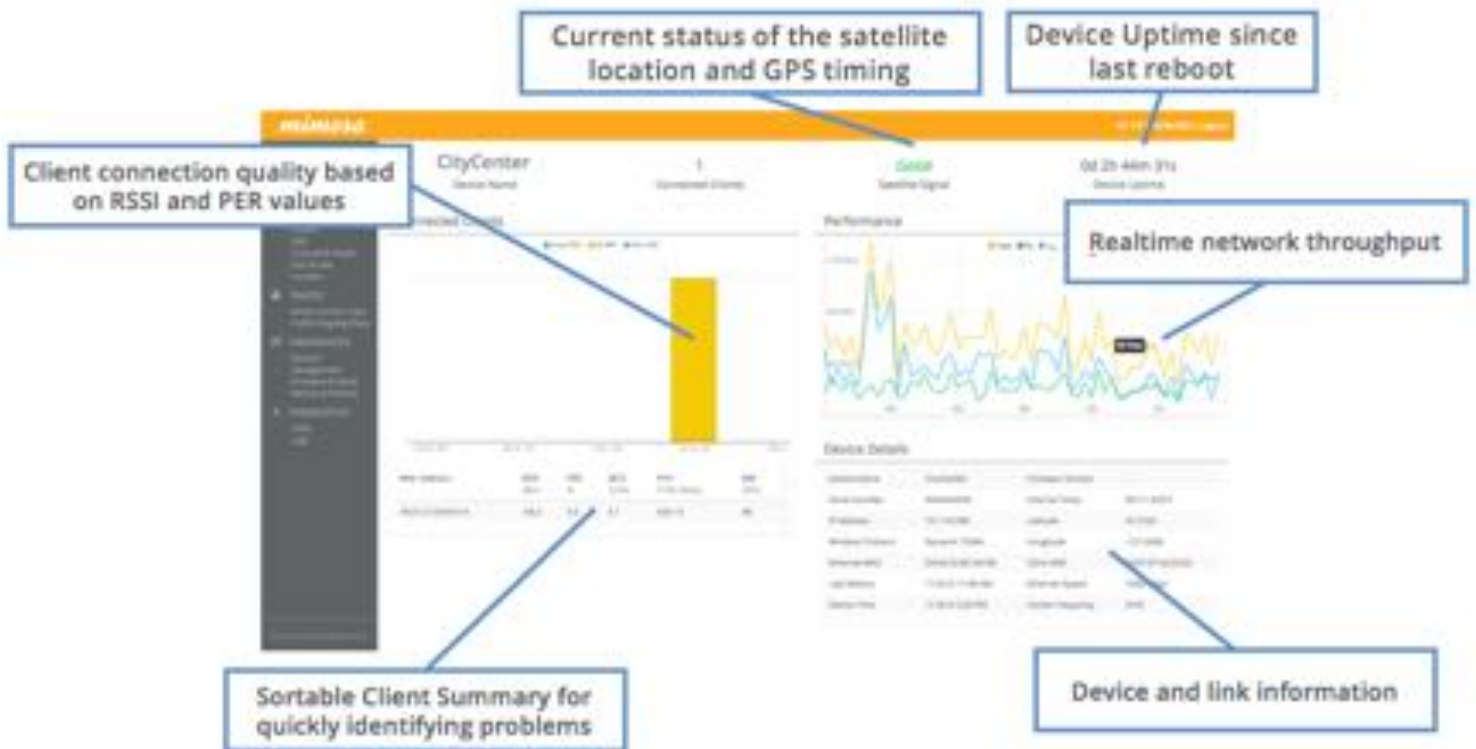
On the left navigation pane, there are four prominent sections: Overview, Wireless, Preferences, and Diagnostics. Each of these sections contains one or more links to pages containing task-related data, controls, and tools used to administer the radio...and you can return the Dashboard at any time by clicking on the Dashboard link in the Overview section.

The pin in the top corner of the left navigation pane allows you to "pin" open the navigation menu for easier access. Else, the menu contracts to provide more workspace within the GUI. Note that the 2.4 GHz Console menu item is not present on the B5-Lite.



The Dashboard

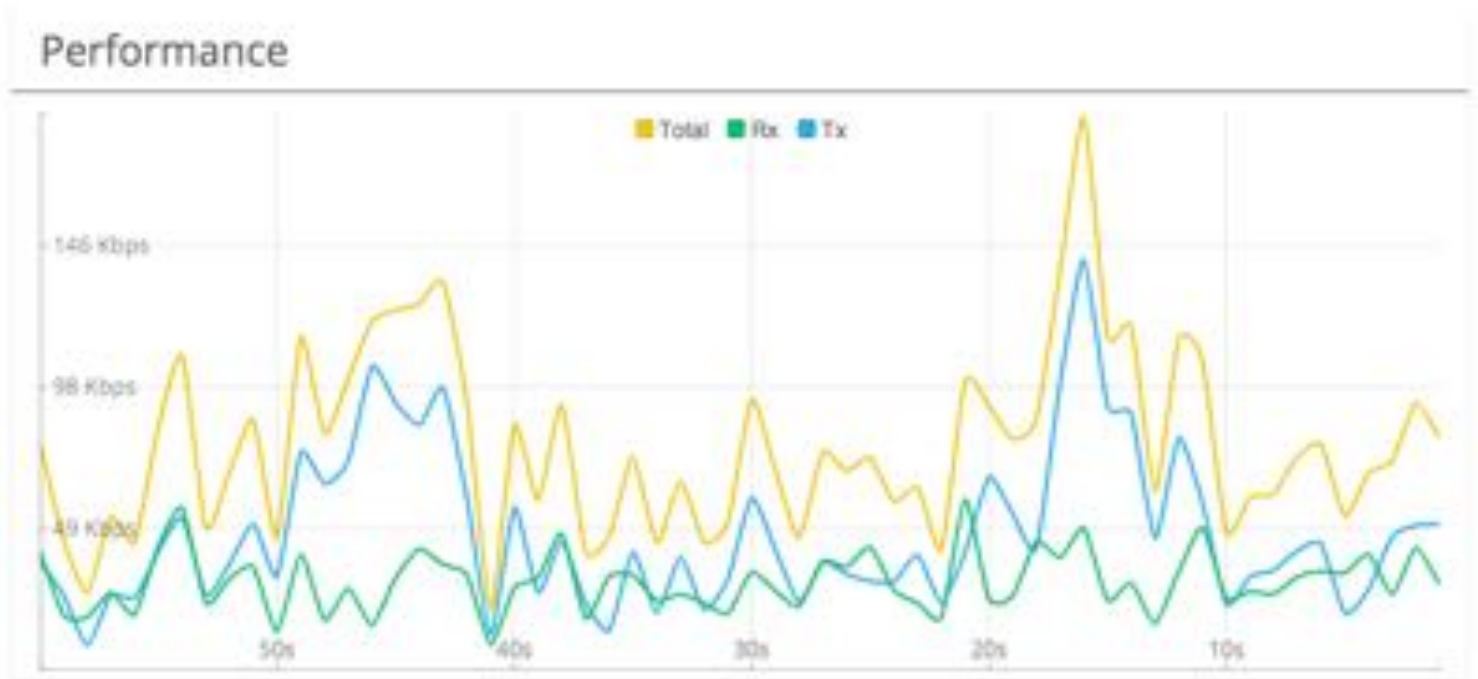
The Dashboard contains several panels used to group related items. The status panel at the top of the page shows the device name, the number of connected clients, GPS signal quality, and Device Uptime since the last reboot. Detailed help text can be found by clicking on the information icon in the upper right hand corner.



Reading the Performance Charts

IP Throughput is charted over 60 seconds in 5-second intervals. The newest data shows up on the right and scrolls to the left over time. If enabled, click on the cloud icon to view historical data within the Manage application.

The IP Throughput graph plots three lines representing transmit, receive, and total (summed) throughputs at the datagram (or packet) layer excluding any protocol or encapsulation overhead. The results here may differ from those measured using speed test tools, due to protocol overhead and encapsulation. Note that internal Bandwidth test results are excluded.



Reading Device Details

The Device Details panel shows the summary of details for the local device configurations and status. Client details are available on the Wireless->Clients page.

The table shows the following for both Local device:

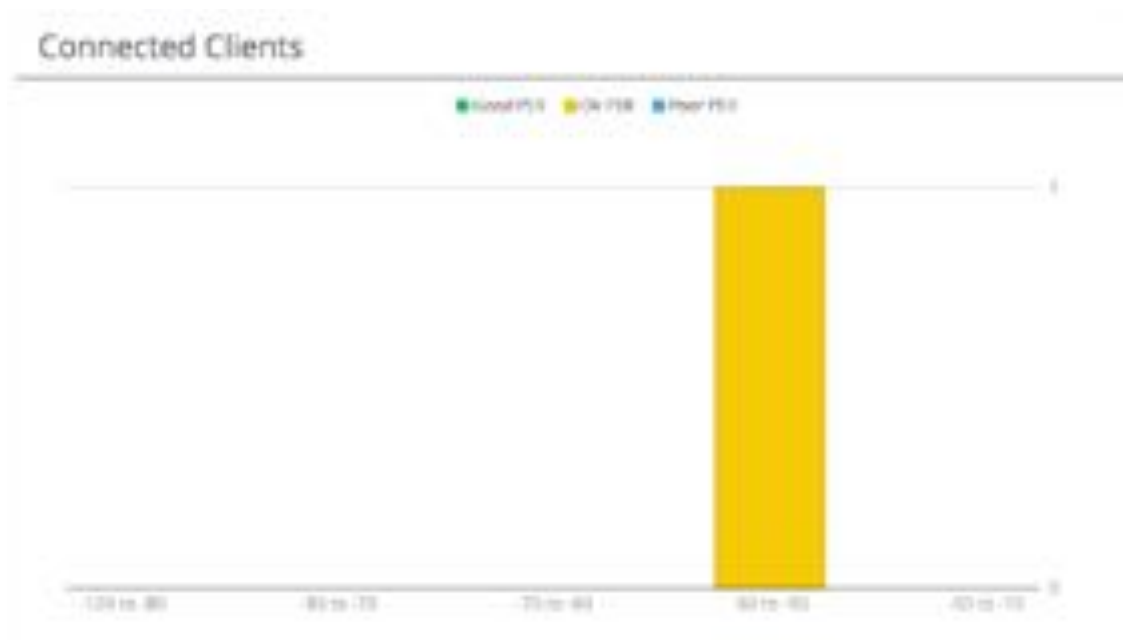
- Device Name: The friendly name given to each device. (Set in *Preferences > General > Naming*)
- Serial Number: The unique identifier for the device assigned at the factory.
- IP Address: The IP address of each device and how it was assigned. (Set in *Preferences > Management*)
- Wireless Protocol: The MAC level protocol is always Dynamic TDMA
- Ethernet MAC: The unique identifier for the physical Ethernet interface.
- Last Reboot: The date and time at which each device last rebooted.
- Device Time: The date and time set on the unit in UTC.
- Firmware: The latest firmware version applied to each device. (Set in *Preferences > Update & Reboot*)
- Internal Temp: Temperature on the device CPU (operating range: -40 °C to +110 °C).
- Latitude: GPS derived latitude coordinates in decimal format
- Longitude: GPS derived longitude coordinates in decimal format.
- 5 GHz MAC: The unique identifier for the 5 GHz radio.
- Ethernet Speed: Data rate and duplex mode of the wired Ethernet interface.
- Center Frequency: Center frequency of the current channel in MHz.

Device Details

Device Name	Charlie360	Firmware Version	--
Serial Number	4545454545	Internal Temp	96°C / 205°F
IP Address	10.1.10.249	Latitude	37.2109
Wireless Protocol	Dynamic TDMA	Longitude	-121.5604
Ethernet MAC	D4:AE:52:BC:A5:08	5GHz MAC	10:01:01:02:02:02
Last Reboot	11/3/15 11:36 AM	Ethernet Speed	1000 Mbps
Device Time	11/3/15 3:38 PM	Center Frequency	5745

Reading the Connected Clients chart and table

The Connected Clients graph shows all the connected clients grouped by RSSI values. It's design allows for quick determination of the network health based on the clients signal strenght from the AP. For each RSSI range, the clients are depicted by Packet Error Rate (PER) grouping showing the total number of clients for specific PER ranges, color coded by their health. The PER ranges for each RSSI cluster of clients is: 0-3% PER = Good, 3-5% PER = Ok, 5+% PER = Bad.



The client list show sortable, summarized data for quickly showing the clients with poor RSSI or PER. The first clicking on the RSSI or PER column heading will sort the list of clients worst to best, then best to worst.

MAC Address	RSSI dBm	PER %	MCS Tx/Rx	PHY Tx/Rx Mbps	BW MHz
78:31:C1:D4:F4:1A	-57.7	9.3	5 /	520 / 0	80

Reading Client List Tables

The client list provides a detailed table of data stream level statistics for MCS index, PHY, Packet Error rates and Rx Error Vector Magnitude (EVM).

MAC/Device Name - If the client device name is known for the remote device it will be shown in the list, otherwise the client MAC address will be shown.

BW (MHz) - This value shows the current channel width setting used by the client.

Tx/Rx Mbps - The current throughput averaged over the past 10 seconds is shown for both the Tx (transmit) and Rx (receive) traffic.

PHY (Tx Mbps, Rx Mbps) -

Streams - The number of streams the client is currently connected to the access point.

Tx MCS is an indicator of how well the remote radio can receive data from the local transmitter. The Rx MCS indicates how well the local radio is receiving data from the remote transmitter.

The Modulation Coding Scheme (MCS) represents how much data can be sent at a time, so directly affects potential throughput represented by the PHY rate. The higher the MCS index (ranging from 0-9), the more data that can be sent per transmission. A disadvantage of higher MCS indices is that they require higher SNR since they are more vulnerable to noise.

PER % - Packet Error rate

RSSI - Receive Signal Strength Indicator

The Error Vector Magnitude (EVM) indicates the difference between the actual and expected amplitude and phase of an incoming signal. Smaller values are better (e.g. -30 dB is better than -10 dB).

Rate Adaptation dynamically adjusts both the MCS and the number of streams depending on RF conditions. Poor RF conditions (i.e. interference) causes PER to increase. PER and MCS are inversely correlated meaning that as PER increases, MCS decreases and vice versa.

Client List														
MAC	BW MHz	Tx/Rx Mbps	PHY Tx/Rx Mbps	Streams #	MCS Tx/Rx	PER %	RSSI 1 dBm	RSSI 2 dBm	RSSI 3 dBm	RSSI 4 dBm	EVM 1 dB	EVM 2 dB	EVM 3 dB	EVM 4 dB
78:31:C1:D4:F4:1A	80	0.00 / 0.00	390 / 0	2	4 /	10.5	-67.8	-63.0	-62.6	-62.7	-29.8	0.0	0.0	0.0

Related:

Backhaul FAQ: What SNR is required for each MCS?

Backhaul FAQ: What is the sensitivity for each MCS index?

Backhaul FAQ: What's a good EVM?

SSID Configuration Settings

The SSID Management panel contains controls for configuring how client devices will connect to the access point. To add a new SSID, click on the Add New SSID circle. To delete an SSID, click on the blue X icon at the top of the SSID panel. The following settings control how the SSID will operate.

- Name - The name of the SSID.
- Which Band? - The frequency operation for the SSID. Choices are 5 GHz or 2.4 GHz.
- TDMA Window - Determines the length of the transmit time slot in milliseconds.
- SSID Type- Selects the type of clients that will connect to an SSID. Choices are CPE for fixed wireless devices for Hotspot for mobile Wi-Fi devices such as mobile phones, laptops, etc.
- Enable - This enables the SSID operation if set to ON. When set to OFF SSID operations are disabled.
- Broadcast SSID- When turned on, this feature does not broadcast the name of the SSID in the beacon. Wireless clients will need to manually enter the SSID name and security settings when operation in this mode. Note, while referred to as a hidden SSID, it is still possible to detect the presence of a non-broadcast SSID.
- Wireless Client Isolation- Wireless Client Isolation prevents clients from communicating with each other on the same SSID.
- Security - Wireless This option is used to configure the security encryption used by the SSID. Options are :
 - Open - No authentication or encryption is used. This operational mode is not secure.
 - Pre-Shared Key - There is no user authentication but the link is encrypted using a pre-shared key.
 - Enterprise - Users are authenticated and encrypted using radius. You must specify the Radius Server IP, Radius Secure, Radius Auth Port and Radius Accounting Port.

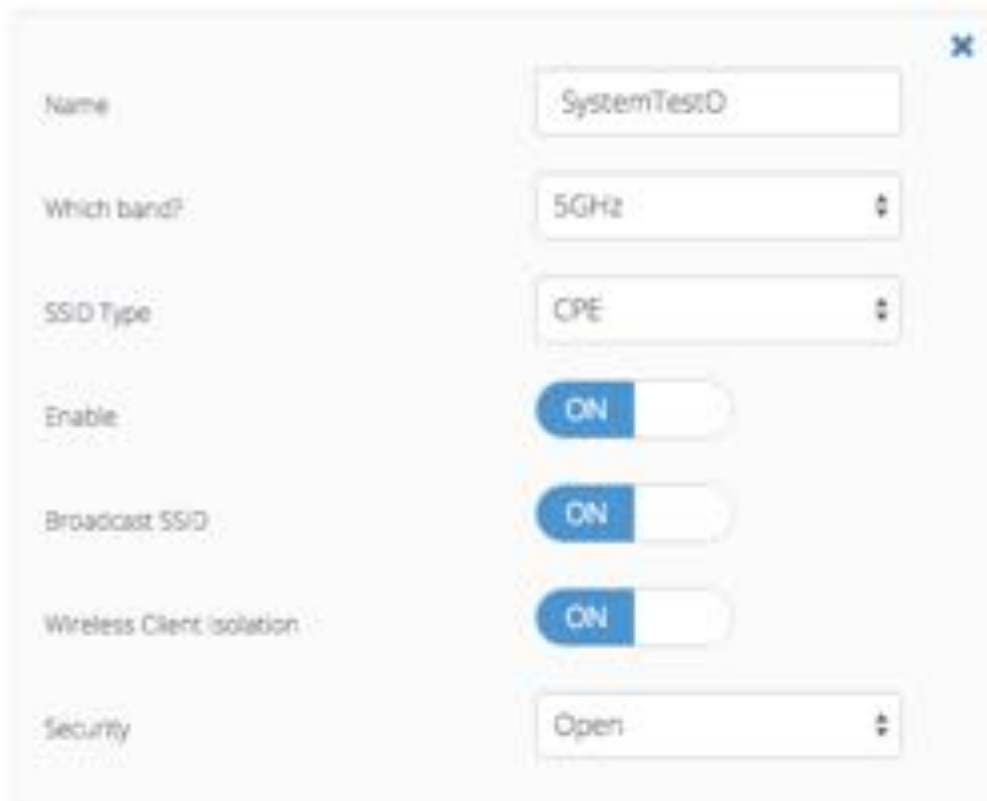
Pre-Shared Key SSID Configuration

SSID Management



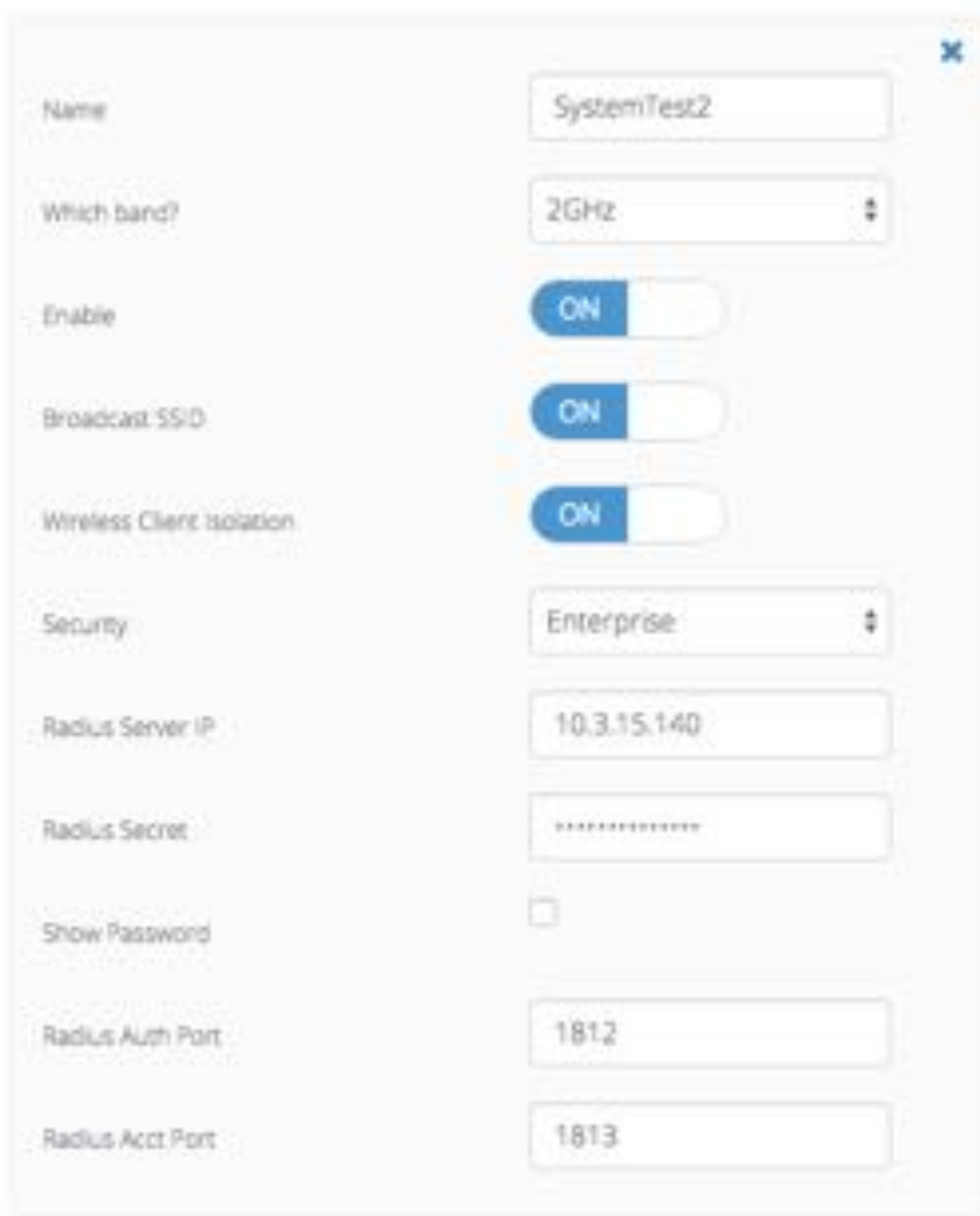
The screenshot displays the SSID Management interface. On the left, a configuration panel for an SSID named 'CharlieSSID' is shown. The settings include: Name: CharlieSSID; Which band?: 5GHz; SSID Type: CPE; Enable: ON; Broadcast SSID: ON; Wireless Client Isolation: ON; Security: Pre-Shared Key; Password: [Redacted]; and Show Password: [Off]. To the right of this panel is a large grey circular button with a blue plus sign and the text 'Add New SSID'.

Open SSID Configuration



The screenshot shows a configuration dialog box for an Open SSID. The settings are: Name: SystemTest0; Which band?: 5GHz; SSID Type: CPE; Enable: ON; Broadcast SSID: ON; Wireless Client Isolation: ON; and Security: Open.

Enterprise SSID Configuration



The image shows a configuration window for an Enterprise SSID. The window has a close button (X) in the top right corner. The configuration fields are as follows:

Field Name	Value / State
Name	SystemTest2
Which band?	2GHz
Enable	ON
Broadcast SSID	ON
Wireless Client Isolation	ON
Security	Enterprise
Radius Server IP	10.3.15.140
Radius Secret	*****
Show Password	<input type="checkbox"/>
Radius Auth Port	1812
Radius Acct Port	1813

Reading Site Survey Results

The Survey Results status table summarizes the results of a site survey, including the SSIDs broadcast by other devices, their configuration and capabilities. Note that the Site Survey function is only available on radios configured as a Station (versus AP).

The table provides the following data per device found:

- SSID - The wireless link name advertised by each detected AP.
- Vendor - The name of the device manufacturer (if known).
- MAC Address - The device's unique identifier.
- Capability - Indicates which 802.11 (Wi-Fi technology standard) is support by the device. Options include A, G, N, AC.
- Channel - Lists the channel on which the device operates.
- Channel Width - The size (in MHz) of the channel on which the device operates.
- Frequency Range - The specific frequency range (in MHz) within the Wi-Fi channel that the device operates.
- Signal Strength - The received power level (in dBm) from each detected AP.

Use the Start Survey button to place the radio into the scan mode to search for 802.11-compatible access points.

NOTE: It is important to note that running a site survey will temporarily take down your 5GHz access point. Once activated, this process cannot be stopped until complete. Please plan accordingly.

Start

The Site Survey may take up to 20 seconds to complete. Your site will be unavailable during this time.

Survey Results

SSID	Vendor	MAC	Capability	Channel	Channel Width (MHz)	Frequency Range	Security	Signal
XXXXXXXXXX	Mimosa	XXXXXXXXXXXX	11a, 11g, 11n	36	40	5140 - 5220	Pre-Shared-Key	-87
XXXXXXXXXX	Mimosa	XXXXXXXXXXXX	11a, 11g, 11n	149	40	5755 - 5795	Pre-Shared-Key	-91
XXXXXXXXXX	TP-Link	XXXXXXXXXXXX	11a, 11n	36	40	5140 - 5200	Pre-Shared-Key	-85
XXXXXX	Aruba	XXXXXXXXXXXX	11a, 11n	36	40	5140 - 5200	Pre-Shared-Key	-81
XXXXXXXXXX	TP-Link	XXXXXXXXXXXX	11a, 11n	36	40	5140 - 5200	Enterprise	-81
XXXXXXXXXX	Mimosa	XXXXXXXXXXXX	11a, 11g, 11n	40	40	5180 - 5240	Pre-Shared-Key	-88
XXXXXXXXXX	TP-Link	XXXXXXXXXXXX	11g, 11n	133	40	5740 - 5785	Enterprise	-85
XXXXXXXXXX	TP-Link	XXXXXXXXXXXX	11a, 11n	133	40	5740 - 5785	Enterprise	-85

Reading the Spectrum Analyzer

The Spectrum Analyzer actively scans the 5 GHz band in the background to report on interference sources that may impact link performance. Click on the half circle icon in the upper right to toggle the graph's background color between black and white.

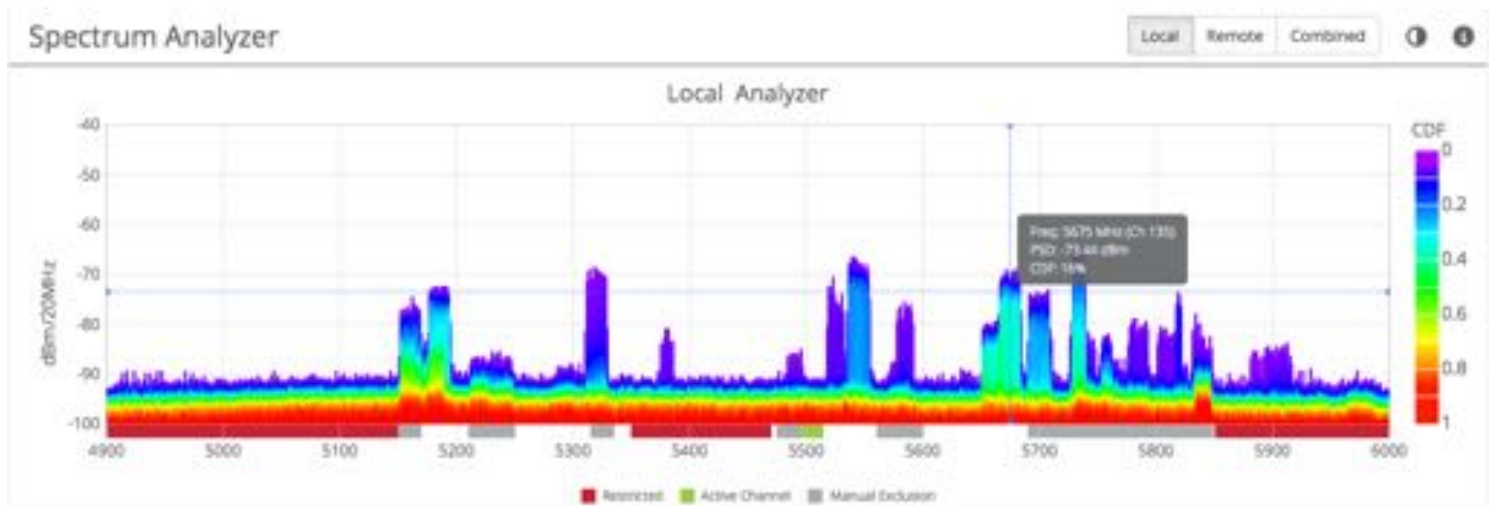
Channels in use have higher Power Spectral Density (PSD) on the vertical axis, and are shaded in different colors to represent how often the signals are likely to be on the same frequency at the same amplitude.

The legend to the right of the graph explains the color code for the Cumulative Distribution Function (CDF). The color red suggests the highest probability (1 = 100%), while purple represents the lowest probability (0 = 0%).

Cross hairs appear on the graph beneath the mouse pointer along with an information box containing the frequency (channel), PSD, and CDF values.

There are three types of markings, or bars, immediately beneath the graph's horizontal axis that indicate frequency ranges that are restricted, manually excluded, or in active use by this link. Note that traffic from the Active Channel is excluded from the display so that noise can be detected.

NOTE: Viewing Remote or Combined Spectrum View is not supported on the A5 at this time.



Managing Channel & Power Settings

The Channel and Power Settings panel allows for either automatic or manual changes to frequency, channel width, and power for either one or two channels.

5 GHz Channel & Power

- Channel Width (MHz) - Choose the channel width access point operation. Choices are 20 MHz, 40 MHz or 80 MHz.
- Center Frequency (MHz) - Select the center frequency of the channel used on the access point. The center frequency represents the absolute center of the selected channel width without any offset.
- Power - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency.
- Wireless Protocol- Select the wireless protocol to limit the maximum connection rates. Choosing 802.11a, 802.11a/n, or 802.11 a/n/ac will limit the clients from connecting at a higher PHY rate than specified.

2.4 GHz Channel & Power

- Channel Width (MHz) - Choose the channel width access point operation. Choices are 20 MHz, 40 MHz or 80 MHz.
- Center Frequency (MHz) - Select the center frequency of the channel used on the access point. The center frequency represents the absolute center of the selected channel width without any offset.
- Power - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency.
- Wireless Protocol - The wireless protocol is fixed to allow any 802.11b/g/n PHY rates.

Automatic Gain Control

- Automatic Gain Control - Choose the Automatic Gain Control setting to set the signal at which the radio ignores incoming RF signals. The choices are Off, Automatic, or Manual. For Manual entry set the max AGC gain level in dB.

5GHz Channel & Power

Channel Width (MHz)

80



Center Frequency (MHz)

5745



Power (dBm)

5



Wireless Protocol

802.11a/n/ac



2.4GHz Channel & Power

Channel Width (MHz)

20



Center Frequency (MHz)

2437



Power (dBm)

16



Wireless Protocol

802.11b/g/n

Automatic Gain Control

Automatic Gain Control

Off



Managing Exclusions & Restrictions

Exclusions list the frequency ranges in which the device should not operate. The excluded bands will be shown as shaded regions on the Spectrum Analyzer.

- Start - Specify the lower limit for the exclusion range, not including this frequency.
- End - Specify the upper limit for the exclusion range, not including this frequency.
- Add Exclusions - The button to add the Start and End frequency range to the exclusion list.
- Existing Exclusions and Restrictions - Exclusions can be removed from the list by clicking on the trash icon. The restricted bands with the lock icon cannot be removed. They are protected because of regulatory requirements.
- Regulatory Domain - The country in which the device has been configured to run.

In the United States, if either the AP or STA are within a 60 km radius of a Terminal Doppler Weather Radar (TDWR) location, one or more 30 MHz restrictions are automatically created to avoid the TDWR operating frequencies.

Exclusions & Restrictions

Add a New Exclusion (MHz)

Start Frequency End Frequency

⊕ Add New Exclusion

Exclusion Start (MHz)	Exclusion End (MHz)	
5000	5100	

Regulatory Domain: US

Related:

Change Unlock Country - Replace an existing unlock code to enable another regulatory domain

Interpreting Local Satellite Signals

The Local Satellite Signals panel contains a chart showing both GPS and GLONASS satellites in blue and green, respectively, from which the radio can obtain position and timing data used for synchronization. Each numbered column represents a unique satellite with the columns' amplitude representing the signal to noise ratio of the satellite's signal at the radio's receiver. The number of satellites the radio detects and the SNR of each both contribute to clock accuracy.

If GPS location is detected, a Google location image of the access point location will be shown on the leftmost portion of the Satellite Signal page. If no GPS signals are detected the Google location map will not be shown.



Reading Satellite Information

The Satellite Information panel contains values that represent and contribute to clock accuracy. Good GPS signal strength is required for maximum performance, as the GPS is used to synchronize timing between devices.

- Satellite Signal Strength - Qualitative assessment based on all items below; also displayed on the Dashboard.
- Satellite Avg SNR - Average signal to noise ratio amongst satellites.
- Total Satellites - Sum of detected GPS and GLONASS satellites.
 - GPS - Number of GPS satellites detected.
 - GLONASS - Number of GLONASS satellites detected.
- Clock Accuracy - Timing signal accuracy measured in parts per billion (ppb).

Satellite Information			
Satellite Signal Strength	Good	Total Satellites	8
Satellite Avg SNR	5.95 dB	GPS	1, 3, 8, 11, 19, 22, 31, 32
		GLONASS	

Viewing Location Data

Status table showing location, altitude, and heading for both the local and remote devices, as well as the link distance between them. The link length in the middle of the table will show "Disconnected" if a connection has not been established.

Location Data	
Latitude	37.21
Longitude	-121.56
Altitude	32.80 m / 107.61 ft

Managing Access Control Lists

Access Control Lists remark QoS settings and control the flow of traffic by allowing or denying network traffic based on matching criteria for MAC or IP address, network protocol. Use the + Add a New Rule button to create a new Access Control List entry or use the Blue Trash icon to remove an existing entry.

- Unique Name - Automatically configure channel, channel width and power to optimize performance based on spectrum data.
- Direction - In Manual Mode, choose the number of link channels (single or dual) and the channel width for each (Example: 2x80 MHz represents two channels with 80 MHz each, totaling 160 MHz). Single channel options ending in "FD" allow for different transmit and receive frequencies on Channel 1 & 2, respectively.
- Match Type - Select the maximum channel width Auto Everything is allowed to use. The decision for single or dual channel modes will be made automatically. For example, selecting 40 MHz as the maximum channel width may result in 1x40 or 2x20 mode. Smaller channel widths may also be selected based on RF conditions. Auto Everything is designed to maintain the highest link bandwidth while maintaining link stability.
- Source Address/Mask - In Off (Manual) mode, select the center frequency of the channel used on the link. In all modes, the center frequency represents the absolute center of the selected channel width without any offset, and the center can be moved in 5 MHz increments. If Auto Everything is set to On, the Channel(s) will be automatically set, and not editable.
- Destination Address/Mask - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency. If Channel Width is set to 1xN MHz, Channel 2 will not be used. If Auto Everything is set to On, Tx Power will be automatically set, and not editable. In "FD" mode, Power 1 and Power 2 represent transmit power on the local and remote sides, respectively.
- Protocol - Set the gain according to antenna specifications and subtract out any cable/connector loss.
- Permit - List of channel widths, center frequencies, and Tx powers that Auto Everything would choose in order of preference (if enabled).
- TC - Set the gain according to antenna specifications and subtract out any cable/connector loss.
- DSCP - List of channel widths, center frequencies, and Tx powers that Auto Everything would choose in order of preference (if enabled).

Access Control List

[+ Add a New Rule](#) Use the Access Control List to specify which ports, MAC addresses, and IP address combinations are permitted to access and use this device.

Unique Name	Direction	Match Type	Source Address	Source Address Mask	Dest. Address	Dest. Mask	Protocol	Permit	TC	DSCP
Block Mgt Traffic	Inbound	IP	192.168.1.1	255.255.255.255	59.50.1.0	255.255.255.0		Deny	N/A	N/A
Remark FTP	Outbound	IP	192.168.1.1	255.255.255.255	192.168.1.1	255.255.255.255	20	Allow	1	16

Managing Traffic Shaping Plans

Traffic Shaping plans allow precise control over rate limiting and rate shaping for client traffic. The topmost summary portion of the Traffic Shaping Plan page shows a snapshot of the number of fixed client assigned a traffic shaping plan. The Aggregate Downlink Commit (Mbps) and Aggregate Uplink commit is a sum from all the fixed clients Downlink Commit and Uplink Commit bandwidth where plans assigned. By default a new fixed client that connects to a Fixed Client SSID will be assigned a default plan. The Aggregate view provides a quick overview of the level of oversubscription on the access point.



Traffic Shaping Plans are used to control the maximum rate limit and committed rate shaping for each fixed client.

By default a new fixed client that connects to a Fixed Client SSID will be assigned a default plan. New plans can be created by clicking the + icon on the upper right portion of the panel. Plans can be removed by clicking the blue trash icon next to the plan name. Note, a plan that has subscribed clients cannot be removed. You must first remove all the fixed clients from the traffic shaping plan.

- Name - The name of the rate shapign plan.
- Downlink Max (Mbps) - This value controls the rate limit, or maximum Mbps a client can download.
- Downlink Max (Mbps) - This value controls the rate limit, or maximum Mbps a client can download.
- Downlink Commit (Mbps) - This value controls the rate shaping for the fixed client. During times of throughput contention the access point will attempt to maintain the Mbps download rate for the client. Other upload traffic above the commit will be de-prioritized. This allows a minimum download throughput to be maintained per client during times of excess demand on the access point.
- Uplink Max (Mbps) - This value controls the rate limit, or maximum Mbps a client can upload.
- Uplink Commit (Mbps) - This value controls the rate shaping for the fixed client. During times of throughput contention the access point will attempt to maintain the Mbps upload rate for the client. Other upload traffic above the commit will be de-prioritized. This allows a minimum upload throughput to be maintained per client during times of excess demand on the access point.
- Clients - This field indicates how many clients are currently assigned to the traffic shaping plan.



Traffic Shaping Plans +

Editing an existing Traffic Shaping Plan may impact its existing subscribers. A plan's name cannot be changed unless there are no connected clients.

Name	Downlink Max (Mbps)	Downlink Commit (Mbps)	Uplink Max (Mbps)	Uplink Commit (Mbps)	Clients	
default	200	150	50	30	0	
test	1000	1000	1000	1000	1	

The Fixed Clients table identifies which fixed clients are assigned to a rate shaping plan. Fixed clients can be manually added by clicking the + icon on the upper right of the panel and removed by clicking on the blue trash icon.

- Friendly Name - The name of the fixed client. This is automatically learned for Mimosa CPE devices.
- Brand - The manufacturer of the CPE device. This is automatically learned for Mimosa CPE devices.
- Model - The model number of the CPE device. This is automatically learned for Mimosa CPE devices.
- MAC - The MAC address of the CPE device.
- SSID - The SSID the fixed client is connected to.
- Plan - The traffic shaping plan assigned to the fixed client.

Fixed Clients						+ 
Friendly Name	Brand	Model	MAC	SSID	Plan	
<input type="text" value="sub_name"/>	<input type="text" value="mimosa"/>	<input type="text" value="c5"/>	<input type="text" value="20:b5:c6:00:8f:c1"/>	<input type="text" value="SystemTestP"/>	<input type="text" value="test"/> 	

Setting a Device Name and Session Timeout

The device name and description are local identifiers for administrative purposes, and are not used as part of the wireless link.

- Device Friendly Name - Name for the local device displayed on the Dashboard.
- Session Management - Setting the Session Timeout controls when the login session will be automatically logged out. Setting to 0 will never logout the management session.

Naming

Device Friendly Name

Session Management

Session Timeout

Time in minutes. 0 is infinite. 60 minutes max.

Setting a Password

Enter the new password in both the New Password and Verify New Password input boxes to validate that they were typed correctly. To finalize the change, enter the existing password and then save. By default, the password is "mimosa", and it should be changed during device configuration to protect your network.

- New Password - Enter the new password.
- Verify New Password - Re-enter the new password (to confirm).
- Current Configure Password - Enter the existing password (as a security measure).

The Password rules are as follows for choosing a password:

- It must be between 6 to 64 characters.
- It can use capital (A-Z) or lower case (a-z) characters, excluding space.
- Valid special characters for the password include ! " # \$ % & ' () * + , - . / : ; < = > ? [] ^ _ ` { | } ~
- The password cannot be blank.
- The password may not have a leading or trailing space.
- There is no complexity required for the password.

Set Password

New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
To change password, you must enter your current password below:	
Current Password	<input type="text"/>

Setting the Management IP Address

The Management IP panel contains controls for setting the device's network address, subnet, gateway and DNS servers.

- IP Mode - Select the preferred mode of network addressing: Static or DHCP+Static Failover. If Static is chosen, the device will always use the IP address that has been assigned. If DHCP+Static Failover is chosen, and a DHCP server is available, then the addresses are automatically assigned by the DHCP server. If a DHCP server is unavailable, the device will use the static IP address listed below.
- IP Address - The network address used to manage the device.
- Netmask - The subnet mask that defines the network subnet.
- Gateway - The gateway address for the subnet.
- Primary DNS - The first DNS server IP Address. Default is 8.8.8.8.
- Secondary DNS - The backup DNS server IP Address. Default is 8.8.4.4.



Note that the wired Ethernet interface is configured by default to use DHCP with a static failover to the IP address in the table below.

Management IP ⓘ

IP Mode	Static
IP Address Current: 184.105.87.18	192.168.1.20
Netmask Current: 255.255.255.240	255.255.255.0
Gateway Current: 184.105.87.17	192.168.1.1
Primary DNS Current: 8.8.8.8	8.8.8.8
Secondary DNS Current: 8.8.4.4	8.8.4.4

VLAN Management

The VLAN Management panel allows the administrator to enable a VLAN (Virtual Local Area Network) for management traffic. When a value is entered, all Web Management traffic must originate from a device on that VLAN.

- ID - The VLAN ID tag.

You can still connect locally via the 2.4 GHz management console on a A5.

Management VLAN

VLAN ID	<input type="text"/>
---------	----------------------

Performing a Firmware Update

The Firmware Update panel displays the current firmware version and date, and allows the user to upload a new firmware image. The latest firmware image may be downloaded from help.mimosa.co. Alternately, firmware can be pushed to the device automatically through the Manage application at manage.mimosa.co.

- Installed Version - The currently installed firmware version.
- Update Firmware - Update to the latest firmware. Click the Browse File button to select a file for upload the file.



When performing a Firmware upgrade, it is advisable to reboot and then upgrade the remote side of the link before the local side. If there is a problem during the upgrade you will still have access to one of the radios within the link and can manage the link details.

The firmware update process occurs in four phases:

1. Upload - Selecting a firmware image and uploading to the radio
2. Verification - Ensuring that the firmware image is complete and without errors
3. Upgrade - Writing the new firmware image to flash memory
4. Reboot - Restarting with the new firmware image (~90 seconds)

Once the remote radio enters the Upgrade phase, it is generally safe to begin the Upload phase to the local radio. Alternately, the Mimosa Manage application offers a parallel upgrade feature which sends the firmware image to both radios, and once both radios receive and verify the image, they upgrade at the same time and reboot in an order that you specify.

Reset & Reboot the Device

Reboot the device or reset it to its original factory settings.

- Factory Reset Device - Clears all configuration settings and locks the device. **WARNING:** This will delete ALL saved configuration settings and return the device to the locked factory state. You will be required to re-enter your unlock key upon device reset. The current version of firmware will remain, however.
- Reset Device Configuration - Clears all configuration settings. The device will remain unlocked.
- Reset Device Unlock - Locks the device and resets the country code. **WARNING:** You will be required to re-enter your unlock key upon reset.
- Reboot Device - Restarts the device.

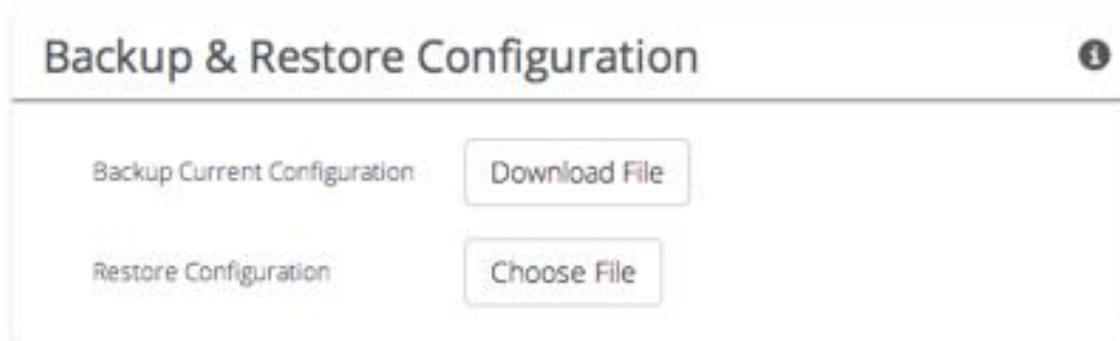
Reset & Reboot

Factory Reset Device	<input type="button" value="Reset"/>
Reset Device Configuration	<input type="button" value="Reset Configuration"/>
Reset Device Unlock	<input type="button" value="Reset Unlock"/>
Reboot Device	<input type="button" value="Reboot"/>

Backup or Restore Configuration Settings

The Backup and Restore Configuration panel contains controls for managing configuration settings files.

- Backup Current Configuration - Perform a configuration backup by downloading the mimosa.conf file.
- Restore Configuration - Click the Choose File button to upload a previously saved mimosa.conf file.



Diagnostic Logs

View Events and download diagnostic information to share with Mimosa Support.

- Logging - This is a persistent (non-volatile) log of all significant events that occur.
- Support Info - Download a single file containing all information required by Mimosa Support to help with troubleshooting.

Logging

Support Info

```
Jan 1 12:00:07 : Startup reason: Console reboot command
2015-01-01 12:00:07 (UTC +0000) (none) user.notice root: System was upgraded
2015-01-01 12:00:45 (UTC +0000) (none) user.notice BBIC: [ 28.915000] SystemTestP: 20:b5:c6:00:8f:c1 associated, tot=1/0
2015-01-01 12:00:50 (UTC +0000) (none) user.notice BBIC: [ 33.535000] SystemTestP: 20:b5:c6:00:8f:c1 disassociated, tot=0/0
2015-11-04 23:35:02 (UTC +0000) (none) user.notice BBIC: [ 51.635000] SystemTestP: 20:b5:c6:00:8f:c1 associated, tot=1/0
```

Logging

Support Info

Customer Support

Download the support file and send it to Mimosa if requested. This file is encrypted and can only be read by Mimosa.

Download

Diagnostic Tests

Three types of tests are available within the Diagnostics section: Ping, Bandwidth and Traceroute.

Ping Test

A low level ICMP test which indicates whether the target host is reachable from the local device.

- Destination Host - The destination IP Address of the device to ping.
- Packet Count - The number of packets to transmit during a ping.
- Packet Size - The size of each packet to transmit during a ping.
- Run Test - Click on the Run Test button to ping the destination IP address. Results are shown in the corresponding table.

Traceroute Test

A network utility used to display the path and transit delay between the local device and a given destination across an IP network.

- Destination Host - The destination IP address for traceroute to send packets.
- Resolve IP Address - Indicate whether the system should resolve and print the host name of the destination.
- Max Number of Hops - Choose the maximum number of intermediate devices (e.g. routers) through which packets must pass between source and destination.
- Run Test - Click on the Run Test button to begin the traceroute test. Results are shown in the corresponding table.

Running a Ping Test

A low level ICMP test which indicates whether the target host is reachable from the local device.

- Destination Host - The destination IP Address of the device to ping.
- Packet Count - The number of packets to transmit during a ping.
- Packet Size - The size of each packet to transmit during a ping.
- Run Test - Click on the Run Test button to ping the destination IP address. Results are shown in corresponding table.

The screenshot shows a web interface for running a ping test. It features two tabs: 'Ping' (selected) and 'Traceroute'. Below the tabs, there are three input fields: 'Destination Host' (highlighted with a red border), 'Packet Count' (set to 5), and 'Packet Size' (set to 64). At the bottom, there is a 'Run Test' button with a play icon.

Running a Traceroute Test

A network utility used to display the path and transit delay between the local device and a given destination across an IP network.

- Destination Host - The destination IP address for traceroute to send packets.



The screenshot shows a web-based interface for running network tests. At the top, there are two tabs: "Ping" and "Traceroute", with "Traceroute" being the active tab. Below the tabs, there is a label "Destination Host" followed by an empty text input field. Below the input field is a button labeled "Run Test" with a circular arrow icon to its left.

SNMP OID Reference

Many SNMP implementations simply provide a MIB which requires a fair amount of study to locate specific values. We took it a step further and summarized them below for easy reference. Each table shows what values are available and where to find them within the GUI for comparison.

General Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.1.1.0	mimosaDeviceName.0	STRING: My A5 AP	Preferences > General > Naming > Device Friendly Name
1.3.6.1.4.1.43356.2.1.2.1.2.0	mimosaSerialNumber.0	STRING: 1000123456	Overview > Dashboard > Device Details > Serial Number (Local)
1.3.6.1.4.1.43356.2.1.2.1.3.0	mimosaFirmwareVersion.0	STRING: 1.2.0	Overview > Dashboard > Device Details > Firmware (Local)
1.3.6.1.4.1.43356.2.1.2.1.4.0	mimosaFirmwareBuildDate.0	STRING: 2015-04-17 18:29:26 (UTC -0700)	Preferences > Firmware & Reset > Firmware Update > Build Date
1.3.6.1.4.1.43356.2.1.2.1.5.0	mimosaLastRebootTime.0	STRING: 2015-04-18 19:54:42 (UTC +0000)	Overview > Dashboard > Device Details > Last Reboot (Local)
1.3.6.1.4.1.43356.2.1.2.1.6.0	mimosaUnlockCode.0	STRING: 8MEDWLWMN	Preferences > General > Miscellaneous > Unlock Code
1.3.6.1.4.1.43356.2.1.2.1.7.0	mimosaLEDBrightness.0	INTEGER: auto(1)	Preferences > General > Miscellaneous > LED Brightness
1.3.6.1.4.1.43356.2.1.2.1.8.0	mimosaInternalTemp.0	INTEGER: 38.2 C	Overview > Dashboard > Device Details > Internal Temp or CPU Temp (Local)
1.3.6.1.4.1.43356.2.1.2.1.9.0	mimosaRegulatoryDomain.0	STRING: United States	Wireless > Channel & Power > Exclusions & Restrictions > Regulatory Domain

TDMA Settings

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.4.1.0	mimosaWirelessMode.0	INTEGER: ap(1)	Wireless > Link > TDMA Configuration > Wireless Mode
1.3.6.1.4.1.43356.2.1.2.4.2.0	mimosaWirelessProtocol.0	INTEGER: tdma(1)	Wireless > Link > TDMA Configuration > Wireless Protocol
1.3.6.1.4.1.43356.2.1.2.4.3.0	mimosaTDMAMode.0	INTEGER: A(1)	Wireless > Link > TDMA Configuration > Gender - Traffic Split
1.3.6.1.4.1.43356.2.1.2.4.4.0	mimosaTDMAWindow.0	INTEGER: 4 ms	Wireless > Link > TDMA Configuration > TDMA Window
1.3.6.1.4.1.43356.2.1.2.4.5.0	mimosaTrafficSplit.0	INTEGER: symmetric(1)	Wireless > Link > TDMA Configuration > Gender - Traffic Split

Radio Information

SSID Table

OID	Object	Output Example	UI Location
TBD	mimosaSsidTable	Formatted Table	Wireless > Link > SSID Management
TBD	mimosaSsidName.1	STRING: 5G_SSID	Wireless > Link > SSID Management > Name
TBD	mimosaSsidBand.1	INTEGER: 80 MHz	Wireless > Link > SSID Management > Band
TBD	mimosaSsidType.1	INTEGER: hotspot(2)	Wireless > Link > SSID Management > Type
TBD	mimosaSsidEnabled.1	INTEGER: enabled(1)	Wireless > Link > SSID Management > Enabled
TBD	mimosaSsidBroadcast.1	INTEGER: enabled(1)	Wireless > Link > SSID Management > Broadcast
TBD	mimosaSsidIntraBssTraffic.1	INTEGER: enabled(1)	Wireless > Link > SSID Management > Intra-BSS Traffic

Channel & Power Settings

OID	Object	Output Example	UI Location
TBD	mimosaApMode.1	INTEGER: ac(3)	Wireless > Channel & Power > Channel & Power Settings > 5 GHz > 802.11 Mode
TBD	mimosaApChannelWidth.1	INTEGER: 80 MHz	Wireless > Channel & Power > Channel & Power Settings > 5 GHz > Channel Width (MHz)
TBD	mimosaApChannelTxPower.1	INTEGER: 4.0 dBm	Wireless > Channel & Power > Channel & Power Settings > 5 GHz > Tx Power (dBm)
TBD	mimosaApChannelCenterFreq.1	INTEGER: 5500 MHz	Wireless > Channel & Power > Channel & Power Settings > 5 GHz > Center Frequency (MHz)
TBD	mimosaApMode.2	INTEGER: ng(1)	Wireless > Channel & Power > Channel & Power Settings > 2.4 GHz > 802.11 Mode
TBD	mimosaApChannelWidth.2	INTEGER: 20 MHz	Wireless > Channel & Power > Channel & Power Settings > 2.4 GHz > Channel Width (MHz)
TBD	mimosaApChannelTxPower.2	INTEGER: 4.0 dBm	Wireless > Channel & Power > Channel & Power Settings > 2.4 GHz > Tx Power (dBm)
TBD	mimosaApChannelCenterFreq.2	INTEGER: 2412 MHz	Wireless > Channel & Power > Channel & Power Settings > 2.4 GHz > Center Frequency (MHz)

Location Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.2.1.0	mimosaLongitude.0	INTEGER: -121.943684	Wireless > Location > Location Data > Latitude (Local)
1.3.6.1.4.1.43356.2.1.2.2.2.0	mimosaLatitude.0	INTEGER: 37.28529	Wireless > Location > Location Data > Longitude (Local)

1.3.6.1.4.1.43356.2.1.2.2.3.0	mimosaAltitude.0	INTEGER: 65 meters	Wireless > Location > Location Data > Altitude (Local)
1.3.6.1.4.1.43356.2.1.2.2.4.0	mimosaSatelliteSNR.0	INTEGER: 38.0 dB	Wireless > Location > Satellite Information > Satellite Avg SNR
1.3.6.1.4.1.43356.2.1.2.2.5.0	mimosaSatelliteStrength.0	INTEGER: good(1)	Wireless > Location > Satellite Information > Satellite Signal Strength
1.3.6.1.4.1.43356.2.1.2.2.6.0	mimosaGPSSatellites.0	INTEGER: 11	Wireless > Location > Satellite Information > Total Satellites > GPS
1.3.6.1.4.1.43356.2.1.2.2.7.0	mimosaGlonassSatellites.0	INTEGER: 8	Wireless > Location > Satellite Information > Total Satellites > GLONASS
1.3.6.1.4.1.43356.2.1.2.2.8.0	mimosaClockAccuracy.0	INTEGER: 1.56 PPB	Wireless > Location > Satellite Information > Clock Accuracy

Subscriber Plans Table

OID	Object	Output Example	UI Location
TBD	mimosaSubscriberPlans	Formatted Table	Management > Subscriber Plans
TBD	mimosaSubPlanName.0	STRING: Plan A	Management > Subscriber Plans > Name
TBD	mimosaSubPlanDownPeak.0	INTEGER: 100 Mbps	Management > Subscriber Plans > DL Peak
TBD	mimosaSubPlanDownCommitl.0	INTEGER: 75 Mbps	Management > Subscriber Plans > DL Commitment
TBD	mimosaSubPlanUpPeak.0	INTEGER: 100 Mbps	Management > Subscriber Plans > UL Peak
TBD	mimosaSubPlanUpCommit.0	INTEGER: 75 Mbps	Management > Subscriber Plans > UL Commitment

Subscribers Table

OID	Object	Output Example	UI Location
TBD	mimosaSubscribers	Formatted Table	Management > Subscribers
TBD	mimosaSubName.0	STRING: John Doe	Management > Subscribers > Friendly Name
TBD	mimosaSubBrand.0	STRING: Mimosa	Management > Subscribers > Brand
TBD	mimosaSubModel.0	STRING: C5	Management > Subscribers > Model
TBD	mimosaSubMac.0	Hex-STRING: 20 B5 C6 00 00 01	Management > Subscribers > MAC
TBD	mimosaSubPlan.0	STRING: Plan A	Management > Subscribers > Plan

Client Table

OID	Object	Output Example	UI Location
Copyright © 2015 Mimosa			
Page 38			

TBD	mimosaClients	Formatted Table	Management > Clients
TBD	mimosaClientName.0	STRING: John Doe	Management > Clients > Client List > Name
TBD	mimosaClientType.0	INTEGER: fixed(1)	Management > Clients > Client List > Type
TBD	mimosaClientIP.0	IpAddress: 192.168.0.2	Management > Clients > Client List > IP
TBD	mimosaClientMac.0	Hex-STRING: 20 B5 C6 00 00 01	Management > Clients > MAC
TBD	mimosaClientTxPower.0	INTEGER: 10.0 dBm	Management > Clients > Client List > Tx Power
TBD	mimosaClientTxPower.1	INTEGER: 10.0 dBm	Management > Clients > Client List > Tx Power > Chain 1
TBD	mimosaClientTxPower.2	INTEGER: 10.0 dBm	Management > Clients > Client List > Tx Power > Chain 2
TBD	mimosaClientRxPower.0	INTEGER: -75.0 dBm	Management > Clients > Client List > Rx Power
TBD	mimosaClientRxPower.1	INTEGER: -75.0 dBm	Management > Clients > Client List > Rx Power > Chain 1
TBD	mimosaClientRxPower.2	INTEGER: -75.0 dBm	Management > Clients > Client List > Rx Power > Chain 2
TBD	mimosaClientRxNoise.0	INTEGER: -95.0 dBm	Management > Clients > Client List > Rx Noise
TBD	mimosaClientRxNoise.1	INTEGER: -95.0 dBm	Management > Clients > Client List > Rx Noise > Chain 1
TBD	mimosaClientRxNoise.2	INTEGER: -95.0 dBm	Management > Clients > Client List > Rx Noise > Chain 2
TBD	mimosaClientSNR.0	INTEGER: 20.0 dB	Management > Clients > Client List > SNR
TBD	mimosaClientSNR.1	INTEGER: 20.0 dB	Management > Clients > Client List > SNR > Chain 1
TBD	mimosaClientSNR.2	INTEGER: 20.0 dB	Management > Clients > Client List > SNR > Chain 2
TBD	mimosaClientTxChannelWidth.0	INTEGER: 80 MHz	Management > Clients > Client List > Channel Width
TBD	mimosaClientTxChannelWidth.1	INTEGER: 80 MHz	Management > Clients > Client List > Channel Width > Stream 1
TBD	mimosaClientTxChannelWidth.2	INTEGER: 80 MHz	Management > Clients > Client List > Channel Width > Stream 2
TBD	mimosaClientRxChannelWidth.0	INTEGER: 80 MHz	Management > Clients > Client List > Rx Channel Width
TBD	mimosaClientRxChannelWidth.1	INTEGER: 80 MHz	Management > Clients > Client List > Rx Channel Width > Stream 1
TBD	mimosaClientRxChannelWidth.2	INTEGER: 80 MHz	Management > Clients > Client List > Rx Channel Width > Stream 2
TBD	mimosaClientTxPhy.1	INTEGER: 100 Mbps	Management > Clients > Client List > Tx PHY > Stream 1
TBD	mimosaClientTxPhy.2	INTEGER: 100 Mbps	Management > Clients > Client List > Tx PHY > Stream 2
TBD	mimosaClientTxMCS.1	INTEGER: 8	Management > Clients > Client List > Tx MCS > Stream 1
TBD	mimosaClientTxMCS.2	INTEGER: 8	Management > Clients > Client List > Tx MCS > Stream 2
TBD	mimosaClientTxEVM.1	INTEGER: -25 dB	Management > Clients > Client List > Tx EVM > Stream 1
TBD	mimosaClientTxEVM.2	INTEGER: -25 dB	Management > Clients > Client List > Tx EVM > Stream 2
TBD	mimosaClientTxPER.0	INTEGER: .25 %	Management > Clients > Client List > Tx PER
TBD	mimosaClientRxPhy.1	INTEGER: 100 Mbps	Management > Clients > Client List > Rx PHY > Stream 1

TBD	mimosaClientRxPhy.2	INTEGER: 100 Mbps	Management > Clients > Client List > Rx PHY > Stream 2
TBD	mimosaClientRxMCS.1	INTEGER: 8	Management > Clients > Client List > Rx MCS > Stream 1
TBD	mimosaClientRxMCS.2	INTEGER: 8	Management > Clients > Client List > Rx MCS > Stream 2
TBD	mimosaClientRxEVM.1	INTEGER: -25 dB	Management > Clients > Client List > Rx EVM > Stream 1
TBD	mimosaClientRxEVM.2	INTEGER: -25 dB	Management > Clients > Client List > Rx EVM > Stream 2
TBD	mimosaClientRxPER.0	INTEGER: .25 %	Management > Clients > Client List > Rx PER
TBD	mimosaClientVlanId.0	INTEGER: 1	Management > Clients > Client List > VLAN ID
TBD	mimosaClientTimeConnected.0	STRING: 2015-04-18 19:54:42 (UTC +0000)	Management > Clients > Client List

WAN Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.3.2.0	mimosaWanMac.0	Hex-STRING: 20 B5 C6 00 00 01	Overview > Dashboard > Device Details > 5 GHz MAC (Local)
1.3.6.1.4.1.43356.2.1.2.3.3.0	mimosaWanStatus.0	INTEGER: connected(1)	Overview > Dashboard > Wireless Status
1.3.6.1.4.1.43356.2.1.2.3.4.0	mimosaWanUpTime.0	Timeticks: (18571300) 2 days, 3:35:13.00	Overview > Dashboard > Link Uptime

Performance Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.7.1.0	mimosaPhyTxRate.0	INTEGER: 940.81 kbps	Overview > Dashboard > Performance > Throughput > Tx
1.3.6.1.4.1.43356.2.1.2.7.2.0	mimosaPhyRxRate.0	INTEGER: 764.06 kbps	Overview > Dashboard > Performance > Throughput > Rx
1.3.6.1.4.1.43356.2.1.2.7.3.0	mimosaPerTxRate.0	INTEGER: .27 %	Overview > Dashboard > Performance > PER > Tx
1.3.6.1.4.1.43356.2.1.2.7.4.0	mimosaPerRxRate.0	INTEGER: .73 %	Overview > Dashboard > Performance > PER > Rx

Management Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.5.2.0	mimosaRecoverySsid.0	STRING: mimosaR456	Not Shown on UI (fixed at factory)
1.3.6.1.4.1.43356.2.1.2.5.8.0	mimosaLocalIpAddr.0	IpAddress: 192.168.1.20	Preferences > Management > Management IP > IP Address

1.3.6.1.4.1.43356.2.1.2.5.9.0	mimosaLocalNetMask.0	IpAddress: 255.255.255.0	Preferences > Management > Management IP > Netmask
1.3.6.1.4.1.43356.2.1.2.5.10.0	mimosaLocalGateway.0	IpAddress: 192.168.1.1	Preferences > Management > Management IP > Gateway
1.3.6.1.4.1.43356.2.1.2.5.11.0	mimosaFlowControl.0	INTEGER: disabled(2)	Preferences > Management > Miscellaneous > Flow Control

Services Information

OID	Object	Output Example	UI Location
1.3.6.1.4.1.43356.2.1.2.8.1.0	mimosaHttpsEnabled.0	INTEGER: disabled(2)	Preferences > Management > Services > Enable HTTPS
1.3.6.1.4.1.43356.2.1.2.8.2.0	mimosaMgmtVlanEnabled.0	INTEGER: disabled(2)	Preferences > Management > Management VLAN > Enable
1.3.6.1.4.1.43356.2.1.2.8.3.0	mimosaMgmtCloudEnabled.0	INTEGER: enabled(1)	Preferences > Management > Miscellaneous > Mimosa Cloud Management
1.3.6.1.4.1.43356.2.1.2.8.4.0	mimosaRestMgmtEnabled.0	INTEGER: enabled(1)	Preferences > Management > REST Services > REST Management
1.3.6.1.4.1.43356.2.1.2.8.5.0	mimosaPingWatchdogEnabled.0	INTEGER: disabled(2)	Preferences > Management > Watchdog > IP Ping Watchdog
1.3.6.1.4.1.43356.2.1.2.8.6.0	mimosaSyslogEnabled.0	INTEGER: disabled(2)	Preferences > Notifications > System Log Notifications > Syslog Remote Log
1.3.6.1.4.1.43356.2.1.2.8.7.0	mimosaNtpMode.0	INTEGER: standard(2)	Preferences > General > Time > NTP Mode
1.3.6.1.4.1.43356.2.1.2.8.8.0	mimosaNtpServer.0	STRING: time.nist.gov	Preferences > General > Time > NTP Server

Related:

[SNMP Usage Examples: Get / Walk / Table - Sample commands for retrieving values](#)

[SNMP Object Names - Query values using SNMP Object Names defined within the Mimosa MIB file](#)

[SNMP Notifications - Enabling SNMP on Mimosa Backhaul products](#)

[SNMP Traps - Configure outgoing notifications for specific events](#)

[SNMP MIB Download - Available values in standard Management Information Base \(MIB\) format](#)

RF Exposure Warning

The radiated output power of this device is below the FCC radio frequency exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during the normal operation is minimized. In order to avoid the possibility of exceeding the FCC radio frequency exposure limit, human proximity to the access point should be more than 20 cm.