

[A] CONTROL™



LOCAL HARDWARE NETWORK CONTROLLER

FEATURES

- Backup and Restore Functionality
- Can Manage Up To 1,000 Alta Labs Devices
- Multi-Site Management
- Mobile App
- Reverse Proxy HTTP Support
- Port Forwarding
- Customizable Dashboard
- Device Cards
- Wireless Network Color Coding
- Status Snapshots
- AltaPass™ Multi-Password Technology*
- Advanced Filtering - DPI Engine*
- Dark Mode
- Site Manager
- Internet Access Schedule
- Extended Access Requests
- On-The-Fly Changes and Scanning
- Hotspot Functionality*
- SSID Broadcasting Flexibility

* Alta Labs Access Points Required

[A] CONTROL™ VERSIONS



Hardware

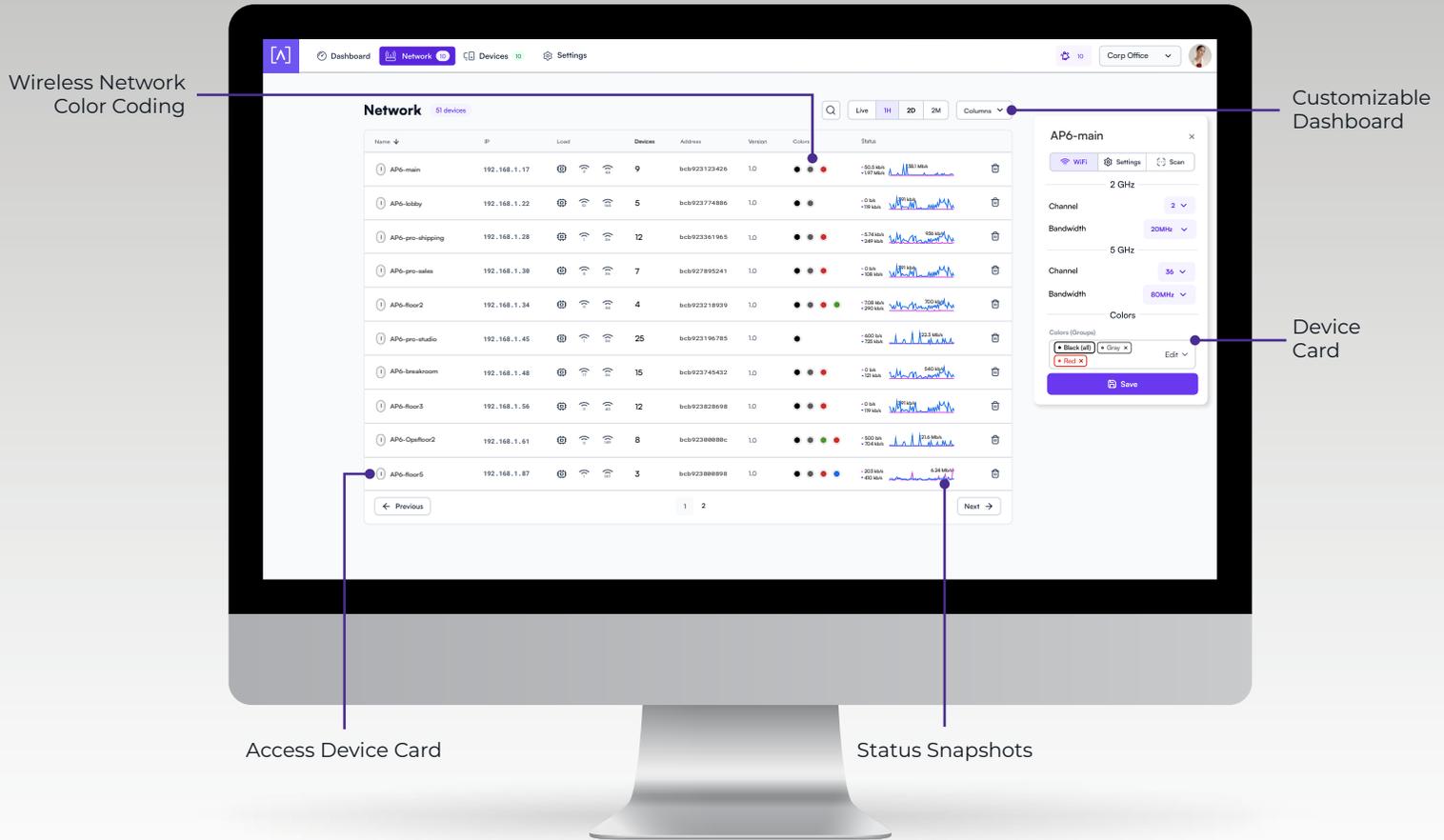
Cloud

Download

Cost/License Fee	\$149 - Hardware & Software Solution	None - included with Alta Labs hardware purchase	\$49 One-Time License Fee
Accessibility	Local*	Global	Local*
Ease Of Install	Mid	Easy	Advanced
Reliability	Network Dependent**	99.99% Uptime	Network Dependent**
Security	Secure	Secure	Secure
Reverse Proxy Support	Yes	N/A	Yes
Bluetooth for Seamless Setup	Yes	Yes	No
Maximum Devices Attached	1000	No Limit	Depends on host
Multitenant Support	Yes	Yes	Yes
AltaPass	Yes	Yes	Yes
Disconnect Notifications	Yes	Yes	Yes
Advanced Site Permissions	Yes	Yes	Yes
Automatic Updates	Yes	Yes	Yes

* Hardware and Download can be global, if properly configured

** Hardware and download are going to be dependent on onsite power, network architecture. Download will be as reliable as the server its installed on.



Access Device Card

Status Snapshots



Customizable Dashboard

Customize your dashboard with the information you want to see: AP name, IP address, Load, MAC address, firmware version, wireless network color assignment, and real-time status details. Details are sortable by column.

Device Cards

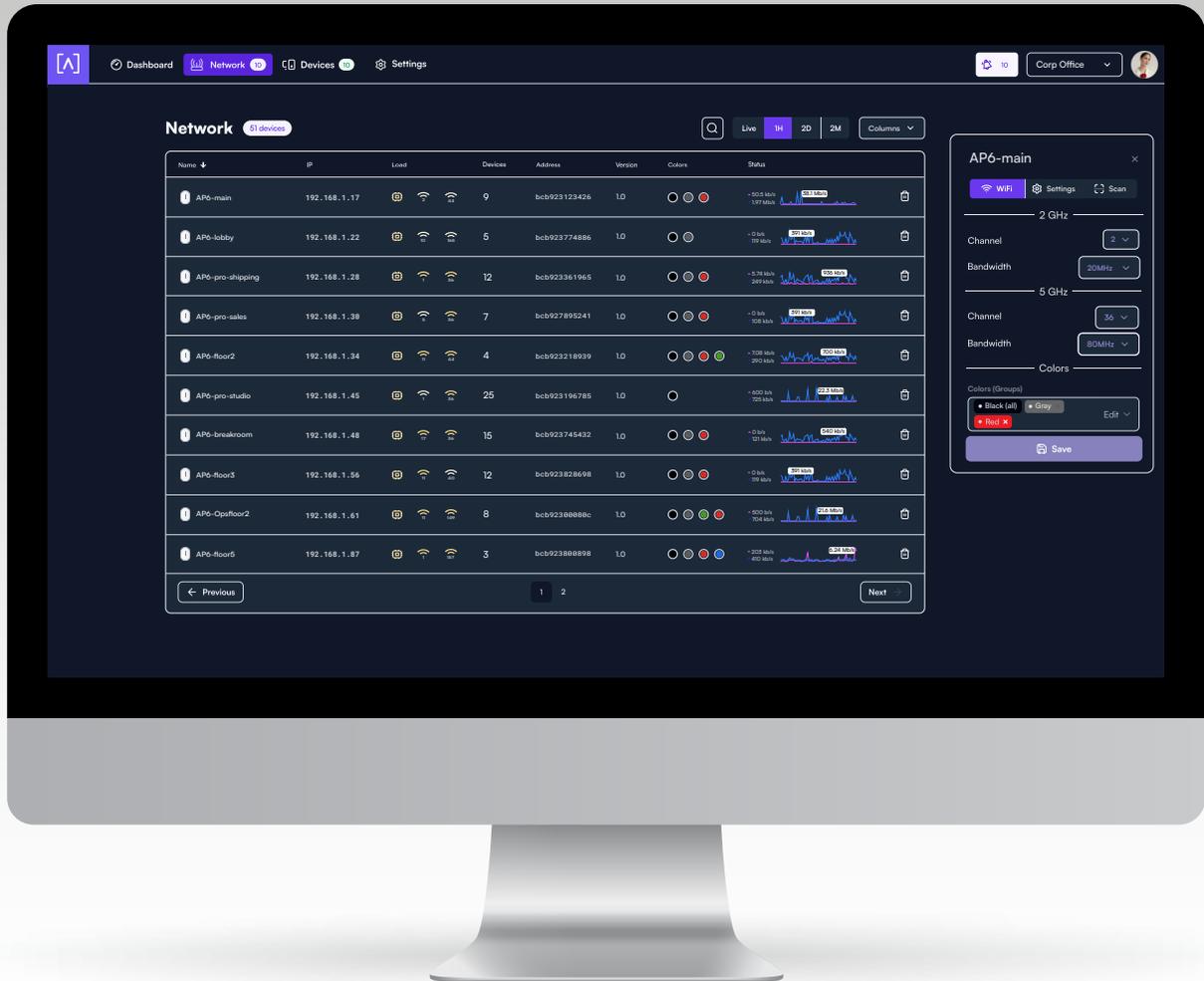
Easily view connection details and configure your access points or client connections by clicking the device icon.

Wireless Network Color Coding

Patent pending functionality that allows you to assign color groups to wireless SSIDs and use them to assign membership to wireless access points.

Status Snapshots

View upload and download throughput with a visual timeline on the dashboard for each AP displayed along with the number of connected devices, average processor load, channel load, and average connected devices. Select a snapshot of the last minute, last hour, last two days, or last two months.

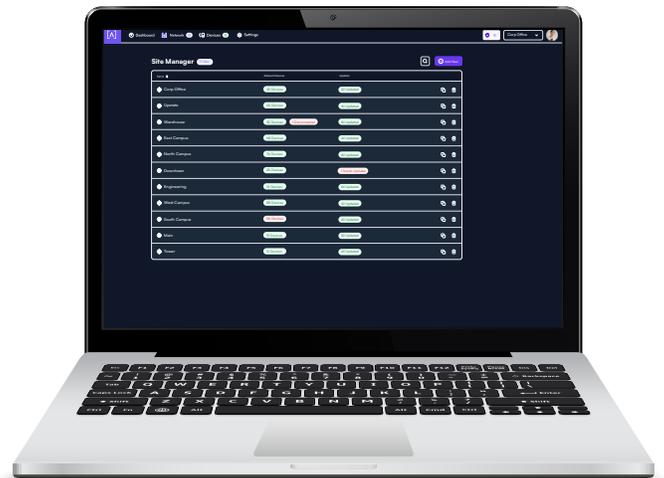


Dark Mode

The Alta interface settings provide the option to match your system theme, use a light theme, or to select a dark theme.

Site Manager

The Alta Site Manager provides an overview of all sites, displays the number of devices for each site, and shows when updates are needed. New sites can be added and current sites can be duplicated or removed. Use the search option to look for a specific site.



Multi-Site Management

Deploy and manage multiple sites quickly and easily. Add, delete, or rename sites instantly. Toggle between sites from a site selection drop-down. Each site contains its own data set.

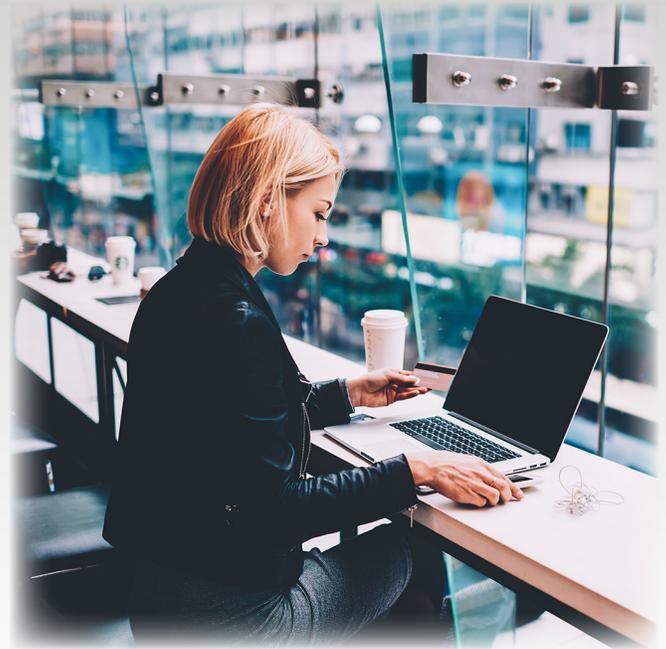
Mobile App

Monitor and manage your networks from the convenience of your mobile device using the Alta Networks app. Sign up for an Alta Labs account using just your name, email, and password.



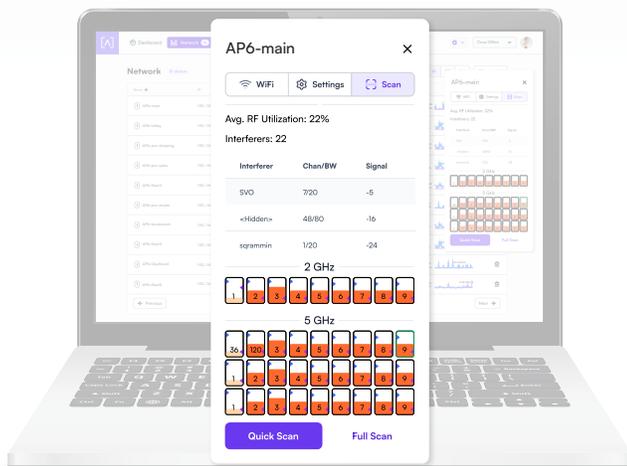
Hotspot Functionality

Built-in functionality to create your own local hotspot with a logo, title page, terms of service, and a final landing page. You also have the option to redirect to an external URL.



On-The-Fly Changes and Scanning

- Configuration changes do not require a reboot of your network. Changes can be made without taking your network down.
- Scan your AP environment without disrupting your WiFi network.

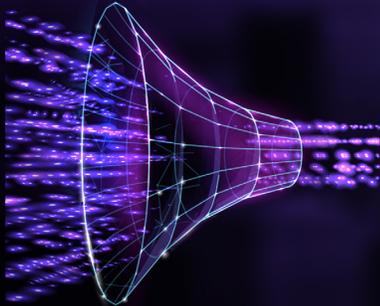


SSID Broadcasting Flexibility

Alta Labs' patented wireless scheduling functionality elevates your network by maximizing availability and user convenience. Instead of shutting off the wireless network completely during scheduled downtime like other wireless access points, your Alta Labs wireless network is always on. During downtime, a captive portal hotspot is presented to the user, as well as the option to request access. This provides network admins with the ability to grant users additional time on the network.

ALTA PASS™
MULTI-PASSWORD TECHNOLOGY

- WiFi-Staff
- WiFi-Guest
- WiFi-HiSpeed
- WiFi-IT
- WiFi-Patio
- WiFi-Lounge
- WiFi-Artists
- WiFi-Public



OneWiFi



AltaPass™ Multi-Password Technology

AltaPass is a unique Alta Labs patented feature that allows clients to connect to the same wireless network SSID using different passwords. The functionality is built in to all Alta Labs Access Points and managed using Control™.

Configure unlimited passwords and effortlessly scale to thousands of users. Clients are provided with different network and internet access levels based on the password they use to connect to the network. Passwords can be utilized by individuals or groups.

When a password is created, select from one of the predefined standard use cases. The password can then also be associated with limited download and/or upload speeds, assigned to a VLAN, or set to bypass the filtering rules, the hotspot functionality, or to ignore the schedule.

- **Standard/Small** Typical network with less than 100 WiFi clients/devices
- **Large** Optimized for hundreds to thousands of WiFi clients/devices
- **IoT** Restricted to Internet and local incoming connections only
- **Internet only** Restricted to Internet only
- **Guest** Restricted to Internet and IoT devices

ALTA PASS™
MULTI-PASSWORD TECHNOLOGY



INTERNET ONLY

STANDARD NETWORK

GUEST NETWORK



Advanced Filtering - DPI Engine

The Alta Labs Access Points have a built-in powerful Deep Packet Inspection (DPI) engine. By incorporating this feature directly in the access points, there is no need to purchase additional hardware to take advantage of this powerful tool.

Restrict access to websites, applications, or application types. Filter settings are easily applied in the Alta Labs web management interface.

Select applications or application types in the Block Applications drop-down menu. Block websites by typing in their domain names in the Block Domains field.

Password-Based Exceptions

There are many scenarios where users can't have or don't need their content filtered. The Alta Labs management interface allows you to bypass the site filter policy using our Multi-Password Authentication technology. Define a password to provide to users that bypasses the defined filter rules. If a hotspot has been created, it can also be bypassed. If a schedule has been defined, it can be ignored. Multiple password options can be defined using various combinations of the options.



Device Specific Exceptions

For instances where specific devices should not have their content filtered, adhere to a schedule, or bypass a hotspot, admins can allow individual devices to bypass the filter, schedule, and/or hotspot settings.

Passwords

Use different passwords to automatically separate different types of... [Show More](#)

Standard [password field] [lock icon]

Guest [Add Password]

VLAN [Number] [Sites]

DL Rate (Mbps) [Mbps]

UL Rate (Mbps) [Mbps] [Edit]

Bypass HotSpot

Ignore Schedule

Bypass Filter [Edit]

Outdoor SmartPlug [close icon]

Blank values will use defaults.

Network Type [Use Default]

VLAN [input]

DL Rate (Mbps) [input]

UL Rate (Mbps) [input]

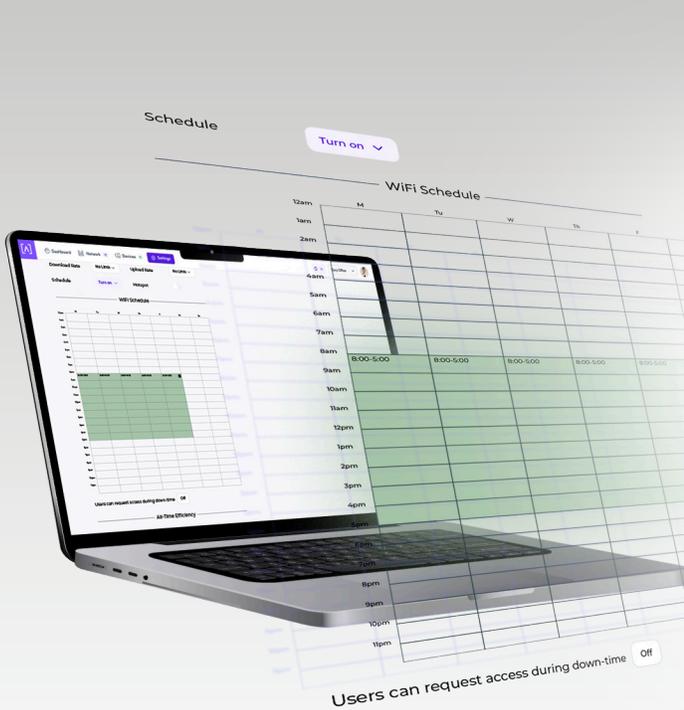
Bypass Hotspot [Yes]

Bypass Schedule [Use Default]

Bypass Filter [Yes]

Device Icon [lightning bolt icon]

[Reset] [Save]



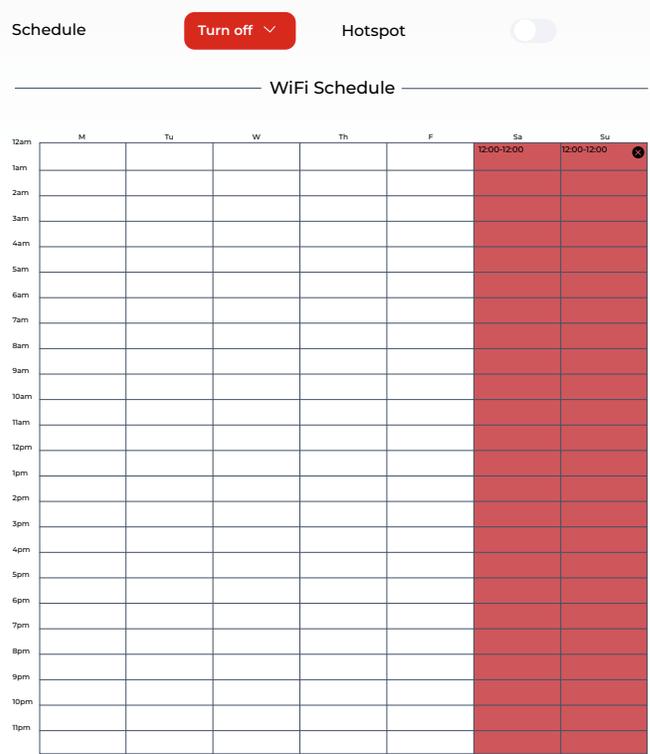
Users can request access during down-time On

Internet Access Schedule

Easily create an internet access schedule to define the times when internet access will be turned on or off. Select a large time block covering the entire week or select hourly and daily times individually. Drag time blocks to move them to a different day or time. Extend or reduce time blocks by adjusting them in any direction. A schedule can be created for each wireless network SSID you create.

Extended Access Requests

When internet access is turned off, users can still access the local network as the wireless network SSID continues broadcasting when the internet is turned off (unless disabled). If the option “Users can request access during down-time” is turned on, a user can request internet access outside of the defined hours. The system admin will be notified of the request and can approve or deny it.



Users can request access during down-time Off

SPECIFICATIONS

MECHANICAL	
Dimensions	25.7 x 91 x 180 mm (1 x 3.6 x 7.1")
Weight	.38 kg (.83 lbs)
Material Type	Injection Molded Plastic
Material Finish	Matte
Color	White
PORTS	
Network Interface	Ethernet, Bluetooth
Management Interface	(1) GbE RJ45 Port
LEDS	
Network	Orange: 10/100 Mbps, Blue: 1000 Mbps
HARDWARE	
Processor	Quad-core Qualcomm 2.2 GHz
Button	Factory reset
Bluetooth	Yes, Setup
POWER	
Power Method	PoE+ or USB 5V
Supported Voltage Range	42.4-57V DC for PoE, 4.75V to 5.25V for USB
Power Consumption	8W max, 5W typical
SOFTWARE	
Reverse Proxy HTTP Support	Yes
Port Forwarding	Yes
ENVIRONMENTAL	
Mounting	Wall, Desktop
Operating Temperature	-5 to 50° C (23 to 122° F)
Operating Humidity	5 to 95% Noncondensing
Certifications	CE, FCC, IC

