

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 two ways to facilitate set-up and management.

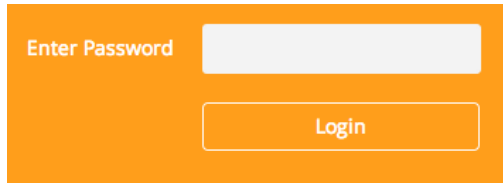
1. Through the local Ethernet interface (LAN)
2. Remotely through the 5 GHz wireless link

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 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 the Mimosa Device Discovery tool. The default password for the device is "mimosa". 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.



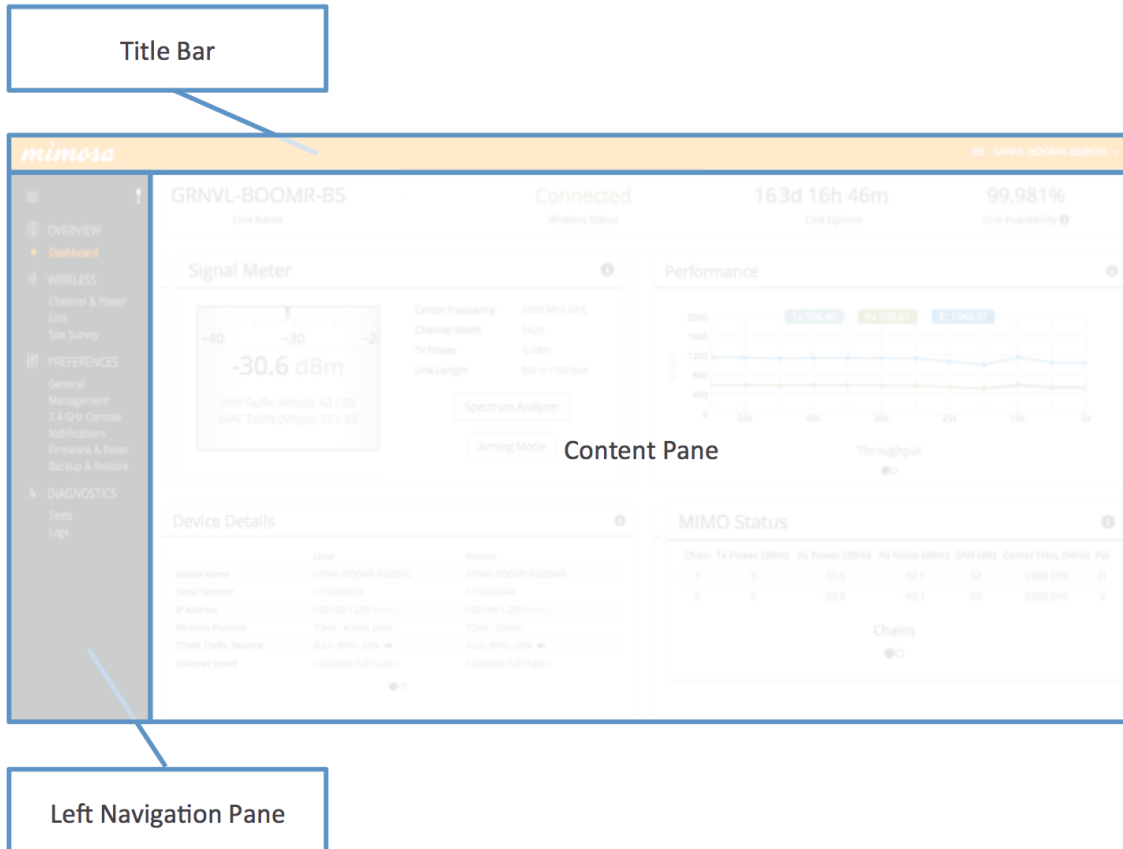
Enter Password

Login

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

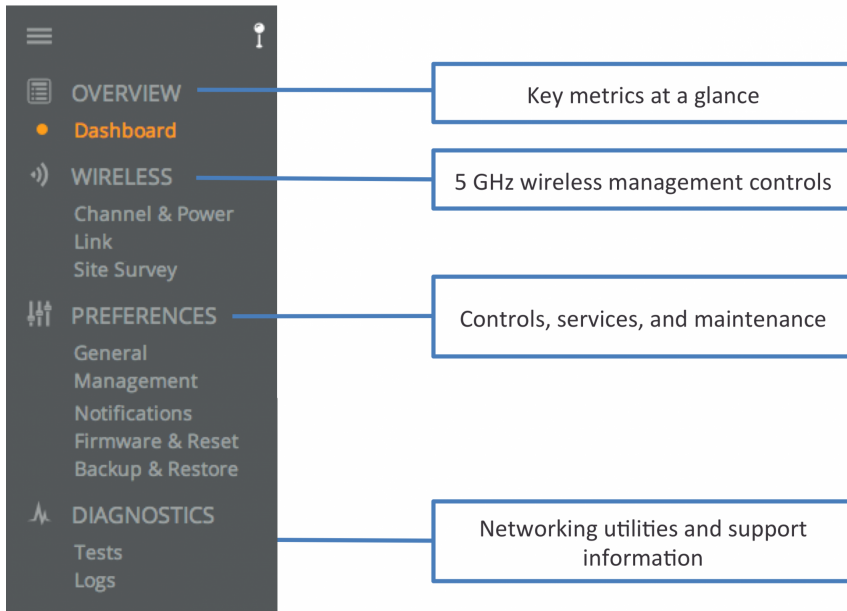
User Interface Overview

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.



The Dashboard

The Dashboard contains several panels used to group related items. The status panel at the top of the page shows the link SSID, the 5 GHz link status, GPS signal quality, Link Uptime, and Link Availability since the last reboot. Two of the values on this panel contain an information icon that shows more information when you click or hover over it with your mouse cursor. On other panels, detailed help text can be found by clicking on the information icon in the upper right hand corner.

The screenshot shows the Mimosa dashboard interface. A callout box labeled "Current wireless connection status" points to the top status bar which displays "GRNVL-BOOMR-B5", "Connected", "16 3d 16h 46m", and "99.981%". Another callout box labeled "Estimated half-duplex IP throughput in Mbps (TCP based)" points to the "Signal Meter" section, which shows a signal level of "-52.0 dBm" and a throughput of "1300 / 1300 Tbits Per Mbps". A third callout box labeled "Device and Link information" points to the "Device Details" table. A fourth callout box labeled "Provides a real time signal level in dBm for the established link" points to the "Performance" section, which includes a line graph showing Tx and Rx throughput over time.

Current wireless connection status

Estimated half-duplex IP throughput in Mbps (TCP based)

Device and Link information

Provides a real time signal level in dBm for the established link

Reading the Signal Meter

Connected Link

Received signal strength is shown in large text in the center of the control, and as a green indicator in the top dial. The blue shaded bar and text immediately below the dial represent target signal strength based on distance and other information exchanged between radios. The objective is to align the green indicator with the blue bar as a guideline during antenna aiming.

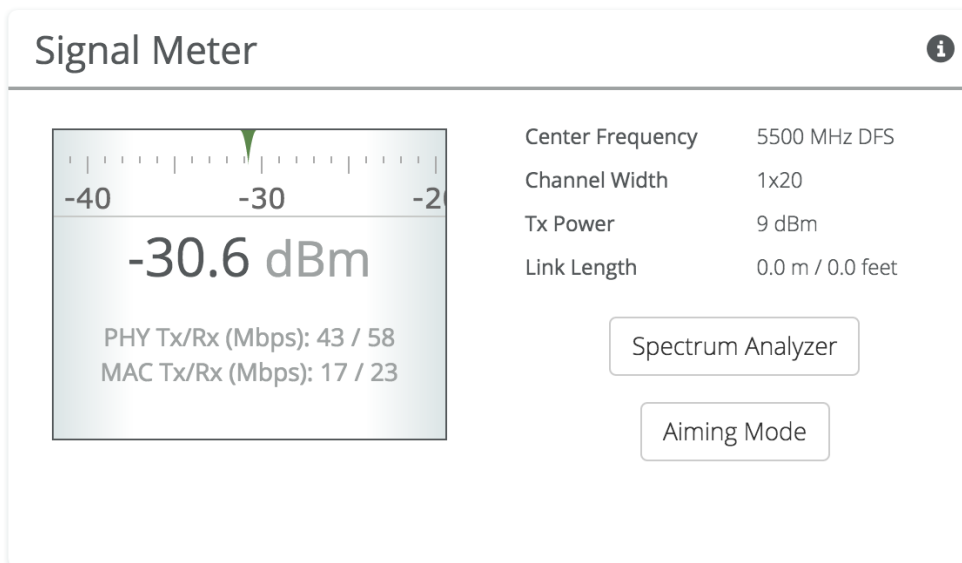
The resulting half-duplex PHY rates shown at the bottom of the Signal Meter control are correlated with the MCS, and represent raw data across the link without protocol overhead. The Max Throughput values include TDMA window size and MAC layer efficiency.

The following settings and values that affect link health are listed for reference:

- Center Frequency: True center of the frequency range (no offset).
- Channel Width: The width of the channel (20, 40 or 80 MHz).
- Tx Power: Total transmit power level (dBm).
- Link Length: Distance between local and remote radios (when connected).

Click the Spectrum Analyzer button to access the Spectrum Analyzer, which can also be found on the Channel & Power page. This will not disturb the link.

When a link is not associated, the signal strength and PHY rates are replaced by an indicator of "Disconnected".



Aiming Mode

Once associated, the Aiming Mode button is shown. Aiming Mode opens a new window that refreshes once per

second for a 5-minute period. The Aim Heading indicates the direction in which the front of the device should be pointed based exchange of coordinates.

U-NII-1 Elevation Requirements

When mounting the Mimosa C5-Client radio, in accordance with the UNII-1 band requirements, neither dish should exceed 30 degrees in elevation.

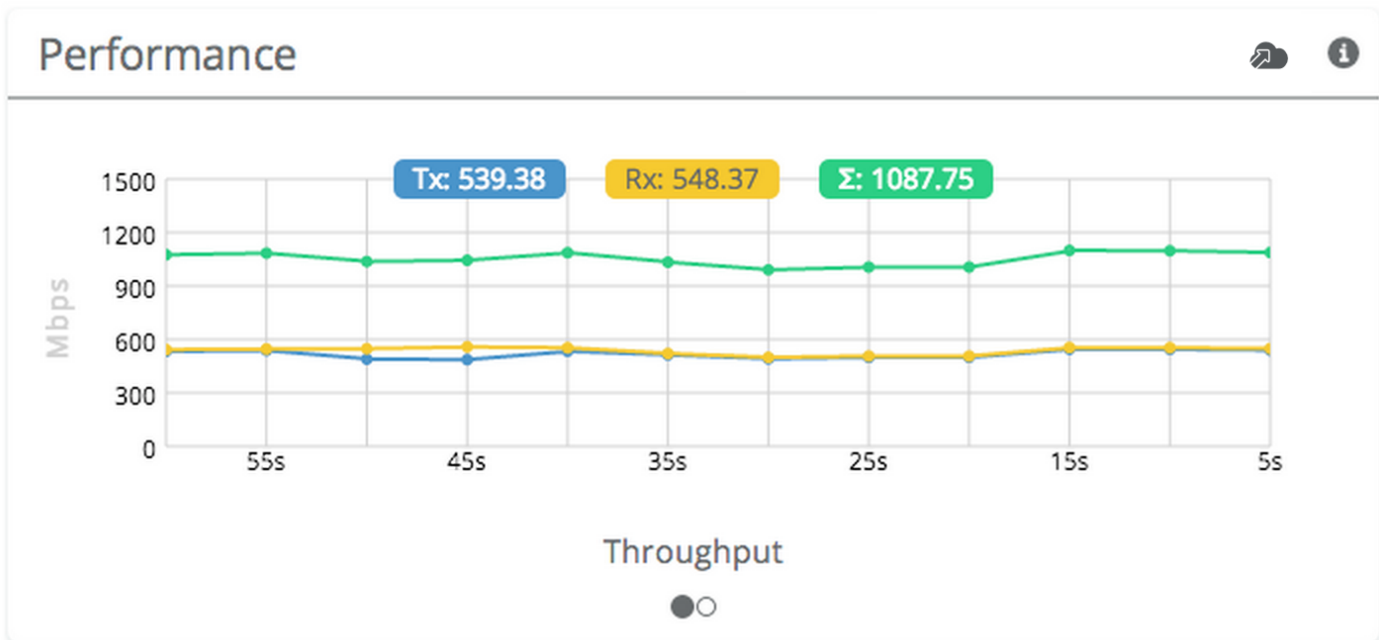
Reading the Performance Table

IP Throughput and Packet Error Rate are charted over 60 seconds in 5-second intervals. The newest data shows up on the right and scrolls to the left over time.

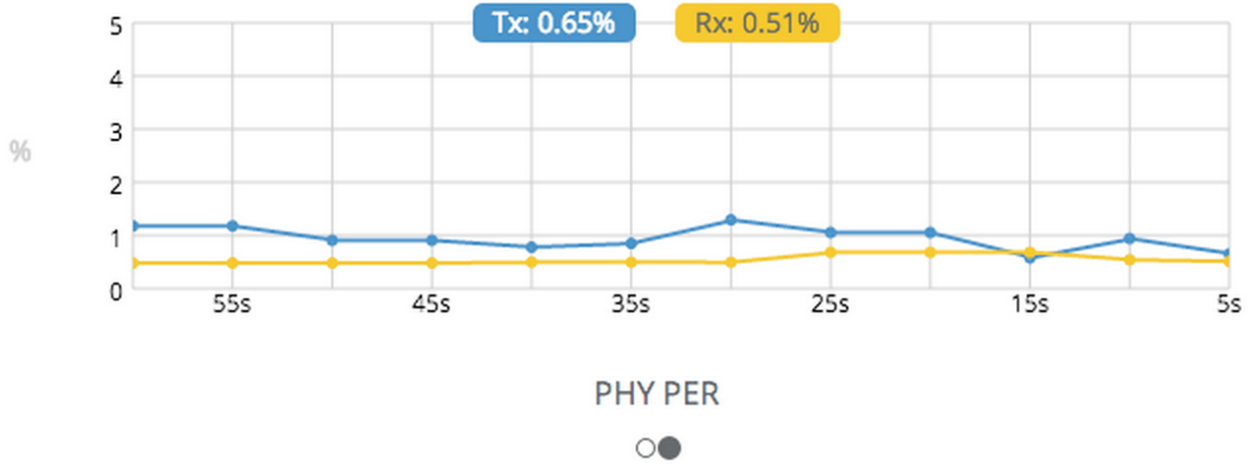
The IP Throughput graph plots three lines representing transmit, receive, and aggregate (summed) throughputs at the datagram (or packet) layer excluding any protocol or encapsulation overhead. The results here may differ from those measured using speed test tools, due to protocol overhead and encapsulation.

You can toggle between the charts by clicking on the navigation circles at the bottom of the panel. The PER chart shows the ratio of packets with errors to packets without errors for both transmit and receive PHY. Lower numbers are better, and higher numbers are an indication of interference.

If enabled, click on the cloud icon button to view historical data within the Manage application.



Performance



Reading Device Details

The Device Details panel shows two summary tables for the local and remote device configurations and their status.

Additional detail can be found by clicking on the navigation circles at the bottom of the panel.

The table shows the following for both Local and Remote devices:

- 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. (Set in *Wireless > Link > MAC Configuration*)
- TDMA Traffic Balance: Identifies the "gender" of the radio, the duration for each TDMA time slot, and ratio of bandwidth allocated for transmission. (Set in *Wireless > Link > MAC Configuration*)
- Ethernet Speed: Data rate and duplex mode of the wired Ethernet interface.
- Firmware: The latest firmware version applied to each device. (Set in *Preferences > Update & Reboot*)
- Internal Temp: The measured temperature inside the device.
- Ethernet MAC: The unique identifier for the physical Ethernet interface.
- Last Reboot: The date and time at which each device last rebooted.

Device Details i

	Local	Remote
Device Name	HE-CP-LINK at HE	HE-CP-LINK_at_CP
Serial Number	55000 [redacted]	101313 [redacted]
IP Address	[redacted] (Static)	[redacted] (Static)
Wireless Protocol	TDMA - Access point	TDMA - Station
TDMA Traffic Balance	A - 4ms - 50% →	B - 4ms - 50% ←
Ethernet Speed	1000Mb/s Full Duplex	1000Mb/s Full Duplex

● ○

Device Details i

	Local	Remote
Firmware	0.4.0-45	0.4.0-45
Internal Temp	42.1°C / 107.8°F	27°C / 80.6°F
Ethernet MAC	20:B5:C6:00:07:4F	20:B5:C6:00:04:DC
Last Reboot	2014-12-08 17:36:48 (UTC +0000)	2014-12-08 17:35:31 (UTC +0000)

○ ●

Reading MIMO Status Tables

The MIMO Status tables describe the Tx/Rx MIMO status: 2 RF chains and up to 2 data streams.

The Chains table describes each chain's power, noise, SNR, frequency and polarization.

The Streams table describes each stream's MCS index, PHY rates and Rx Error Vector Magnitude (EVM).

Each table can be found by clicking on the navigation circles at the bottom of the panel.

MIMO Status i

Chain	Tx Power (dBm)	Rx Power (dBm)	Rx Noise (dBm)	SNR (dB)	Center Freq. (MHz)	Pol
1	6	-35.5	-92.1	57	5500 DFS	H
2	6	-33.4	-92.1	59	5500 DFS	V

Chains

● ○

MIMO Status i

Stream	Tx MCS	Tx PHY (Mbps)	Rx MCS	Rx PHY (Mbps)	Rx EVM (dB)
1	4	43	2	21	-13.3
2	--	--	2	21	-13.3

Streams

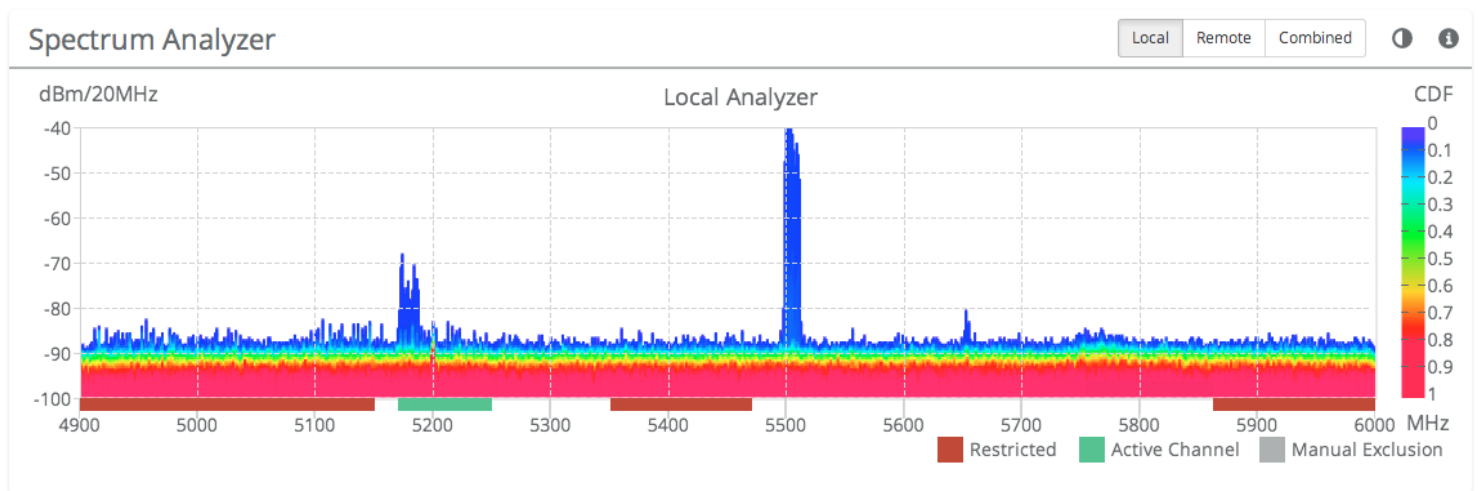
○ ●

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 by frequency, amplitude, and probability of recurrence. The display can be shown for the local radio, remote radio or a combination of both. Click on the half circle icon in the upper right to toggle the graph's background color between black and white. Click the Local, Remote, or Combined buttons to view spectrum individually or simultaneously. Please note that the remote side data may be as much as 5 minutes behind the local radio.

Channels that are already in use have “above average” amplitude 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 (closer to 1), while blue represents the lowest probability (closer to 0).

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.



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.

- Auto Everything - Automatically configure channel, channel width and power to optimize performance based on spectrum data.
- Channel Width (MHz) - Choose the width for each (20, 40, Or 80 MHz).
- Channel Center Frequency - 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.
- Power - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency. If Auto Everything is set to On, the Channel & power will be automatically set, and not editable.
- Antenna Gain (dBi) - Set the gain according to antenna specifications and subtract out any cable/connector loss. By default, this value is set to 25 dBi for the B5 and not shown.
- Channel Recommendations - List of channel widths, center frequencies, and Tx powers that Auto Everything would choose in order of preference (if enabled).

Channel & Power Settings i

Auto Everything	Off (Manual) ▾	Channel Width (MHz)	1x20 ▾
Center Frequency (MHz)	5500 (ch 100) DFS ▾	Tx Power (dBm)	-1 ▾

Channel Recommendations

Channel Width (MHz)	Frequency (MHz)	Tx Power (dBm)
2x80	5880	-1
2x80	5875	-1
2x80	5870	-1

Note: Tx power selections may be limited based on your regulatory domain (refer to the Maximum Power chart for more details).

Managing Exclusions & Restrictions


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

- Start - Specify the start of the frequency range to be excluded.
- End - Specify the end of the frequency range to be excluded.
- Add Exclusions - The button to add the Start and End frequency 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.





Exclusions & Restrictions

Add a New Exclusion (MHz)

Start Frequency End Frequency

 Add Exclusion

Existing Exclusions and Restrictions

4900 - 4940	
4990 - 5150	
5350 - 5470	
5850 - 6000	

Regulatory Domain United States Licensed

TDMA Configuration Settings

The TDMA Configuration panel contains controls for configuring and fine tuning TDMA performance. One side of the radio link must be set as an Access point, and the other set as a Station. The Station inherits the other settings from the AP, so the other fields are grayed out and not accessible when Station is selected.

- Wireless Mode - Choose whether the device will act as an Access Point or a Station.
- Wireless Protocol - TDMA is a deterministic protocol where each device is assigned a time slot during which it is allowed to transmit.
- Gender - Traffic Split - The radio can be configured to allocate bandwidth symmetrically (50/50) or biased towards downstream (75/25) in environments where traffic direction is expected to be heavier in one direction than the other. With an asymmetrical split, the local radio is represented first in the slash notation, (local/remote). For example, in the (75/25) split, the local radio gets 75, while the remote radio gets 25. If "Auto" is selected the radio will automatically determine, based upon traffic flow, which ratio will be used. The radio will continue to evaluate the flow and adjust accordingly.
- TDMA Window - Determines the length of the transmit time slot in milliseconds.

Example Access Point Settings

TDMA Configuration i

Wireless Mode	Access point
Wireless Protocol	TDMA
Gender - Traffic Split	A - 50/50
TDMA Window	4 ms

Example Station Settings

TDMA Configuration



Wireless Mode	Station
Wireless Protocol	TDMA
Gender - Traffic Split	B - 50/50
TDMA Window	4ms

Link Configuration Settings

The Link Configuration panel includes controls to define the 5 GHz SSID and passphrase between radios:

- Link Friendly Name - A friendly name to describe the link between the Access Point (AP) and Station. This name is used to differentiate amongst other links.
- SSID - The wireless link name used by both radios. Both AP and Station must use the same SSID to communicate with each other.
- Encryption Key - Enter the ASCII Passphrase to connect with the broadcasted SSID. Select "Show Key" to see passphrase in plain text. Enter any combination of printable characters. The passphrase should be between 8 to 63 characters in length. The Encryption Key must be the same on both the Access Point and Station for them to communicate with each other.
- Scan for SSID - Causes the Station to scan and display a list of Access Points and the SSIDs they broadcast.
- Status (Connect) - Click button to connect to the SSID. This button will be grayed out if already connected to that network. Status shows "Connected" or "Not Connected".

Example Access Point Link Configuration

Link Configuration ?

Link Friendly Name

SSID

Encryption Key
ASCII Passphrase - 128bit AES

Show Key

Example Station Link Configuration

Link Configuration i

Link Friendly Name -

SSID

Encryption Key
ASCII Passphrase - 128bit AES

Show Key

Status **Connected**

Example SSID Scan after pressing the "Scan SSID" button. To connect to a particular SSID, click the "Select" button.

SSID Scan x

SSID scan may take up to 60 seconds to complete.

Encryption	SSID	Vendor	MAC Address	Signal Strength	
	XXXXXXXXXX	Mimosa	XXXXXXXXXX	-34 dBm	Select
	XXXXXXXXXX	Mimosa	XXXXXXXXXX	-81 dBm	Select
	XXXXXXXXXX	Mimosa	XXXXXXXXXX	-78 dBm	Select
	XXXXXXXXXX	Mimosa	XXXXXXXXXX	-34 dBm	Select
	XXXXXXXXXX	XXXXXX	XXXXXXXXXX	-79 dBm	Select

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.

The table provides the following data per device found:

- SSID - The wireless link name advertised by each detected AP.
- Capability - Indicates which 802.11 (Wi-Fi technology standard) is support by the device. Options include A, G, N, AC.
- MAC Address - The device's unique identifier.
- Vendor - The name of the device manufacturer (if known).
- Wi-Fi 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.

Note: The Site Survey will temporarily interrupt your link. Once started, this process cannot be stopped until complete.

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

The Last Updated field indicates (down to the second) when the last Site Survey was requested.

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

Survey Results i								
SSID	Vendor	MAC Address	Capability	Frequency Channel	Channel Width (MHz)	Frequency Range	TDMA	Signal Strength (dBm)
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	28	1x40	5120-5160	A, 50/50, 4ms	-38
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	18	1x40	5070-5110	A, 50/50, 4ms	-77
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	32	1x40	5140-5180	B, 50/50, 4ms	-34
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	76	2x40	5360-5400, 5070-5110	B, 50/50, 4ms	-81
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	33	1x20	5155-5175	B, 50/50, 4ms	-77
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	33	1x20	5155-5175	B, 50/50, 4ms	-77
[blurred]	[blurred]	[blurred]	11a, 11n	163	1x20	5805-5825	N/A	-81
[blurred]	Mimosa	[blurred]	11a, 11n, 11ac	33	1x20	5155-5175	B, 50/50, 4ms	-77
[blurred]	[blurred]	[blurred]	11a, 11n	53	1x20	5255-5275	N/A	-78
[blurred]	[blurred]	[blurred]	11a, 11n	104	1x20	5510-5530	N/A	-81

Setting a Device Name and Description

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.
- Device Description - A more detailed device description (up to 150 characters) for administrative purposes.

Naming

Device Friendly Name	<input type="text" value="MimosaB5JPK"/>
Device Description	<input type="text" value="Backhaul device near the data center"/>

Reading the Date/Time & Setting the Install Date

The Time panel shows the current date and time in Coordinated Universal Time (UTC). The Install Date input box can be used for administrative purposes, but it is optional and has no other affect.

- Current Date (UTC) - Current date as set by GPS.
- Current Time (UTC) - Current time as set by GPS.
- Install Date - Used to track the date when the device was installed. This date will be set when the device first obtains timing from GPS. It can be manually overwritten.
- NTP Server - .

Time ⓘ

Current Date (UTC)	2015-02-11
Current Time (UTC)	18:19:16
Install Date	<input type="text"/>
NTP Server	0.mimosa.pool.ntp.org ▼

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

Verify New Password


To change password, you must enter your current password below.

Current Password

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

Enabling Watchdog

The Watchdog panel contains controls to monitor a remote host and reboot the local device under configurable failure conditions.

- IP Ping Watchdog - Enables the IP Ping Watchdog feature, which resets the device if it cannot ping a certain IP after a number of retry attempts.
- Ping IP Address - Enter the IP address of the device to ping.
- Interval - Set the number of seconds between ping attempts.
- Delay After Startup - Set the delay in number of seconds between device start up and the first ping attempt.
- Failure Count Triggering Reboot - Set the number of failed ping attempts before rebooting the device. This range can be anywhere from 0 to 100. **WARNING:** rebooting will take the device offline.

Watchdog ⓘ

IP Ping Watchdog	<input type="checkbox"/> Off
Ping IP Address	<input type="text"/>
Interval (Seconds)	<input type="text" value="300"/>
Delay After Startup (Seconds)	<input type="text" value="300"/>
Failure Count Triggering Reboot	<input type="text" value="3"/>

Management Services

The Services panel holds controls to secure management traffic by specifying how it should be served over the network. Options include the use of a VLAN, HTTPS, standard and secure web server port selections, and session timeout.

- Enable HTTPS - Use SSL to access the web interface of this device.
- Web Server Port - Indicate which TCP port will be used for the web server. This web server is for the web interface.
- Secure Web Server Port - Indicate which TCP port will be used for the secure web server.
- Session Time Out - List the number of minutes of inactivity that will be allowed on the interface before automatic log-out for sessions. If set to "0", the session will have no timeout.

Services ⓘ

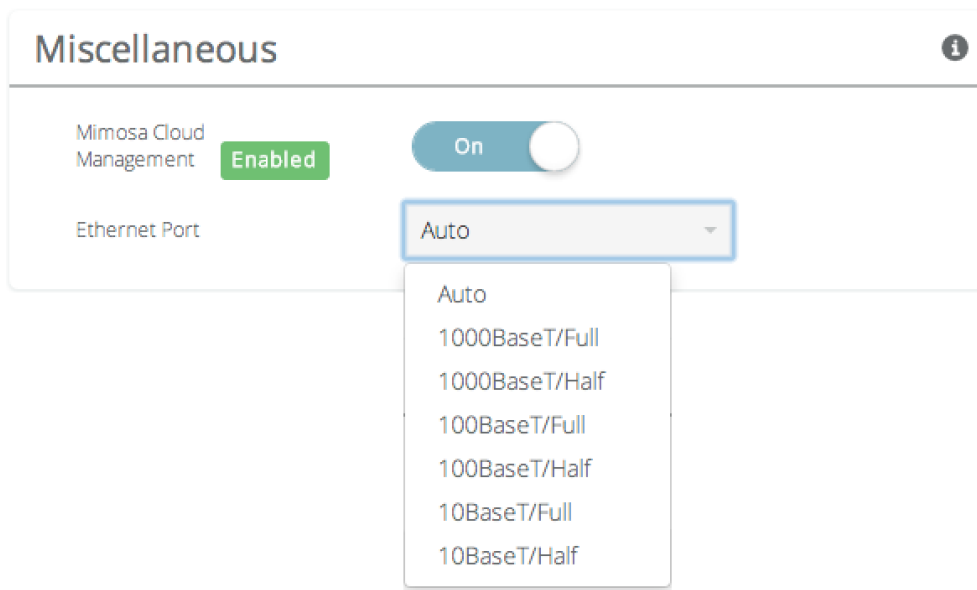
Enable HTTPS	<input type="checkbox"/> Off
Web Server Port	80
Secure Web Server Port - HTTPS	443
Session Timeout (Minutes)	10

Management Miscellaneous Settings

The Miscellaneous panel contains controls to enable Mimosa Cloud Management and to select the Ethernet Port data rate, either automatically or manually.

- Mimosa Cloud Management - Enables the device to use the Mimosa Cloud Management tools.
- Ethernet Port - Set the Ethernet port transfer rate or allow it to be automatically determined. Manually selectable options are 10, 100, or 1000BaseT at either full or half duplex. Note that Auto or 1000BaseT/Full is recommended so that the Ethernet port does not create a bottleneck.

Note: Your firewall must be configured for outbound access to enable Mimosa Cloud Management.



VLAN Management

The VLAN Management panel allows the administrator to enable a VLAN (Virtual Local Area Network) for management traffic. When enabled, all B5/B5c Web Management traffic must originate from a device on that VLAN.

- Enable - Use the slider control to turn VLAN Management on or off.
- ID - The VLAN ID tag.

Note: After saving changes to activate the Management VLAN, the device GUI will become inaccessible over Ethernet, unless connecting over a network configured with a matching VLAN ID. Both ends of the the backhaul link (AP and Station) should be in the same VLAN (configured to use the same VLAN ID).

Management VLAN ⓘ

Enable	<input type="checkbox"/> Off
ID	<input type="text" value="1"/>

Configuring REST Services

The REST Services panel contains controls to enable remote access to the radio's REST API, and then set a username and password that will be used to log in. Note that this feature need only be activated when using a third-party monitoring system that supports REST calls. REST services require that HTTPS is enabled.

- REST Management - Use the slider control to turn REST on or off.
- Management Username - The username that will be used to log into the local device through the REST interface.
- Management Password - The password that will be used to log into the local device through the REST interface.

REST Services ⓘ

REST Management Requires HTTPS	<input checked="" type="checkbox"/> On
Management Username	<input type="text" value="Mimosa"/>
Management Password	<input type="password"/>

Enabling SNMP Notifications

Enable the SNMP service to allow SNMP requests and enable push notifications to a remote server.

- SNMP - Enable or disable SNMP service on the local device.
- Contact - Specify an (optional) administrative contact for the SNMP system.
- Location - Specify the (optional) physical location for the SNMP system.
- Trap Server - Define the server to receive the notifications.

SNMP Notifications ⓘ

SNMP	<input checked="" type="checkbox"/> On
Contact	<input type="text"/>
Location	<input type="text"/>
Trap Server	<input type="text"/>

Configuring SNMP Traps

Define which traps (or notifications) are sent to the remote SNMP server.

- Critical Fault - Notification created if the device is forced to reboot or if GPS signal is lost.
- Boot/Reboot - Notification created if the system boots or reboots.
- Wireless Up/Down - Notification created if the device connects to (Wireless Up) or disconnects from (Wireless Down) another device.
- Ethernet Up/Down - Notification created if the Ethernet Port is connected (Ethernet Up) or disconnected (Ethernet Down).
- Ethernet Speed Change - Notification created when the Ethernet port changes from one speed (10, 100, or 1000BaseT) to another.
- Temperature Low/High - Notification created if the device temperature drops below -40C or rises above +60C.
- Multiple Login Attempts - Notification created if multiple failed login attempts are made from the same IP Address.

SNMP Traps ⓘ

Critical Fault	<input type="checkbox"/> Off
Boot/Reboot	<input type="checkbox"/> Off
Wireless Up/Down	<input type="checkbox"/> Off
Ethernet Up/Down	<input type="checkbox"/> Off
Ethernet Speed Change	<input type="checkbox"/> Off
Temperature Low/High	<input type="checkbox"/> Off
Multiple Login Attempts	<input type="checkbox"/> Off

Enabling System Log Notifications

Enable Syslog service on the local device to send traps to a remote Syslog server.

- Syslog Remote Log - Enable or disable Syslog service on the local device.
- Transport Server - Choose the desired protocol for the Syslog connection. Note that most devices send UDP messages by default. UDP is an unreliable transmission protocol, thus messages may get lost. Choose TCP for higher reliability if any message loss is unacceptable.
- Remote Log IP Address - List the IP Address of the remote Syslog server to which Notifications will be sent.
- Remote Log Port - List the Port on the remote Syslog server to which Notifications will be sent.

System Log Notifications ⓘ

Syslog Remote Log Off

Transport Server

Remote Log IP Address

Remote Log Port

Configuring System Log Traps

Define which traps (or notifications) are sent to the remote server for the System Log.

- Critical Fault - Notification created if the device is forced to reboot or if GPS signal is lost.
- Boot/Reboot - Notification created if the system boots or reboots.
- Wireless Up/Down - Notification created if the device connects to (Wireless Up) or disconnects from (Wireless Down) another device.
- Ethernet Up/Down - Notification created if the Ethernet Port is connected (Ethernet Up) or disconnected (Ethernet Down).
- Ethernet Speed Change - Notification created when the Ethernet port changes from one speed (10, 100, or 1000 BaseT) to another.
- Temperature Low/High - Notification created if the device temperature drops below -40C or rises above +60C.
- Multiple Login Attempts - Notification created if multiple login attempts are made from the same IP Address.

System Log Traps ?

Critical Fault	<input type="checkbox"/> Off
Boot/Reboot	<input type="checkbox"/> Off
Wireless Up/Down	<input type="checkbox"/> Off
Ethernet Up/Down	<input type="checkbox"/> Off
Ethernet Speed Change	<input type="checkbox"/> Off
Temperature Low/High	<input type="checkbox"/> Off
Multiple Login Attempts	<input type="checkbox"/> Off

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.
- Build Date - The date that the installed firmware was created.
- Image File - Update to the latest firmware. Click the Choose File button to select a file for upload the file.

Firmware Update ?

Installed Version	0.1.1-64
Build Date	2014-10-25 15:37:01 (UTC -0700)
Image File	<input type="button" value="Choose File"/>

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

Reset

Reset Device Configuration

Reset Configuration

Reset Device Unlock

Reset Unlock

Reboot Device

Reboot

Backup or Restore Configuration Settings

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

- Backup Current Config - 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.

Backup & Restore Configuration

Backup Current Configuration	<input type="button" value="Download File"/>
Restore Configuration	<input type="button" value="Choose File"/>

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.

Bandwidth Test

A manual test to assess maximum throughput (in Mbps) when minimal or no traffic is present using a proprietary UDP-like protocol. The default test time is approximately 30 seconds.

- **Test Duration** - The length of the bandwidth test in seconds.
- **Run Test** - Click on the Run Test button to assess the maximum throughput. 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 number of hops that you want the trace to take. If no issues are found along the route, this number may be increased.
- **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.

Ping	Bandwidth	Traceroute
Destination IP	127.0.0.1	
Packet Count	600	
Packet Size	64	
<input type="button" value="Run Test"/>		

Running a Bandwidth Test

A manual test to assess maximum throughput when minimal or no traffic is present using a proprietary UDP-like protocol.

- Test Duration - The length of the bandwidth test in seconds.
- Run Test - Click on the Run Test button to assess the maximum throughput. Results are shown in corresponding table.

Ping **Bandwidth** Traceroute

Test Duration
Seconds

30

⏪ Run Test

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.
- Resolve IP Address - Indicate whether the system should resolve and print the host name of the destination.
- Max Number of Hops - Choose the number of hops that you want the trace to take. If no issues are found along the route, this number may be increased.

Ping Bandwidth **Traceroute**

Destination Host 127.0.0.1

Resolve IP Address Off

Max Number of Hops 30

Diagnostic Logs

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

- Event Log - 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.

Events Support Info

```
Sep 17 13:57:55 : : set TDD 1
Sep 17 13:57:55 : : tx_mode: TDD -> TDD
Sep 17 13:57:55 : : set TDD 0
Sep 17 13:57:56 : : set TDD 1
Sep 17 13:57:56 : :Cancel scan
Sep 17 13:57:56 : : StpScan
Sep 17 13:57:56 : reason_code=0x3a000118,0x00000000
Sep 17 13:57:57 : : hal_keyset: idx 4,mac addr Low: 0xb520, Hi: 0x120300c6
```

Events Support Info

This is for customer support

Click the button to download a file to be sent to Mimosa Support.

Support Files

Mimosa REST API

Mimosa provides a REST API that allows developers to access information from our hardware products, such as configuration and status, for integration with third-party applications and services.

Using the API

There are four calls available through the REST API to access different types of information: Device Status, Device Information, Ethernet Data, and Link Information. Each REST API request returns an XML response object.

Accessing the API

All requests to the APIs require authentication. Authentication requires completing both of the following actions:

1. Enable HTTPS within the device GUI.
 - NOTE: For security reasons, REST can not be enabled until HTTPS is activated. This will also activate HTTPS for access to the GUI.
2. Enable REST Management within the device's embedded GUI, and assign a REST-specific Management Username and Password.
3. Include the Management Username and Management Password parameters in the Request URL.

REST Services ⓘ

REST Management
Enabling requires HTTPS Enabled as well. On

Management Username

Management Password

GET Device Status

Returns device status found on the Mimosa embedded Dashboard.

Resource URL

`https://{DEVICE-IP}/core/api/service/status?`

Resource Information

Response Formats	XML
Requires Authentication	Yes (Username / Password), must also be set in the Mimosa embedded GUI.

Parameters

DEVICE-IP Required	The Management IP Address assigned to the Mimosa Device. Example: 192.168.20.1
REST-USERNAME Required	The REST Management username as set in the REST Services Panel within the Mimosa embedded GUI. Example: mimosacloud
REST-PASSWORD Required	The REST Management password as set in the REST Services Panel within the Mimosa embedded GUI. Example: pass123

Request Format

GET

`https://{DEVICE-IP}/core/api/service/status?username={REST-MANAGEMENT-USERNAME}&password={REST-MANAGEMENT-PASSWORD}`

Example Request

GET

https://192.168.20.1/core/api/service/status?username=mimosacloud&password=pass123

Example Response

```
<?xml version="1.0" encoding="UTF-8"?>
<response status="ok">
  <mimosaContent>
    <values>
      <SignalStrength>-58.0753</SignalStrength>
      <TxRate>650</TxRate>
      <RxRate>650</RxRate>
      <Noise>-88.627</Noise>
      <Chains_1_2>5050-5130 MHz</Chains_1_2>
      <Chains_3_4>5050-5130 MHz</Chains_3_4>
      <Tx_Power>0</Tx_Power>
      <Tx_Phys_Rate>650</Tx_Phys_Rate>
      <Rx_Phys_Rate>650</Rx_Phys_Rate>
      <Rx_MCS>7</Rx_MCS>
      <Details>
        <_ELEMENT index="1">
          <Tx />
          <Rx />
          <Noise>-27.0</Noise>
          <Encoding />
        </_ELEMENT>
        <_ELEMENT index="2">
          <Tx />
          <Rx />
          <Noise>-27.8</Noise>
          <Encoding />
        </_ELEMENT>
        <_ELEMENT index="3">
          <Tx />
          <Rx />
          <Noise>0.0</Noise>
          <Encoding />
        </_ELEMENT>
        <_ELEMENT index="4">
          <Tx />
          <Rx />
          <Noise>0.0</Noise>
          <Encoding />
        </_ELEMENT>
      </Details>
      <Noise2 />
    </values>
    <errors />
  </mimosaContent>
  <mimosaStatus>
    <status>0</status>
    <message>Command succeeded</message>
  </mimosaStatus>
  <mimosaSession>4lijtluaodqer2jp90nddednf5</mimosaSession>
</response>
```

Glossary

Signal Strength	The current signal level (in dBm) for the established link.
TxRate	The current IP transmit throughput rate (in Mbps) for the established link.
RxRate	The current IP receive throughput rate (in Mbps) for the established link.
Noise	The receive noise level for the established link.
Chains_1_2	The frequency range for chains 1 and 2.
Chains_3_4	The frequency range for chains 3 and 4.
Tx_Power	The transmit power level for the channel.
Tx_Phys_Rate	The half-duplex transmit PHY rate.
Rx_Phys_Rate	The half-duplex receive PHY rate.
Rx_MCS	The current MCS index for the established link.

GET Device Info

Returns detailed device information found in the summary tables of the Device Details panel of the Mimosa embedded GUI.

Resource URL

`https://{DEVICE-IP}/core/api/service/device-info?`

Resource Information

Response Formats	XML
Requires Authentication	Yes (Username / Password), must also be set in the Mimosa embedded GUI.

Parameters

DEVICE-IP Required	The Management IP Address assigned to the Mimosa Device. Example: 192.168.20.1
REST-USERNAME Required	The REST Management username as set in the REST Services Panel within the Mimosa embedded GUI. Example: mimosacloud
REST-PASSWORD Required	The REST Management password as set in the REST Services Panel within the Mimosa embedded GUI. Example: pass123

Request Format

GET

`https://{DEVICE-IP}/core/api/service/device-info?username={REST-MANAGEMENT-USERNAME}&password={REST-MANAGEMENT-PASSWORD}`

Example Request

GET

https://192.168.20.1/core/api/service/device-info?username=mimosacloud&password=pass123

Example Response

```
<?xml version="1.0" encoding="UTF-8"?>
<response status="ok">
  <mimosaContent>
    <values>
      <DeviceName>Mimosa-Test-Link</DeviceName>
      <Description />
      <InstallDate />
      <Model>B02</Model>
      <DeviceMode>Access point</DeviceMode>
      <SerialNumber>10-0000-0001</SerialNumber>
      <Version>0.4.0-31</Version>
      <Country>United States</Country>
      <Temperature>35.4</Temperature>
      <LastReboot>11d 7h 46m 46s</LastReboot>
      <IPAddress>192.168.1.20</IPAddress>
      <WLANMAC>20:B5:C6:00:07:50</WLANMAC>
      <WANMAC>20:B5:C6:00:07:51</WANMAC>
      <GigabitEthernetPort>20:B5:C6:00:07:50</GigabitEthernetPort>
      <WirelessMode>802.11</WirelessMode>
      <NumberOfAntenna>2</NumberOfAntenna>
      <CableLength>100</CableLength>
      <Location>37.2856 -- -121.9440</Location>
      <BuildDate>2014-11-25 16:09:00 (UTC -0800)</BuildDate>
      <UnlockCode>YKD6ZQ3FZ</UnlockCode>
    </values>
    <errors />
  </mimosaContent>
  <mimosaStatus>
    <status>0</status>
    <message>Command succeeded</message>
  </mimosaStatus>
  <mimosaSession>4lijtluaodqer2jp90nddednf5</mimosaSession>
</response>
```

Glossary

DeviceName	The device friendly name for the local device.
Description	The detailed device description (up to 150 characters) for administrative purposes
InstallDate	The installation date used to track when the device was installed.
Model	Model of the Mimosa Product
DeviceMode	The listing of whether the device is the Access Point or Station.
SerialNumber	The unique identifier for the device assigned at the factory
Version	The currently installed version of the firmware
Country	The regulatory domain (country) in which the device has been configured to run.
Temperature	The measured temperature inside the device.
LastReboot	The date and time at which the device last rebooted.
IPAddress	The IP address of the device.
WLANMAC	The wireless LAN MAC address.
WANMAC	The 5 GHz radio MAC address.
GigabitEthernetPort	The unique identifier for the physical Ethernet interface.
WirelessMode	N/A
Number of Antennas	N/A
Cable Length	N/A
Location	The GPS longitude and latitude coordinates for the device.
Build Date	The date that the installed firmware was created.
Unlock Code	Displays the code to unlock the device.

GET Ethernet Configuration

Returns detailed device networking information found in the Preferences Management page of the Mimosa embedded GUI.

Resource URL

`https://{DEVICE-IP}/core/api/service/ethernet?`

Resource Information

Response Formats	XML
Requires Authentication	Yes (Username / Password), must also be set in the Mimosa embedded GUI.

Parameters

DEVICE-IP Required	The Management IP Address assigned to the Mimosa Device. Example: 192.168.20.1
REST-USERNAME Required	The REST Management username as set in the REST Services Panel within the Mimosa embedded GUI. Example: mimosacloud
REST-PASSWORD Required	The REST Management password as set in the REST Services Panel within the Mimosa embedded GUI. Example: pass123

Request Format

GET

`https://{DEVICE-IP}/core/api/service/ethernet?username={REST-MANAGEMENT-USERNAME}&password={REST-MANAGEMENT-PASSWORD}`

Example Request

GET

https://192.168.20.1/core/api/service/ethernet-conf?username=mimosacloud&password=pass123

Example Response

```
<?xml version="1.0" encoding="UTF-8"?>
<response status="ok">
  <mimosaContent>
    <values>
      <PortSpeed>Auto</PortSpeed>
      <SpanningTree>0</SpanningTree>
      <IPAddressMode>Static</IPAddressMode>
      <CurrIP>184.105.87.18</CurrIP>
      <CurrNetmask>255.255.255.240</CurrNetmask>
      <CurrGateway>184.105.87.17</CurrGateway>
      <CurrDNS1>8.8.8.8</CurrDNS1>
      <CurrDNS2>8.8.4.4</CurrDNS2>
      <StaticIP>184.105.87.18</StaticIP>
      <StaticNetmask>255.255.255.240</StaticNetmask>
      <StaticGateway>184.105.87.17</StaticGateway>
      <StaticDNS1>8.8.8.8</StaticDNS1>
      <StaticDNS2>8.8.4.4</StaticDNS2>
      <Curr>
        <IP>184.105.87.18</IP>
        <Netmask>255.255.255.240</Netmask>
        <Gateway>184.105.87.17</Gateway>
        <PrimaryDNS>8.8.8.8</PrimaryDNS>
        <SecondaryDNS>8.8.4.4</SecondaryDNS>
      </Curr>
      <Static>
        <IP>184.105.87.18</IP>
        <Netmask>255.255.255.240</Netmask>
        <Gateway>184.105.87.17</Gateway>
        <PrimaryDNS>8.8.8.8</PrimaryDNS>
        <SecondaryDNS>8.8.4.4</SecondaryDNS>
      </Static>
      <ActualIP>184.105.87.18</ActualIP>
      <MTU>1500</MTU>
    </values>
    <errors />
  </mimosaContent>
  <mimosaStatus>
    <status>0</status>
    <message>Command succeeded</message>
  </mimosaStatus>
  <mimosaSession>4lijtluaodqer2jp90nddednf5</mimosaSession>
</response>
```

Glossary

PortSpeed	The Ethernet Port Speed (in Mbps) for the device. (Options include: Auto, 10/100/1000)
SpanningTree	N/A
IPAddressMode	Lists the preferred mode of network addressing
CurrIP	The network address used to manage the device.
CurrGateway	The gateway address for the subnet.
CurrDNS1	The default DNS server IP Address.
CurrDNS2	The backup DNS server IP Address.

GET Link Info

Returns detailed link information typically found in the Wireless section of the Mimosa embedded GUI.

Resource URL

`https://{DEVICE-IP}/core/api/service/link-info?`

Resource Information

Response Formats	XML
Requires Authentication	Yes (Username / Password), must also be set in the Mimosa embedded GUI.

Parameters

DEVICE-IP Required	The Management IP Address assigned to the Mimosa Device. Example: 192.168.20.1
REST-USERNAME Required	The REST Management username as set in the REST Services Panel within the Mimosa embedded GUI. Example: mimosacloud
REST-PASSWORD Required	The REST Management password as set in the REST Services Panel within the Mimosa embedded GUI. Example: pass123

Request Format

GET

`https://{DEVICE-IP}/core/api/service/link-info?username={REST-MANAGEMENT-USERNAME}&password={REST-`

MANAGEMENT-PASSWORD}

Example Request

GET

https://192.168.20.1/core/api/service/link-info?username=mimosacloud&password=pass123

Example Response

```
<?xml version="1.0" encoding="UTF-8"?>
<response status="ok">
  <mimosaContent>
    <values>
      <LinkName>HECPLINK</LinkName>
      <MaxCapacity />
      <Distance>150</Distance>
      <Frequency>5090 MHz (ch 18)</Frequency>
      <BandWidth>80</BandWidth>
      <PacketsReceived>861413377</PacketsReceived>
      <PacketsSent>1009901282</PacketsSent>
      <BytesReceived>1526527039</BytesReceived>
      <BytesSent>1357421940</BytesSent>
    </values>
    <errors />
  </mimosaContent>
  <mimosaStatus>
    <status>0</status>
    <message>Command succeeded</message>
  </mimosaStatus>
  <mimosaSession>4lijtluaodqer2jp90nddednf5</mimosaSession>
</response>
```

Glossary

LinkName	The friendly name to describe the link between the Access Point (AP) and Station
MaxCapacity	N/A
Distance	Link Distance In km

Frequency	The center frequency of the selected channel width and its associated channel number.
BandWidth	The channel width (in MHz) for the radio.
PacketsReceived	The number of packets received on this link.
PacketsSent	The number of packets sent on this link.
BytesReceived	The number of bytes received on this link.
BytesSent	The number of bytes sent on this link.

FCC/IC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.*
- Increase the separation between the equipment and receiver.*
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.*
- Consult the dealer or an experienced radio/TV technician for help.*

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Purple Communications, Inc, may void the user's authority to operate the equipment.

English

This device complies with Industry Canada license-exempt RSS standard(s).
Operation is subject to the following two conditions:

1. This device may not cause harmful interference;
2. This device must accept any interference received, including interference that may cause undesired operation of the device.

French

Cet appareil est conforme à Industrie Canada une licence standard RSS
exonérés (s). Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne doit pas provoquer d'interférences
2. Cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant provoquer un fonctionnement indésirable de l'appareil.

RF EXPOSURE

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 antenna should be more than 1m.

La puissance de sortie rayonnée de cet appareil est inférieure aux limites d'exposition de radio de fréquence FCC. Néanmoins, le dispositif doit être utilisé de telle manière que le potentiel pour le contact humain pendant l'utilisation normale soit minimisé. Afin d'éviter la possibilité de dépasser la limite d'exposition de fréquence radio de la FCC, la proximité humaine à l'antenne devrait être plus que 1m.