SonicWave 600 Series Wireless Access Points

Superior Performance in Wireless Solutions

SonicWall's 600 series access points (APs) use 802.11ax - the most advanced technology available - for superior performance in high-density, multi-device environments. In addition to performance, these APs offer a number of additional features that provide an enhanced experience, as well as deliver best-in-class security that you expect from SonicWall.

HIGHLIGHTS

Performance

- 802.11ax
- Increased throughput
- Reduced latency
- Better power management

User experience

- Longer battery life
- Zero-Wait Dynamic Frequency Selection (DFS)
- Neighboring network avoidance
- Target Wake Time (TWT)

Best-in-class wireless security

- WIDS for threat detection
- WIPS for active threat remediation
- Rogue AP and device detection

Intuitive cloud management and monitoring tool

- Integrated Switch management
- Alerts and rich analytics
- Automatic firmware updates
- Integrates with Wireless Network Manager and WiFi Planner
- RF spectrum analysis

Zero-Touch Deployment

- Fast and easy deployment
- Auto-detection and auto-provisioning
- SonicExpress mobile app-compatible

DATASHEET

Performance

SonicWall's SonicWave 600 series access points utilize 802.11ax technology, which provides for improved performance in high-density environments. The use of 1024 QAM allows more data to pass through, and 802.11ax provides improvements in MU-MIMO, with both uplink and downlink capabilities.

Additionally, 802.11ax works in both the 2.4 GHz and 5 GHz bands, and latency is reduced by 75%. The result is overall throughput improvement of up to 400%, with nominal data rate improvement of 37% compared to 802.11ac Wave 2.

Enhanced user experience

SonicWave APs enhance the user experience in a number of ways. Not only are processor speeds faster, but beamforming allows for a more direct connection that is faster and more reliable than without beamforming. Also, improved power control methods help to avoid interference with nearby networks, making for a better experience, and Target Wake Time management allows for longer battery life for mobile devices.

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 patended Real-Time Deep Memory Inspection (RTDMI™) technology. RTDMI blocks zero-day and unknown threats at the gateway – even those that hide via encryption or don't exhibit malicious behavior, using real-time memory-based inspection techniques to force malware to reveal its weaponry into 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.

Most SonicWave APs have a radio 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, wireless packet capture, and zero-wait DFS, which identifies and avoids interference with radar systems while eliminating the wait associated with being booted from one DFS channel and finding another to connect with.

Intuitive cloud management and monitoring tool

Easily set up and deploy APs. SonicWave APs integrate with SonicWall Wireless Network Manager, which is a highly intuitive, scalable, and centralized Wi-Fi network management system capable of delivering rich wireless and switching analytics, powerful features, and simplified onboarding via the cloud with a single pane of glass. The APs also integrate with WiFi Planner, a site survey tool that enables you to optimally design and deploy a wireless network, resulting in a reduced total cost of ownership. With RF spectrum analysis, you can detect and identify the source of RF interference and monitor the health of a wireless system.

Zero-Touch Deployment

Zero-Touch makes it easy to register your unit and onboard SonicWave APs with the help of the 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.

SonicWave 600 Series Specifications

HARDWARE SPECIFICATIONS	SONICWAVE 641	SONICWAVE 681
Location	Indoor	Indoor
Maximum power consumption (W)	23	34
Status indicators	Seven (7) LED (Power, security, BLE, LAN, 5G, 2.4G, WWAN)	
Antennas	8 internal	12 internal
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 (model 641); (1) 100/1000/5.0 GbE auto-sensing RJ-45 for Ethernet (model 681); (1) Micro-USB console; (1) USB 3.0	
5G/4G/LTE USB modem support	Yes	Yes
Accessories included	Ceiling Mounting Kit	Ceiling Mounting Kit
Virtual access points/SSID group	Up to 8 per access point	
Chassis	UL 1024 plenum rated	
Ethernet interface	1 x 2.5GbE	1 x 5GbE
USB 3.0	1	1
Console (micro USB-type)	1	1
Kensington lock hold	Yes	Yes
PoE Power Requirement	802.3at	802.3bt type 3
12V DC Jack	Yes	Yes
Unit Dimensions (cm)	20 x 20 x 3.7	21.3 x 21.3 x 3.9
Shipping Dimensions (cm)	23 x 22.9 x 7.4	26.5 x 24 x 9.5
Unit Weight (kg)	0.85	1.10
WEEE weight (kg)	1.2	1.49
Shipping weight (kg)	1.2	1.49

STANDARDS AND COMPLIANCE	SONICWAVE 641	SONICWAVE 681
IEEE Standards	802.11ax, 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, WPA3, WPA2, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w	
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) 641 MU-MIMO 8x8 (8 streams) 681	
Max/Recommended connected clients per radio	256/150	
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union	
USB WAN failover and load balancing	Yes	Yes

ENVIRONMENTAL	SONICWAVE 641	SONICWAVE 681
Temperature range	32 to 104°F, 0 to 40°C	32 to 104°F, 0 to 40°C
Humidity	10 - 95%, non-condensing	

RADIO SPECIFICATIONS	SONICWAVE 641	SONICWAVE 681
Radio 1: 2.4GHz	11ax 4x4	11ax 4x4
Radio 2: 5GHz	11ax 4x4	11ax 8x8
Radio 3: Scanning radio (dual-band selectable)	11ac 1x1	11ac 1x1
Radio 4: 2.4GHz BLE/BT 5.0	Yes	Yes
Antenna Type	Internal	Internal
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	Regulatory and Country Code compliant	
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, 802.11ax: update to 1147.5 Mbps (Radio 1) and 4804 Gbps (Radio 2)	
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), 802.11ax: Orthogonal Frequency-Division Multiple Access (OFDMA)	

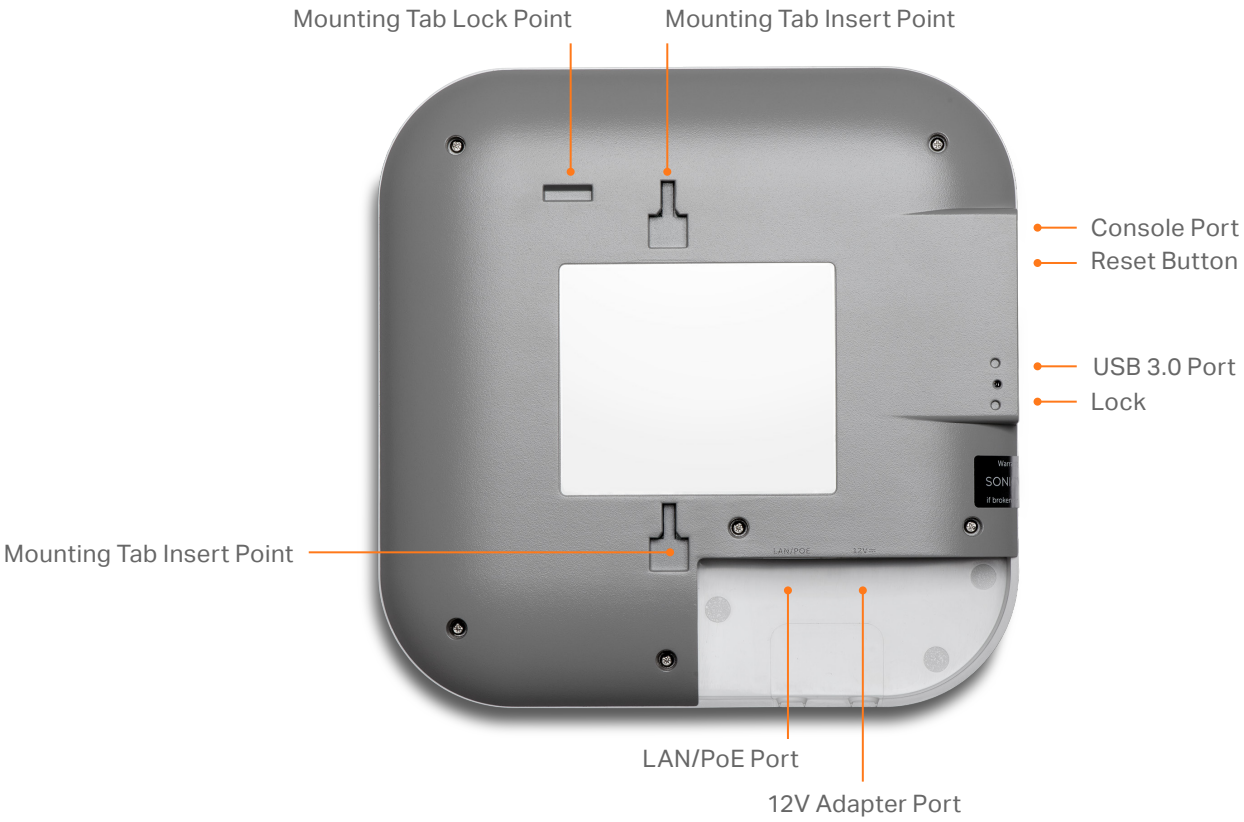
SECURITY	SONICWAVE 641	SONICWAVE 681
Data Encryption	WPA3, WPA2, IPSec, 802.11i, AES, SSL VPN**	
SSL-VPN Client*	NetExtender, Connect Tunnel	
Advanced Security Services	Capture ATP, CFS, Geo-IP, Botnet, Anti-virus (Cloud)	

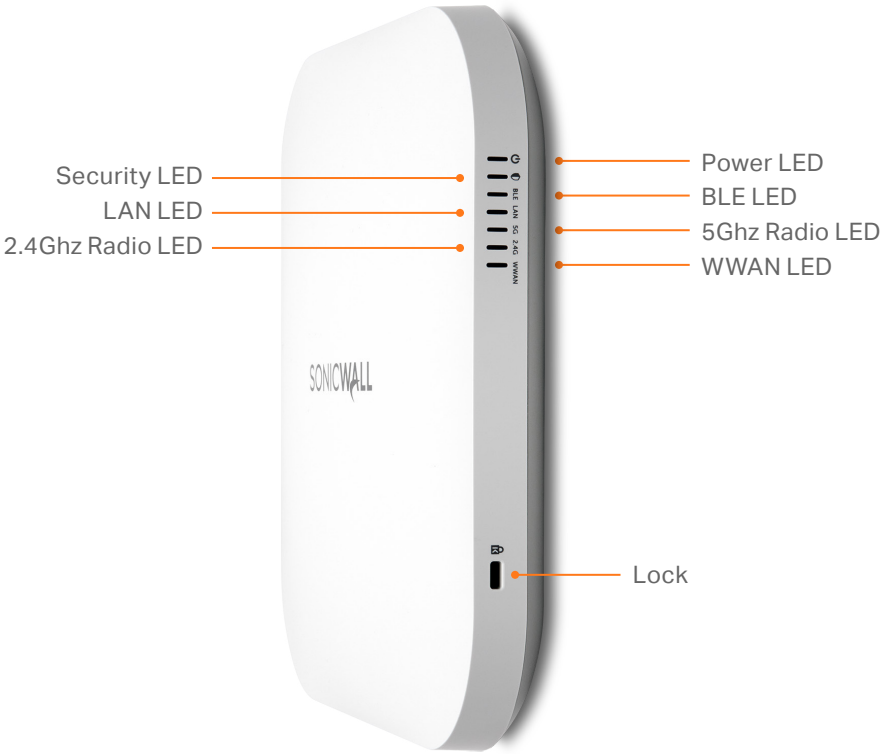
AUTHENTICATION	SONICWAVE 641	SONICWAVE 681
Authentication	RADIUS, Active Directory, single sign-on (SSO), local user	
Captive Portal	Click-through, external server, social account (Facebook, Google, Twitter, and LinkedIn) sign-on	
Captive Portal Sign On	Local users, RADIUS, LDAP, OTP, AD	

REPORTING	SONICWAVE 641	SONICWAVE 681
Alerts	Critical alert notification via SMS	

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

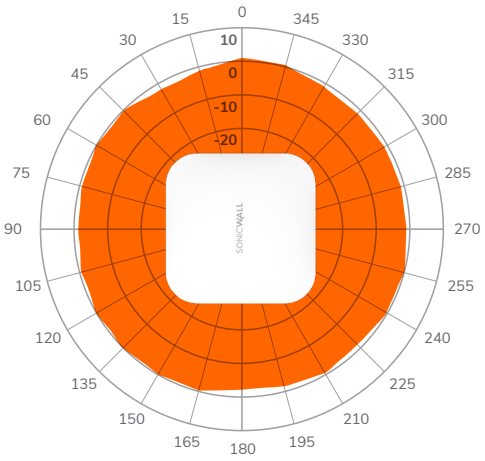
SonicWave 641



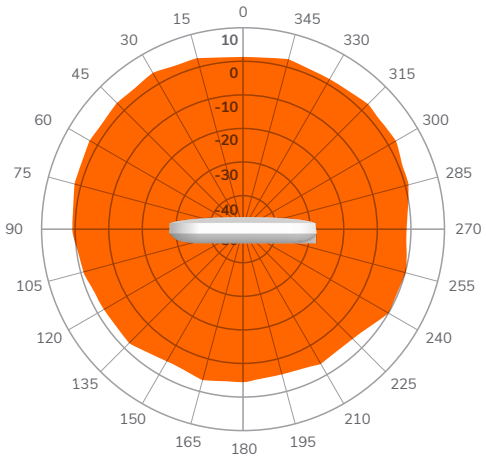


Antenna Radiation Patterns

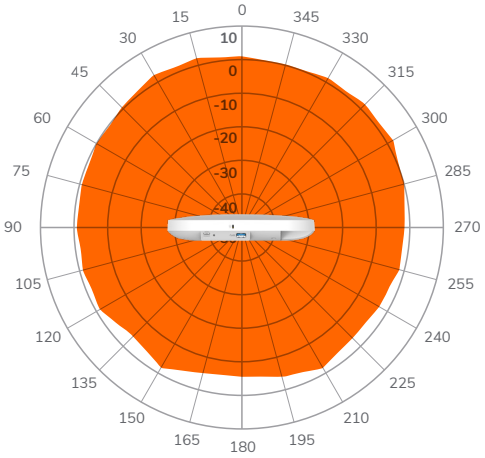
2.4 GHz, XY-Plane



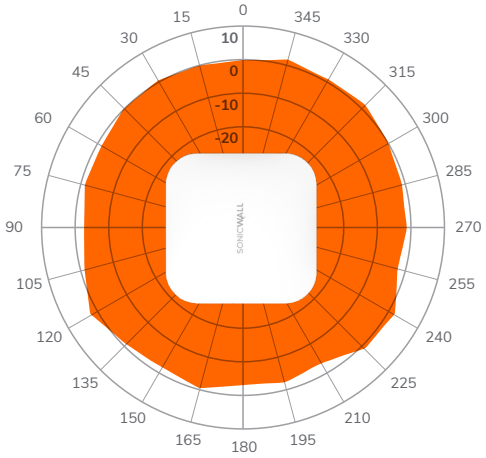
2.4GHz, XZ-Plane



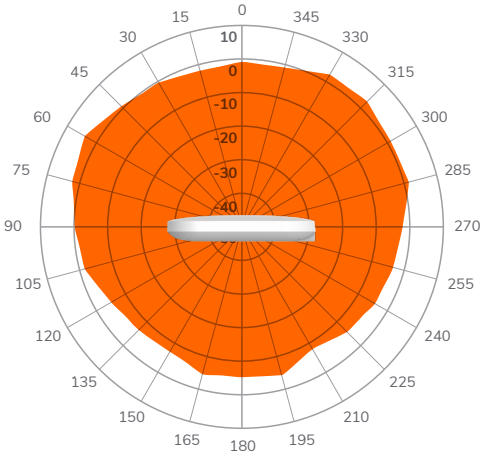
2.4GHz, YZ-Plane



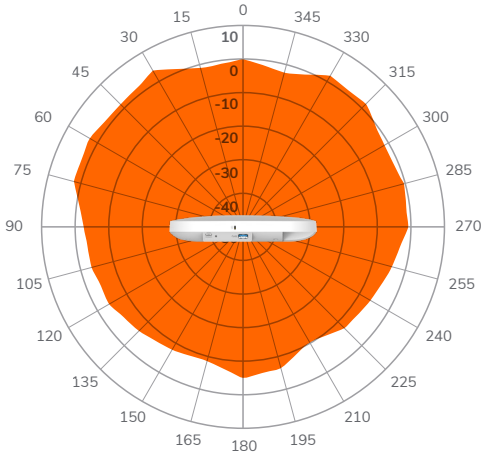
5GHz, XY-Plane



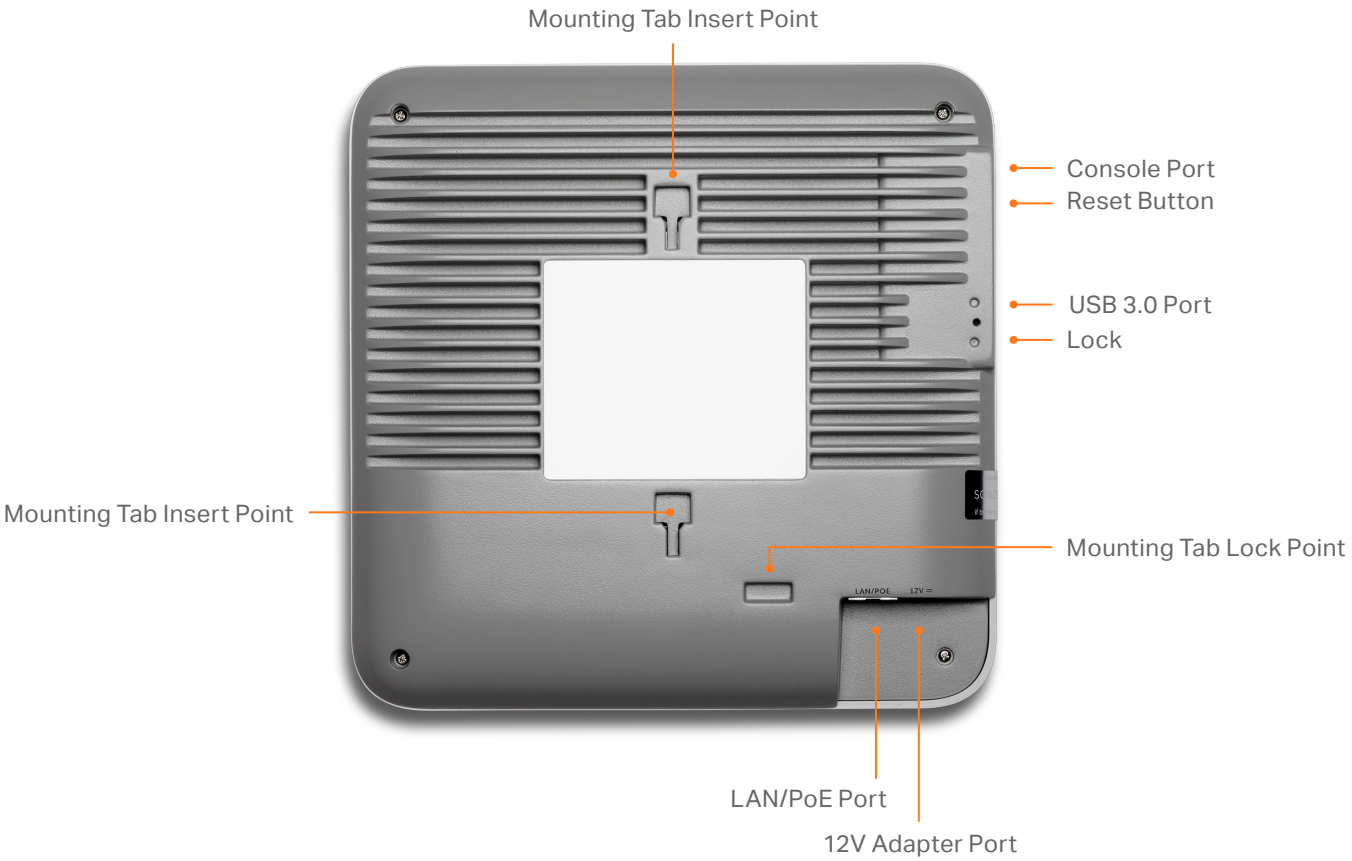
5GHz, XZ-Plane



5GHz, YZ-Plane



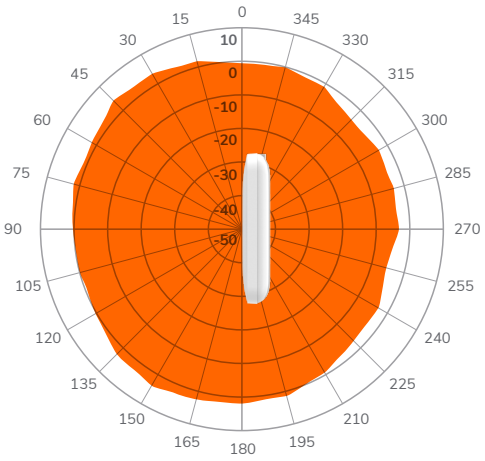
SonicWave 681



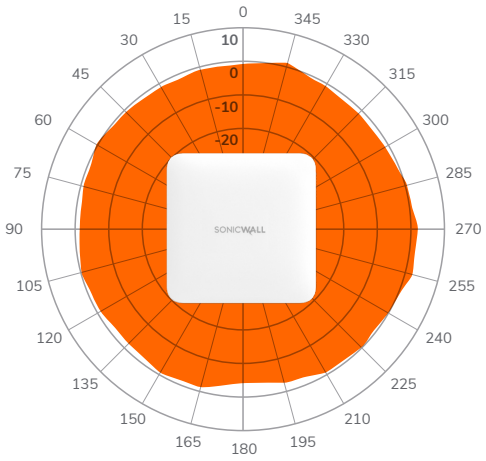
SonicWave 681

Antenna Radiation Patterns

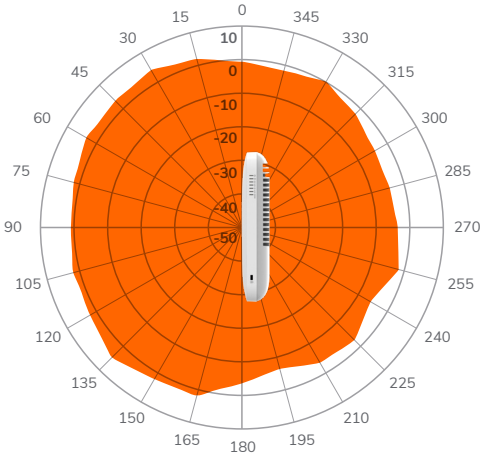
2.4 GHz, XY-Plane



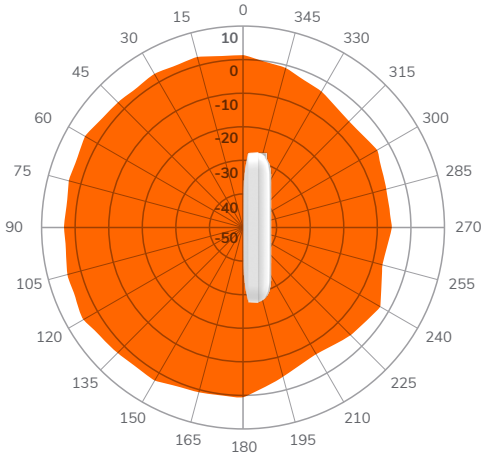
2.4GHz, XZ-Plane



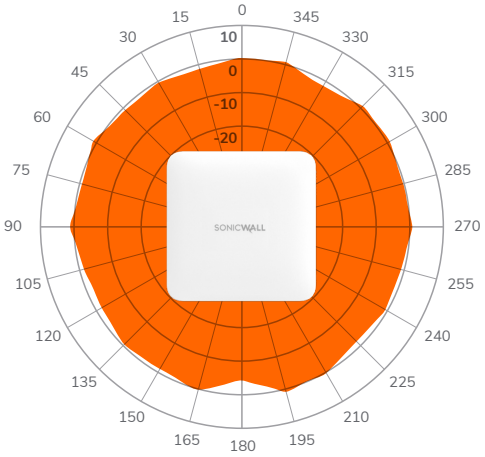
2.4GHz, YZ-Plane



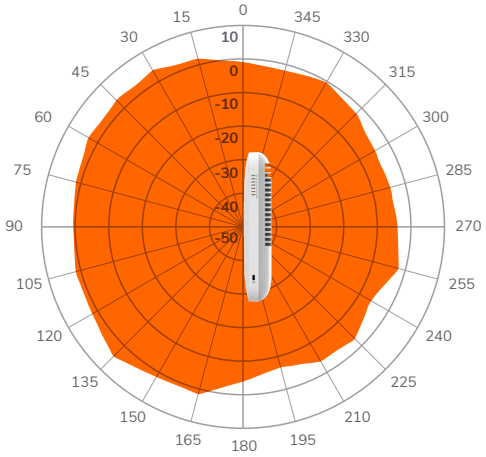
5GHz, XY-Plane



5GHz, XZ-Plane



5GHz, YZ-Plane



SonicWave Feature Summary

SUPERIOR USER EXPERIENCE	
Feature	Description
High-speed wireless performance and range	Optimal Wi-Fi network performance truly relies less on the PHY (physical) data rate of the chipset or standard used. Wi-Fi networks that are properly designed afford users the highest throughput their clients can utilize.
Enhanced signal quality	The 802.11ax standard operates in both the 2.4 GHz and 5 GHz bands.
Increased wireless reliability	The increase in bandwidth capacity and greater number of spatial streams combined with MU-MIMO and the improved processing offered by 802.11ax result in more reliable wireless coverage.
Target Wake Time	Enables devices to determine when and how frequently they will take up to send or receive data, resulting in longer battery life for mobile devices.
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.
Tx and Rx 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 network enables devices in the network to have faster speeds and greater coverage.
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	SonicWave 600 series access points include a dedicated radio 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 802.11ax 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.

COMPREHENSIVE WIRELESS SECURITY

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.
Wi-Fi Planner	To optimize access point placement before deployment, the Wi-Fi planning tool 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/ax, 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.
Mi-Fi extender	Mi-Fi 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 Wi-Fi network outage.
Green access points	SonicWave access points reduce costs by supporting green access points, which enable 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.

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®