SonicWave 432o Outdoor Wireless Access Point

Secure Wireless Solution

SonicWall SonicWave series wireless access points (APs) combine high-performance IEEE 802.11ac Wave 2 wireless technology with flexible deployment options. These highly secure APs can be managed via the cloud using SonicWall Wireless Network Manager (WNM) or through SonicWall's industry-leading next-generation firewalls. The result is a solution that could be untethered from the firewall to provide a superior experience for Wi-Fi users that's as secure as any wired connection.

Mounting Options. View full specs »

Outdoor

SonicWave 432o

HIGHLIGHTS

Intuitive cloud management

- Integrated Switch management
- Alerts and rich analytics
- Automatic firmware updates
- Integrated WiFi Planner tool
- Easily switch to firewall management

Enhanced user experience

- 802.11ac Wave 2
- Auto channel selection
- Application control and visibility
- RF spectrum analysis
- AirTime Fairness and fast roaming

Best-in-class wireless security

- Dedicated third scanning radio
- WPA3 support
- Capture ATP and content filtering service
- Deep packet inspection technology

Zero-Touch Deployment powered by SonicExpress mobile app

- Easy registration and onboarding
- Auto-detection and auto-provisioning
- App available on iOS and Android

Ruggedized outdoor design

- IP67 rated, industrial-grade enclosure

Find the right SonicWall solution for your small business and branch:

sonicwall.com/secure-wireless

DATASHEET

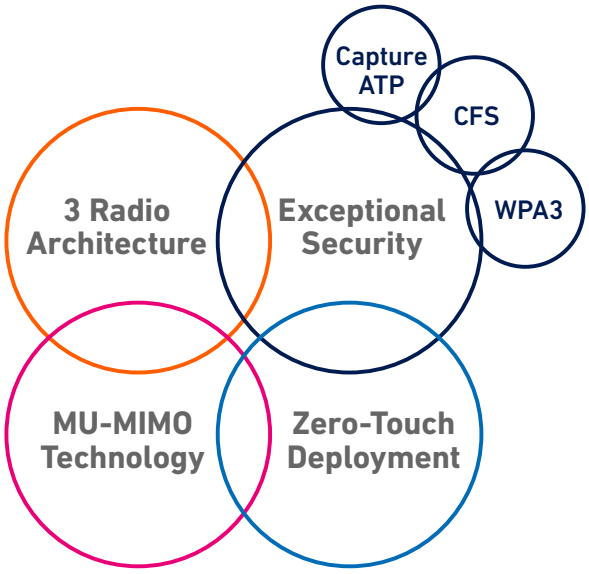
Intuitive cloud management

SonicWall WNM provides an intuitive user interface to manage all SonicWave APs from a single pane of glass via SonicWall Capture Security Center (CSC). Additionally, the dashboard provides integrated SonicWall Switch management, providing centralized management of switches and APs. Easily monitor and manage networks with alerts and rich analytics updated in real-time. Always stay up-to-date with the current features and enhancements from the latest firmware. Updates are pushed automatically to APs, eliminating manual updates and chances of human error.

Enhanced user experience

SonicWave APs take advantage of the capabilities in 802.11ac Wave 2 and advanced RF capabilities to deliver high-speed wireless performance. MU-MIMO technology allows the APs to communicate to multiple client devices at the same time, improving the overall network performance, efficiency and user experience. In combination, mesh technology supported on SonicWave 432o APs enables ease of installation and deployment. Mesh networks are easy to set up, effortless to expand, and require fewer cables and less manpower to deploy, reducing installation costs.

With multiple transmitting and receiving antennas, SonicWave APs are engineered to optimize signal quality, range and reliability for wireless devices. SonicWave APs support fast roaming so that users can roam from one location to another seamlessly. Feature-rich portfolio includes air-time fairness, band steering, and signal analysis tools for monitoring and troubleshooting.



Best-in-class wireless security

SonicWall firewalls scan all wireless traffic coming into and going out of the network using deep packet inspection technology and then remove harmful threats such as malware and intrusions, even over SSL/TLS encrypted connections. Other security and control capabilities such as content filtering, application control and intelligence and Capture Advanced Threat Protection (ATP) provide added layers of protection.

Capture ATP is our award-winning multi-engine sandboxing service that features SonicWall's patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine of Capture ATP proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds.

Manage SonicWave APs independently — even where firewalls are not deployed.

The SonicWave 432o AP includes three radios, where the third radio is dedicated to security and performs rogue AP detection, passive scanning and packet capturing. The SonicWave solution also integrates additional security-related features including wireless intrusion detection and prevention, virtual AP segmentation, wireless guest services, RF monitoring and wireless packet capture.

Simplified firewall management

Deployment and setup of APs are greatly simplified, reducing total cost of ownership. Optionally, SonicWave APs can be managed by SonicWall next-gen firewalls. Integrated into every SonicWall firewall is a wireless controller that auto-detects and auto-provisions SonicWave APs across the network.

Management and monitoring for wireless and security are handled centrally through the firewall, providing network administrators with a single pane of glass from which to manage all aspects of the network.

Zero-Touch Deployment (ZTD) powered by SonicExpress app

Easily register and onboard SonicWave APs with the help of SonicWall SonicExpress mobile app. The APs are automatically detected and provisioned with Zero-Touch Deployment. Available on iOS and Android, SonicExpress mobile app lets network administrators monitor and manage networks.

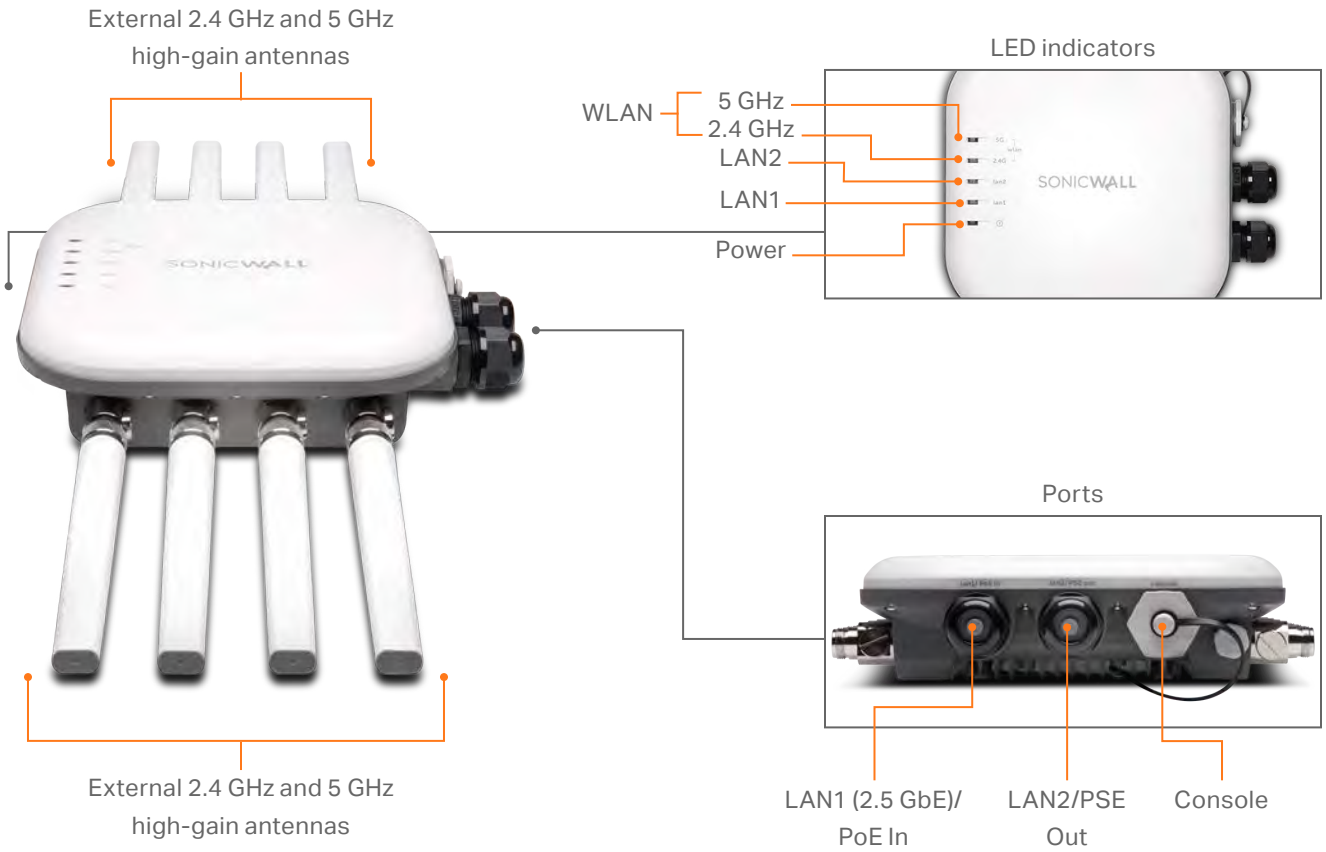
Design with WiFi Planner

SonicWall WiFi Planner is a cloud-based, advanced wireless site survey tool that enables to optimally design and deploy a wireless network for enhanced wireless user experience.

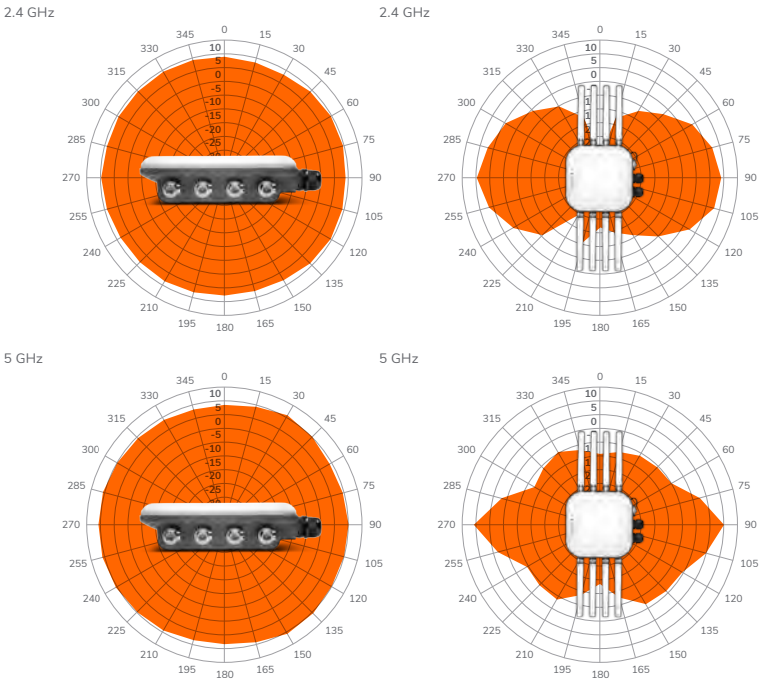
Ruggedized outdoor design

SonicWave outdoor APs are built to withstand rough outdoor conditions with industrial-grade enclosure. These APs are IP67 rated, which ensures protection against dust and water immersion.

SonicWave 432o - The Outdoor AP



RF coverage maps



SonicWave 400 Series Specifications

HARDWARE SPECIFICATIONS	SONICWAVE 432o
Location	Outdoor
Dimensions	9.5 (W) x 9.3 (D) x 2.4 (H) in 24.1 (W) x 23.6 (D) x 6.1 (H) cm
Weight	2.2 kg / 4.9 lbs
WEEE weight	4.1 kg / 9.1 lbs
Shipping weight	4.7 kg / 10.4 lbs
PoE injector	802.3at
Maximum power consumption (W)	21.2 W
Status indicators	Six (6) LED (WLAN/Link) (LAN/Link) Power, Test
Antennas	8 N-type dipole
Wired network ports	(1) 10/100/1000 auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE); (1) 100/1000/2.5 GbE auto-sensing RJ-45 for Ethernet; (1) RJ-45 console
5G/4G/LTE USB modem support	Yes
Accessories included	Pole mount kit
Virtual access points/SSID group	Up to 8 per access point
Chassis	UL 1024 plenum rated
USB WAN card security clamp	N/A

STANDARDS AND COMPLIANCE	SONICWAVE 432o
IEEE Standards	802.11ac Wave 2, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.11e, 802.11i, 802.11r, 802.11k, 802.11v, 802.11w
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA, TKIP, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w
Wi-Fi Alliance Certification ID	WFA74189
Regulatory	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE
Safety Approvals	UL E211396, UL 62368-1, UL 60950-1 cUL CAN/CSA C22.2 No. 62368-1-14, CAN/CSA C22.2 No. 62368-1-14, EN 60950-1 Or EN 62368-1, IEC 60950-1, IEC 62368-1, Europe: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1
Radio Approvals	USA: FCC Part 15C, 15E, Canada: ISED RSS-247, Europe: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Additional country approvals for Japan, Korea, China, India, Brazil
EMI Approvals	USA: FCC P15B, Canada: ICES-003, Europe: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438
Exposure Approvals	USA: FCC Part 2, Canada: RSS-102, Europe: EN 50385, Aus/Nz: ASNZS 2772
MIMO	MU-MIMO 4x4 (4 streams)
Max/Recommended connected clients per radio	128/48
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union
USB WAN failover and load balancing	N/A

ENVIRONMENTAL	SONICWAVE 432o
Temperature range	-40 to 140°F, -40 to 60°C
Humidity	10 - 95%, non-condensing

RADIO SPECIFICATIONS	SONICWAVE 432o
Radios	Dual: 4x4 11n + 4x4 11ac MU-MIMO; Dedicated third scanning radio; Bluetooth Low Energy radio

RADIO SPECIFICATIONS	SONICWAVE 432o
Frequency bands	802.11a: 5.180-5.825 GHz, 802.11b/g: 2.412-2.472 GHz, 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz, 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz
Operating channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4, 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only), 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64
Transmit output power	Based on the regulatory domain specified by the system administrator
Transmit power control	Supported
Data rates supported	802.11a: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11b: 1,2,5.5,11 Mbps per channel, 802.11g: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel, 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7, 1040, 1170, 1300, 1560, 1733.4 Mbps per channel
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM), 802.11b: Direct Sequence Spread Spectrum (DSSS), 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS), 802.11n: Orthogonal Frequency Division Multiplexing (OFDM), 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)

SECURITY	SONICWAVE 432o
Data encryption	WPA3, WPA2, IPSec, 802.11i, WPA, 64/128/152-bit WEP, TKIP, AES, SSL VPN**
SSL-VPN client*	NetExtender, Connect Tunnel
Advanced security services	Capture ATP, CFS, Geo-IP, Botnet, Anti-virus (Cloud)

AUTHENTICATION	SONICWAVE 432o
Authentication	RADIUS, Active Directory, single sign-on (SSO), local user
Captive Portal	Click-through, external server, social account (facebook, google, twitter and linkedin), sign on
Captive Portal Sign On	Local users, RADIUS, LDAP, OTP, AD

REPORTING	SONICWAVE 432o
Alerts	Critical alert notification via SMS

*SonicWave acts as an SSL-VPN client
**When used with SonicWall Secure Mobile Access Series appliance

SonicWave Feature Summary

SUPERIOR USER EXPERIENCE

Feature	Description
High-speed wireless performance and range	SonicWave access points are based on the 802.11ac Wave 2 standard, which can achieve a PHY rate of up to 2.34 Gbps while maintaining a higher performance level at greater ranges depending on environmental conditions.
Enhanced signal quality	The 802.11ac standard operates in the 5 GHz frequency band, which has fewer wireless devices competing for airspace and is therefore less prone to signal interference.
Increased wireless reliability	The increase in bandwidth capacity and greater number of spatial streams combined with MU-MIMO and the improved processing offered by 802.11ac, result in more reliable wireless coverage.
MU-MIMO	MU-MIMO (Multi-user, multiple-input, multiple-output) technology enables simultaneously transmission from the access point to numerous wireless clients instead of just one.
Band steering	Band steering improves the user experience by steering dual-band clients to automatically connect to the less crowded 5 GHz frequency band leaving the more crowded 2.4 GHz frequency for legacy clients.
Beamforming	Beamforming improves wireless performance and range by focusing the wireless signal on an individual client instead of spreading the data transmission equally in all directions.
AirTime Fairness	AirTime Fairness distributes air time equally among connected clients, ensuring faster clients get more data in their time while slower clients receive less.
Wireless mesh	A wireless mesh enables to extend wifi coverage instantly without requiring cables.
FairNet wireless bandwidth allocation	FairNet guarantees a minimum amount of bandwidth to each wireless client in order to prevent disproportionate bandwidth consumption by a single user.

COMPREHENSIVE WIRELESS SECURITY

Feature	Description
Reassembly-Free Deep Packet Inspection technology	SonicWall next-generation firewalls tightly integrate Reassembly-Free Deep Packet Inspection® (RFDPI) technology to scan all inbound and outbound traffic on wired and wireless networks and eliminate intrusions, ransomware, spyware, viruses and other threats before they enter the network.
Real-Time Deep Memory Inspection (RTDMI)	This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware.
SSL/TLS decryption and inspection	The SonicWall firewall decrypts and inspects SSL/TLS traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL/TLS-encrypted traffic.
Dedicated third scanning radio	Most SonicWave access points include a dedicated that performs continual scanning of the wireless spectrum for rogue access points plus additional security functions that help with PCI compliance.
Wireless intrusion detection and prevention	Wireless intrusion detection and prevention scans the wireless network for unauthorized (rogue) access points and then the managing firewall automatically takes countermeasures, such as preventing any connections to the device.
Wireless guest services	Wireless guest services enables administrators to provide internet-only access for guest users. This access is separate from internal access and requires guest users to securely authenticate to a virtual access point before access is granted.
Lightweight hotspot messaging	Lightweight hotspot messaging extends the SonicWall wireless guest services model of differentiated internet access for guest users, enabling extensive customization of the authentication interface and the use of any kind of authentication scheme.
Captive portal	Captive portal forces a user's device to view a page and provide authentication through a web browser before internet access is granted.
Virtual access point segmentation	Administrators can create up to eight SSIDs on the same access point, each with its own dedicated authentication and privacy settings. This provides logical segmentation of secure wireless network traffic and secure customer access.
Cloud ACL	An extension to local ACL, cloud ACL is deployed and managed from a centralized RADIUS server in the cloud. This eliminates local ACL scalability issues, enabling organizations to configure authentication accounts based on their specific requirements. In addition, MAC authentication can be enforced on all Wi-Fi-enabled devices even if they are not capable of 802.1x support. This adds another layer of protection to the wireless network.
Multi-RADIUS authentication	Multi-RADIUS Authentication provides enterprise-class redundancy by enabling organizations to deploy multiple RADIUS servers in active/passive mode for high availability. Should the primary RADIUS server fail, the managing SonicWall firewall discovers the failure and switches to the secondary server, ensuring wireless devices can continue to authenticate. Further, multi-RADIUS authentication can be supported on each virtual access point and configured for WPA-Enterprise, WPA2-Enterprise or WPA2-Auto-Enterprise mode.
Granular security policy enforcement	Network administrators can implement and enforce firewall rules on all wireless traffic and control all wireless client communications to any host on the network — wired or wireless.

SIMPLIFIED DEPLOYMENT AND CENTRALIZED MANAGEMENT

Feature	Description
Simplified setup and centralized management	SonicWave access points are automatically detected, provisioned and updated by the cloud or though SonicWall next-gen firewalls. WLAN administration is also handled directly from the managing firewall, simplifying setup and centralizing ongoing management.
Integrated Switch Management	SonicWall Wireless Network Manager provides integrated management of SonicWave Access Points and SonicWall Switches for unified visibility and management of the network.
WiFi Planner	To optimize access point placement before deployment, WiFi Planner provides comprehensive visualization of the Wi-Fi environment including obstacles that impact signal performance plus both covered and non-covered zones.
Floor plan view	Floor plan view is a Wi-Fi planning tool that enables users to upload or create a floor plan and place SonicWave access points appropriately to ensure required wireless coverage.
Topology view	Topology view is a Wi-Fi tool that automatically maps devices and how they are connected in the wireless network architecture in order to aid in troubleshooting.
Plenum rated	SonicWave access points are plenum rated for safe installation in air-handling spaces such as in or above suspended ceilings.
Multiple power options	SonicWave access points are powered from a SonicWall Power over Ethernet (PoE) Injector or third-party device for easy deployment where electrical outlets are not readily accessible.
Light controls	With dimmable LEDs (excluding power), SonicPoints fit perfectly into environments that need discreet wireless coverage.
Broad standards and protocols support	SonicWave access points support a wide range of wireless standards and security protocols, including 802.11 a/b/g/n/ac, WPA2 and WPA. This allows organizations to leverage prior investments in devices that are incapable of supporting higher encryption standards.

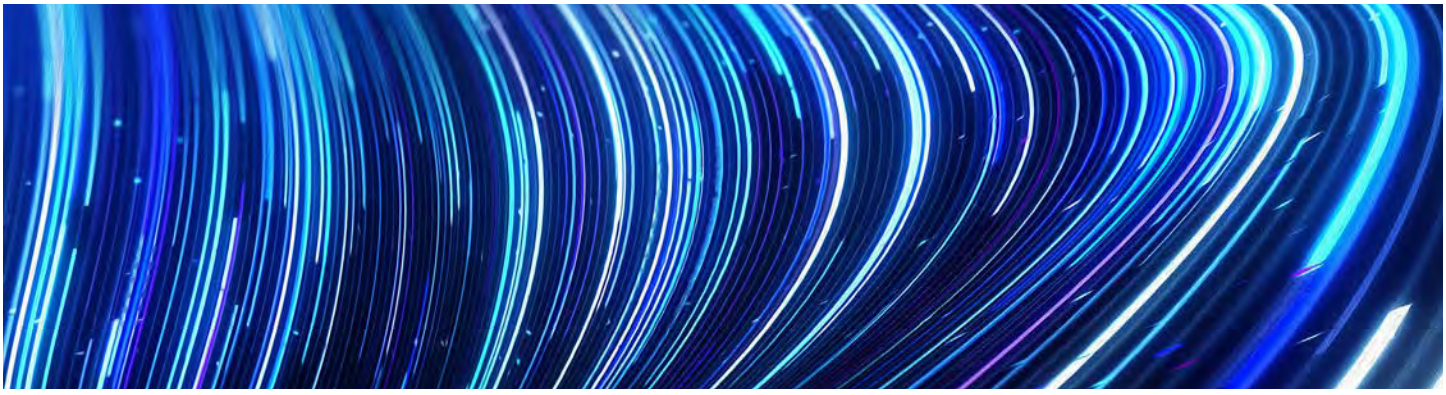
LOW TOTAL COST OF OWNERSHIP

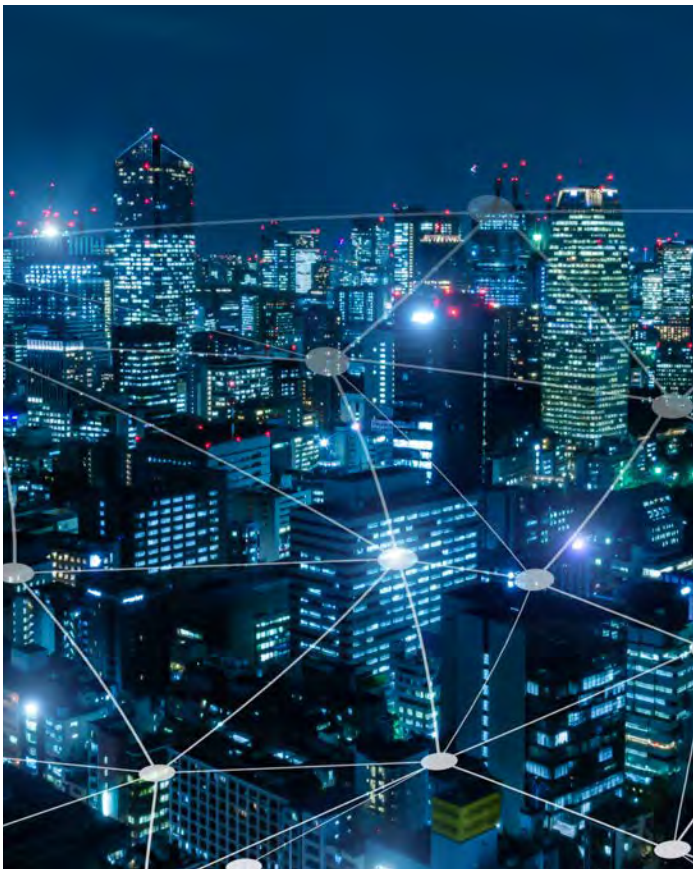
Feature	Description
Low TCO	Features such as simplified deployment, single pane of glass management for both wireless and security, and no need to purchase a separate wireless controller drastically reduce an organization's cost to add wireless into a new or existing network infrastructure.
MiFi Extender	MiFi Extender enables the attachment of a 3G/4G/LTE modem to the SonicWave access point for use as either the primary WAN or as a secondary failover WAN link for business continuity.
Bluetooth Low Energy	SonicWave access points include a Bluetooth Low Energy radio that enables the use of ISM (industrial, scientific and medical) applications for healthcare, fitness, retail beacons, security and home entertainment over a low energy link.
USB port	Access points with USB port supports 3G/4G failover. Plug in a dongle to the port and network continues to function over cellular connection, in case of WiFi network outage.
Green access points	SonicWave access points reduce costs by supporting green access points, which enables both radios to enter sleep mode for power saving when no clients are actively connected. The access point will exit sleep mode once a client attempts to associate with it.

For info on legacy SonicPoint APs, click here.

REGULATORY MODEL NUMBER

432o	APL42-0C1





PARTNER ENABLED SERVICES

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at:

www.sonicwall.com/PES

To try our secure wireless solution, visit:

www.sonicwall.com/products/secure-wireless/live-demo

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL