

# Wireless-Access-Points der SonicWave 600 Series

Höchste Leistung für Wireless-Lösungen

Die Wireless-Access-Points (APs) der 600 Series von SonicWall nutzen mit 802.11ax die modernste Technologie auf dem Markt und liefern so eine überragende Performance in komplexen Umgebungen mit mehreren Geräten. Diese extrem sicheren APs können via Cloud mit dem SonicWall Wireless Network Manager (WNM) oder über die SonicWall-Firewalls verwaltet werden und bieten eine Reihe zusätzlicher Funktionen für eine verbesserte Erfahrung. Dabei genießen Sie die erstklassige Sicherheit, die Sie von SonicWall erwarten.



## HIGHLIGHTS

### Leistung

- 802.11ax
- Erhöhter Durchsatz
- Verringerte Latenz
- Bessere Energieverwaltung

### Benutzererfahrung

- Längere Akkulaufzeit
- Abschirmung von benachbarten Netzwerken
- Target Wake Time (TWT)

### Erstklassige Sicherheit für Wireless-Anwendungen

- WIDS zur Bedrohungserkennung
- WIPS zur aktiven Bedrohungsbehebung
- Erkennung unberechtigter APs und Geräte

### Intuitives Tool für Cloud-Management und Überwachung

- Integriertes Switch-Management
- Warnmeldungen und umfassende Analysen
- Automatische Firmware-Updates
- Integration mit Wireless Network Manager und WiFi Planner
- Analyse des HF-Spektrums

### Vollautomatische Implementierung

- Schnelle und einfache Implementierung
- Automatische Erkennung und Bereitstellung
- Kompatibel mit der mobilen App „SonicExpress“

## Leistung

Die Access-Points der SonicWave 600 Series von SonicWall sind dank 802.11ax-Technologie optimal für komplexe Umgebungen geeignet und sorgen für eine höhere Performance. Durch 1024 QAM ist ein höherer Datendurchsatz möglich, und 802.11ax sorgt für Verbesserungen bei MU-MIMO, sowohl für Uplink als auch Downlink.

Darüber hinaus unterstützt 802.11ax sowohl das 2,4-GHz- als auch das 5-GHz-Band. Tests haben gezeigt, dass 802.11ax im Vergleich zu 802.11ac Wave 2 die Latenz um 75 % reduzieren, den Gesamtdurchsatz um bis zu 4-mal steigern und die Nenndatenrate um bis zu 37 % optimieren kann.

## Hoher Benutzerkomfort

Die Benutzer profitieren in vielfältiger Weise von den neuen SonicWave-Features und -APs. Dazu zählt neben schnelleren Prozessoren auch das Beamforming, mit dem schnellere und zuverlässigere Verbindungen erreicht werden. Verbesserte Methoden zur Leistungsregulierung verhindern Interferenzen mit benachbarten Netzwerken und damit Störungen für die Benutzer. Zusätzlich schont die Target Wake Time die Akkus von Mobilgeräten.

## Erstklassige Sicherheit für Wireless-Anwendungen

Die meisten SonicWave-Access-Points haben eine Funkeinheit eigens für die Sicherheit, die unberechtigte APs erkennt, passive Scans durchführt und Pakete erfasst.

SonicWave bietet auch zusätzliche Sicherheitsfeatures wie die Erkennung und Vermeidung von Wireless-Angriffen, die Segmentierung mithilfe virtueller APs, Wireless Guest Services, HF-Überwachung und die Erfassung von Wireless-

Paketen. SonicWave-APs verfügen außerdem über DFS ohne Wartezeit, womit eventuelle Interferenzen mit Radarsystemen erkannt und vermieden werden können. Dabei entfällt die Wartezeit, die normalerweise anfällt, wenn von einem DFS-Kanal aus gestartet wird und ein weiterer für den Verbindungsaufbau gesucht werden muss.

## Intuitives Tool für Cloud-Management und Überwachung

SonicWave-APs können unkompliziert eingerichtet und implementiert werden. Sie sind mit dem SonicWall Wireless Network Manager kompatibel, einem überaus intuitiven und skalierbaren zentralen Verwaltungssystem für WLAN-Netzwerke. Es liefert umfassende Analysen zu Wireless und Switching und ermöglicht ein vereinfachtes Onboarding mit einer zentralen Konsole über die Cloud. Die APs lassen sich außerdem mit WiFi Planner integrieren, einem Site-Survey-Tool, mit dem Sie kabellose Netzwerke optimal planen und implementieren können. Dadurch können Sie die Gesamtbetriebskosten niedrig halten. Schließlich profitieren Sie noch von der Analyse des HF-Spektrums, mit der Sie die Quelle von HF-Interferenzen aufspüren und den Zustand des Wireless-Systems überwachen können.

## Vollautomatische Implementierung

Die vollautomatische Implementierung erleichtert Ihnen die Registrierung Ihrer Einheit und das Onboarding von SonicWave-APs über die mobile App „SonicExpress“ von SonicWall. Die APs werden mithilfe vollautomatischer Implementierung erkannt und bereitgestellt. Mit der für iOS und Android erhältlichen App „SonicExpress“ können Netzwerkadministratoren Netzwerke von überall überwachen und verwalten.



## SonicWave 600 Series – Systemdaten

HARDWARE	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Ort	Indoor	Indoor	Indoor
Maximaler Stromverbrauch (W)	21	23	34
Statusanzeigen	Sieben (7) LEDs (Betriebsanzeige, Sicherheit, BLE, LAN, 5G, 2,4G, WWAN)		
Antennen	4 intern	8 intern	12 intern
LAN-Anschlüsse	(1) 100-/1.000-/2,5-GbE-Autosensing-RJ-45 für Ethernet und Power over Ethernet (PoE) (Modell 621/641); (1) 100-/1.000-/5,0-GbE-Autosensing-RJ-45 für Ethernet und Power over Ethernet (PoE) (Modell 681); (1) Mikro-USB-Konsole; (1) USB 3.0		
Unterstützung für USB-Modem (5G/4G/LTE)	Ja	Ja	Ja
Im Lieferumfang enthaltenes Zubehör	Kit für Deckenhalterung	Kit für Deckenhalterung	Kit für Deckenhalterung
Virtuelle Access-Points / SSID-Gruppe	Bis zu 8 pro Access-Point		
Gehäuse	UL 1024, feuerfest		
Ethernet-Schnittstelle	1 x 2,5-GbE	1 x 2,5-GbE	1 x 5-GbE
USB 3.0	1	1	1
Konsole (Micro-USB)	1	1	1
Kensington-Schlosshalterung	Ja	Ja	Ja
Anforderungen an die PoE-Stromversorgung	802.3at	802.3at	802.3bt Art 3
12 V DC, Klinke	Ja	Ja	Ja
Produktmaße (cm)	17,4 x 17,4 x 3	20 x 20 x 3,7	21,3 x 21,3 x 3,9
Versandmaße (cm)	23 x 22,9 x 7,4	23 x 22,9 x 7,4	26,5 x 24 x 9,5
Produktgewicht (kg)	0,68	0,85	1,10
WEEE-Gewicht (kg)	0,79	1,2	1,49
Versandgewicht (kg)	1,27	1,2	1,49

STANDARDS UND RICHTLINIEN	SONICWAVE 621	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		
Richtlinien	FCC/ICES Klasse B, CE, RCM/ACMA, VCCI Klasse B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europa/China), WEEE		
Sicherheitszertifizierungen	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 oder EN 62368-1, IEC 60950-1, IEC 62368-1, Europa: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1		
Zulassungen für Funkeinheiten	USA: FCC Part 15C, 15E, Kanada: ISSED RSS-247, Europa: (RED) EN 300 328, EN 301 893, Aus./NZ: AS/NZs 4268, Taiwan: NCC LP002, zusätzliche nationale Zulassungen für Japan, Korea, China, Indien, Brasilien		
EMI-Zulassungen	USA: FCC P15B, Kanada: ICES-003, Europa: EN 301 489-1, -17, EN 55032, EN 55024, Aus./NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438		
Genehmigungen Strahlenbelastung	USA: FCC Part 2, Kanada: RSS-102, Europa: EN 50385, Aus./NZ: ASNZS 2772		
MIMO	MU-MIMO 2x2 (2 Streams) 621 MU-MIMO 4x4 (4 Streams) 641 MU-MIMO 8x8 (8 Streams) 681		
Max./Empfohlene Anzahl verbundener Clients pro Funkeinheit	256/150		
Sicherheit	UL, cUL, TÜV/GS, CB, CE, BSMI, Mexico CoC, Customs Union		
USB-WAN-Failover und Lastverteilung	Ja	Ja	Ja

UMGEBUNGSBEDINGUNGEN	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Temperaturbereich	0 bis 40 °C		
Luftfeuchtigkeit	10–95 %, nicht kondensierend		

<b>FUNKDATEN</b>	<b>SONICWAVE 621</b>	<b>SONICWAVE 641</b>	<b>SONICWAVE 681</b>
Funkeinheit 1: 2,4 GHz	11ax 2x2	11ax 4x4	11ax 4x4
Funkeinheit 2: 5 GHz	11ax 2x2	11ax 4x4	11ax 8x8
Funkeinheit 3: Funkeinheit zur Paketprüfung (Dualband wählbar)	11ac 1x1	11ac 1x1	11ac 1x1
Funkeinheit 4: 2,4 GHz BLE/BT 5.0	Ja	Ja	Ja
Antennentyp	Intern	Intern	Intern
Frequenzbänder	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		
Verwendete Kanäle	802.11a: USA und Kanada 12, Europa 11, Japan 4, Singapur 4, Taiwan 4, 802.11b/g: USA und Kanada 1–11, Europa 1–13, Japan 1–14 (Kanal 14 nur nach 802.11b-Standard), 802.11n (2,4 GHz): USA und Kanada 1–11, Europa 1–13, Japan 1–13, 802.11n (5 GHz): USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64, 802.11ac: USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64		
Sendeleistung	Entspricht gesetzlichen Richtlinien und den landesspezifischen Bestimmungen		
Steuerung der Sendeleistung	Unterstützt		
Unterstützte Datenübertragungsraten	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 MBit/s pro Kanal, 802.11b: 1, 2, 5, 5 und 11 MBit/s pro Kanal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 MBit/s pro Kanal, 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 MBit/s pro Kanal, 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, 1.040, 1.170, 1.300, 1.560, 1.733,4 MBit/s pro Kanal, 802.11ax: Update auf 1.147,5 MBit/s (Funkeinheit 1) und 4,804 GBit/s (Funkeinheit 2)		
Modulationstechnologie/ Frequenzspreizung	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)		

<b>SICHERHEIT</b>	<b>SONICWAVE 621</b>	<b>SONICWAVE 641</b>	<b>SONICWAVE 681</b>
Datenverschlüsselung	WPA3, WPA2, IPSec, 802.11i, AES, SSL-VPN**		
SSL-VPN-Client*	NetExtender, Connect Tunnel		
Erweiterte Sicherheitsdienste	Capture ATP, CFS, Geo-IP, Botnet, Antivirus (Cloud)		

<b>AUTHENTIFIZIERUNG</b>	<b>SONICWAVE 621</b>	<b>SONICWAVE 641</b>	<b>SONICWAVE 681</b>
Authentifizierung	RADIUS, Active Directory, Single-Sign-on (SSO), lokaler Benutzer		
Captive Portal	Anmeldung über Click-through, externen Server, Social Media (Facebook, Google, Twitter, LinkedIn)		
Captive-Portal-Anmeldung	Lokale Benutzer, RADIUS, LDAP, OTP, AD		

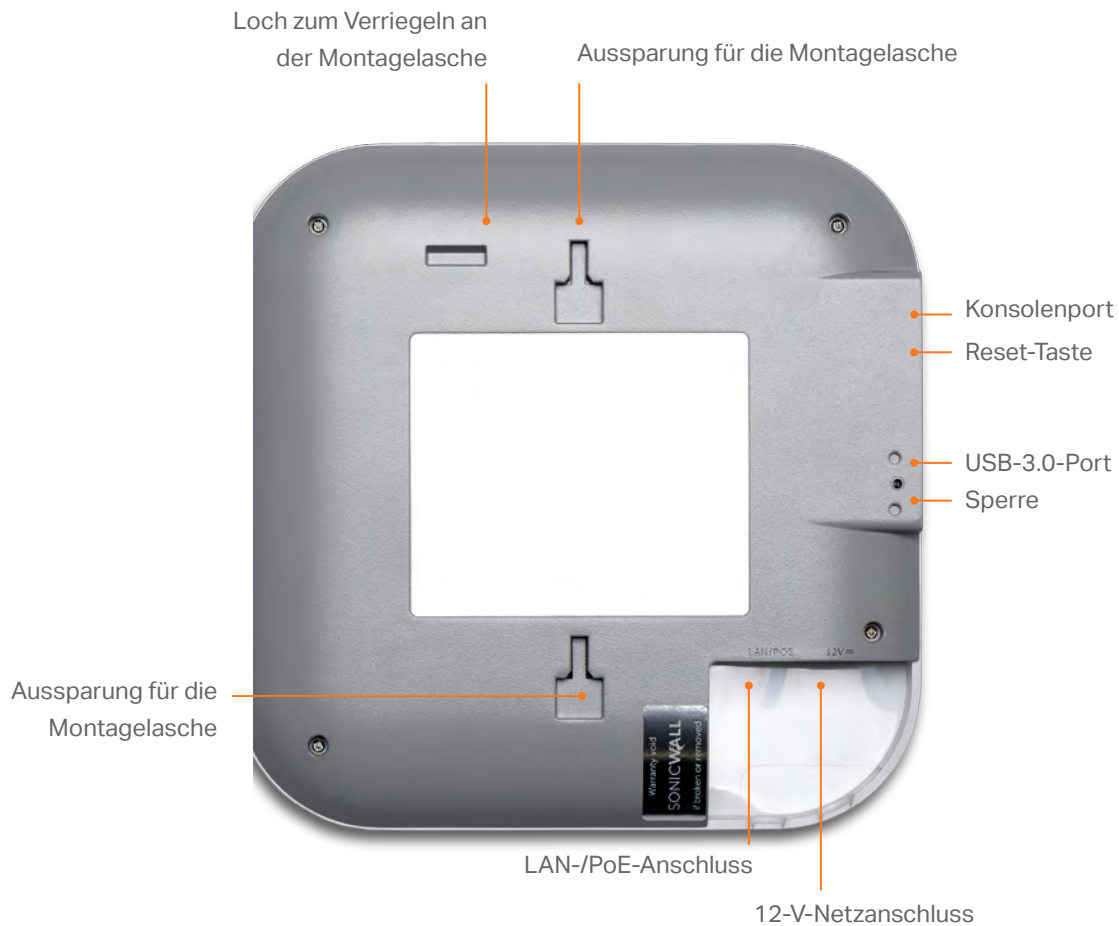
<b>REPORTING</b>	<b>SONICWAVE 621</b>	<b>SONICWAVE 641</b>	<b>SONICWAVE 681</b>
Warnmeldungen	Dringende Warnmeldungen per SMS		

\* SonicWave ist ein SSL-VPN-Client.

\*\* Bei Einsatz mit einer SonicWall-Appliance der Secure Mobile Access Series.

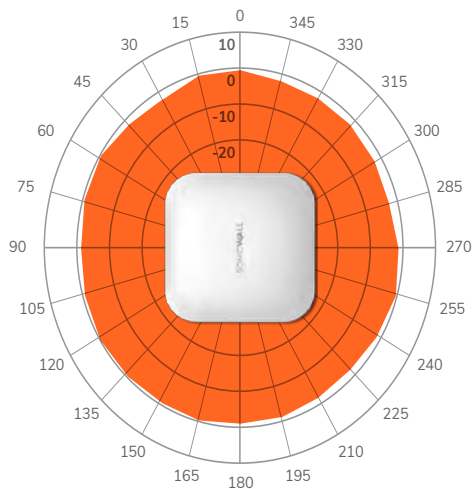


## SonicWave 621

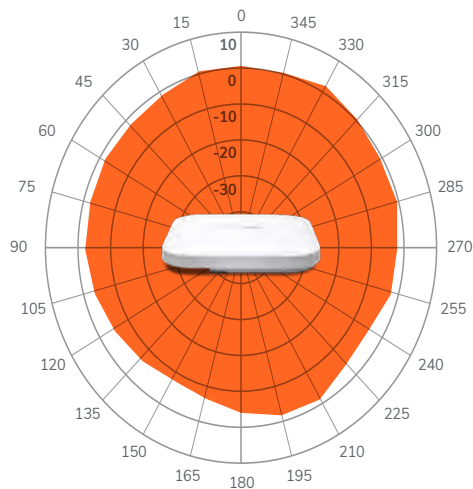


Antennencharakteristik

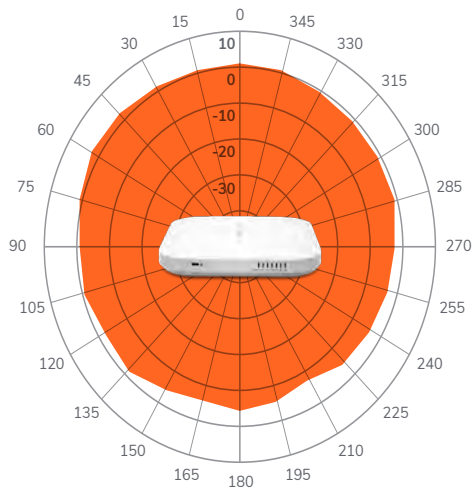
2,4 GHz, XY-Ebene



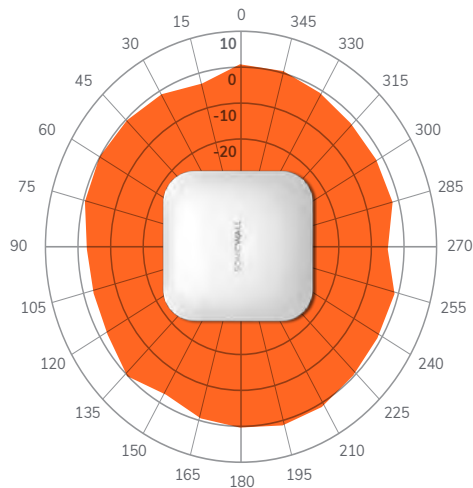
2,4 GHz, XZ-Ebene



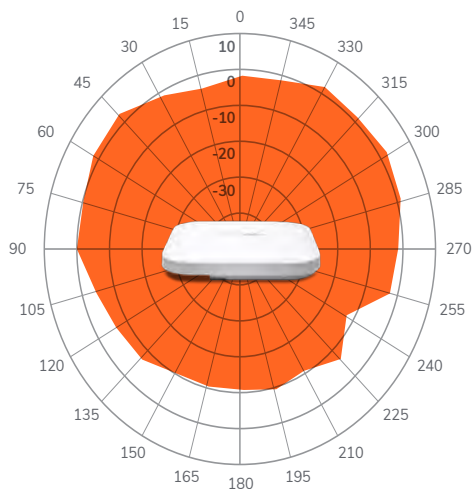
2,4 GHz, YZ-Ebene



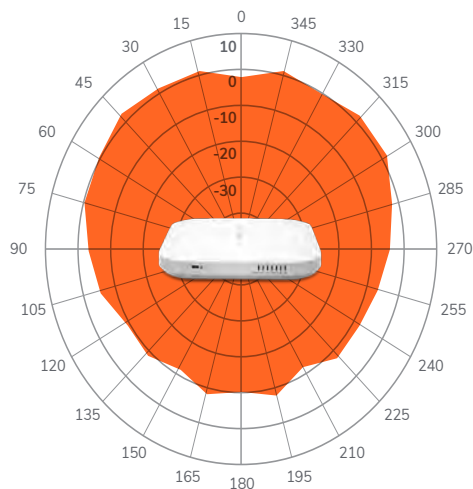
5 GHz, XY-Ebene



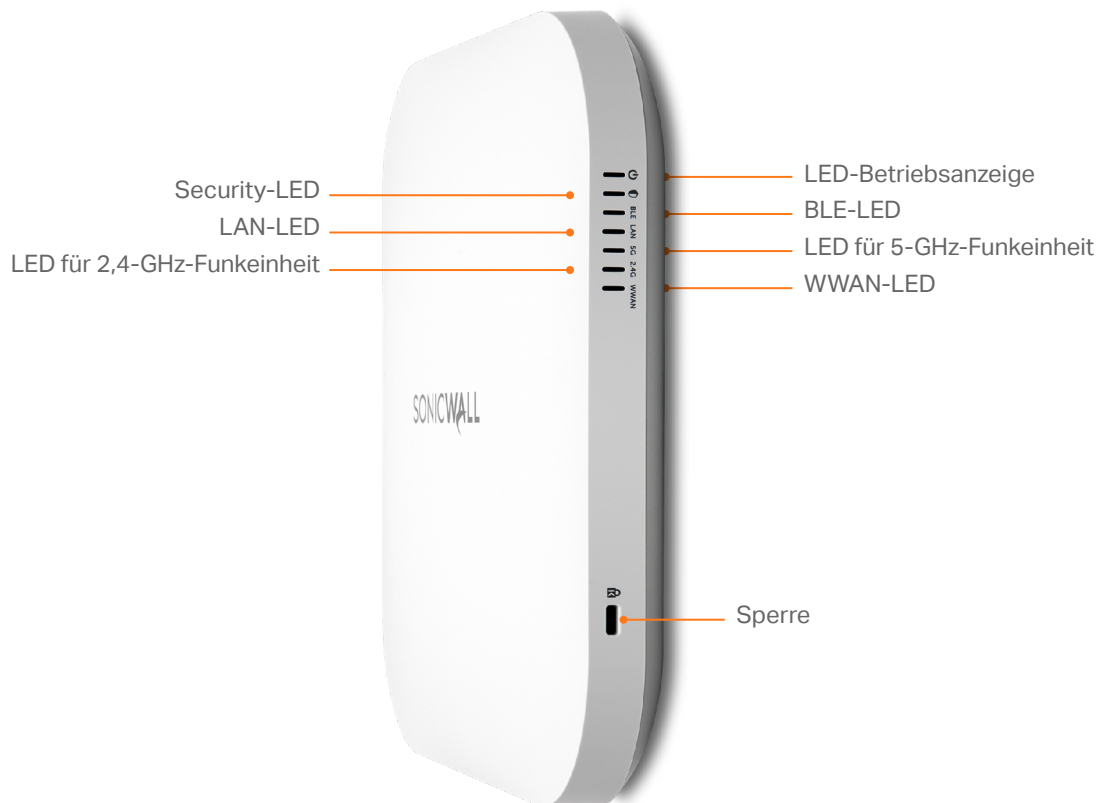
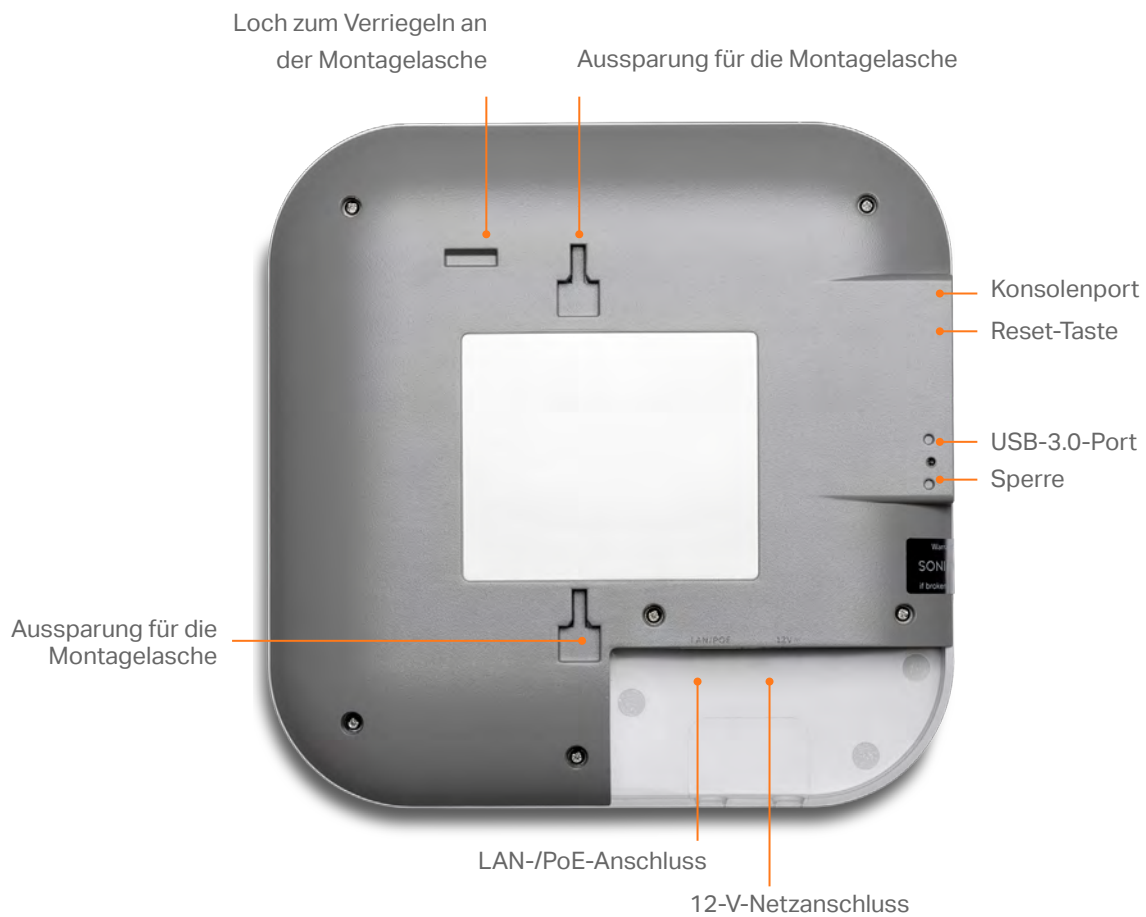
5 GHz, XZ-Ebene



5 GHz, YZ-Ebene

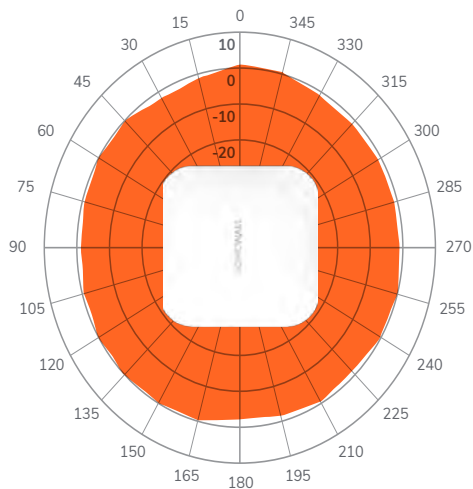


## SonicWave 641

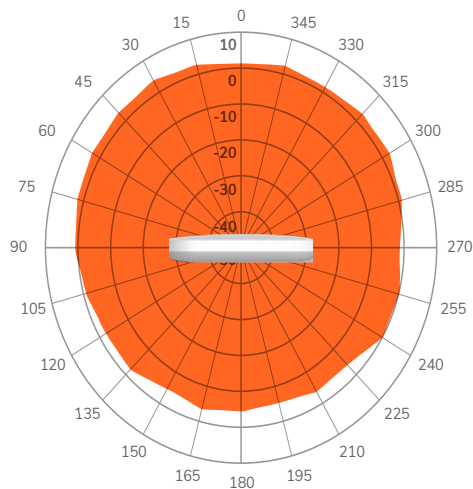


Antennencharakteristik

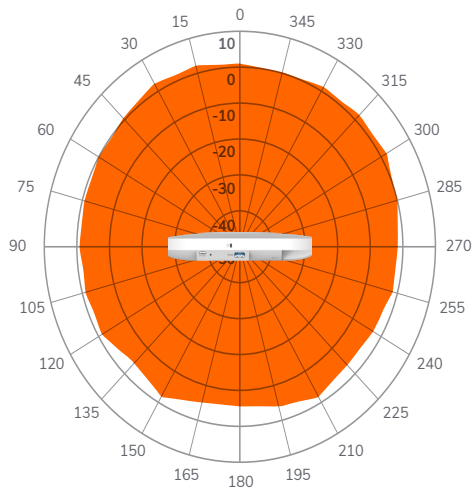
2,4 GHz, XY-Ebene



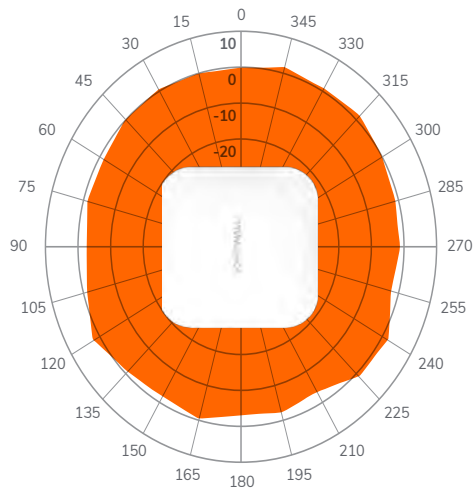
2,4 GHz, XZ-Ebene



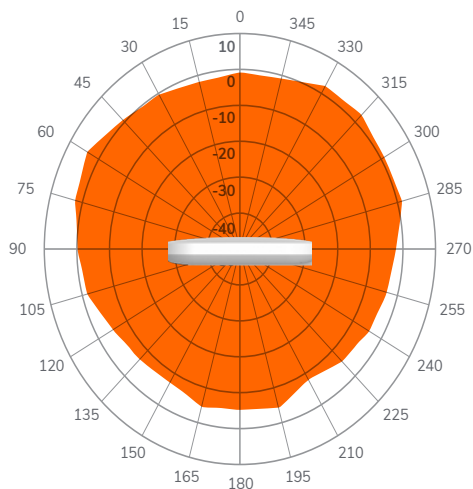
2,4 GHz, YZ-Ebene



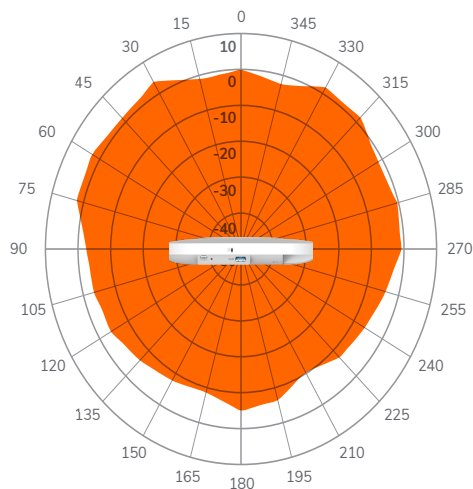
5 GHz, XY-Ebene



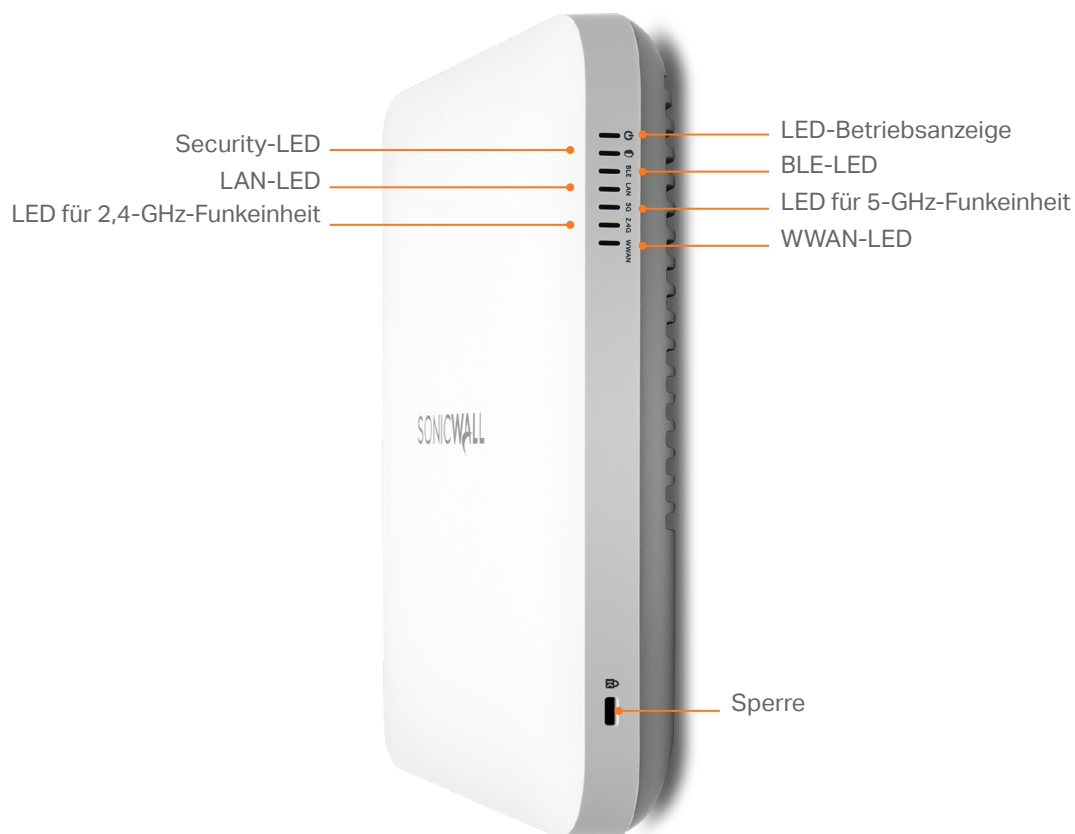
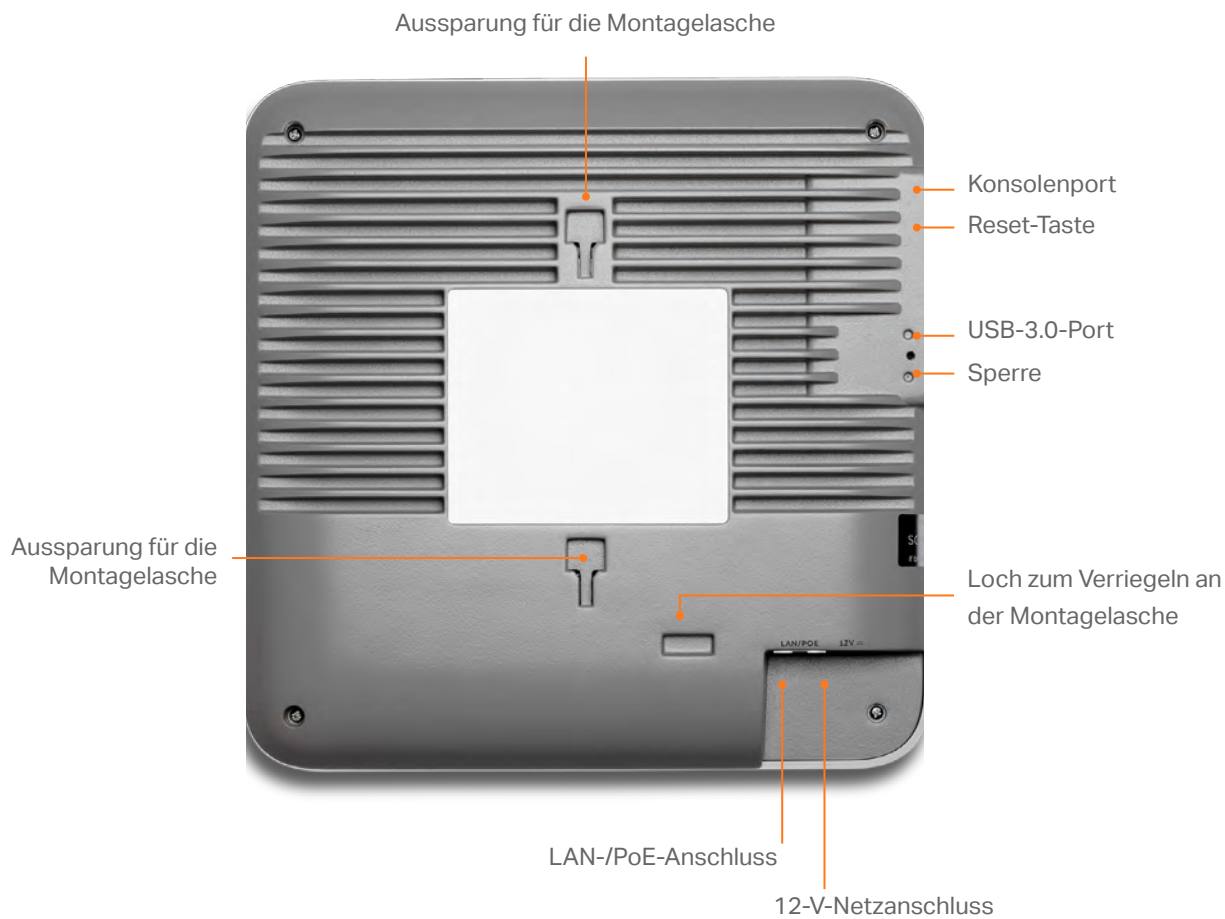
5 GHz, XZ-Ebene



5 GHz, YZ-Ebene

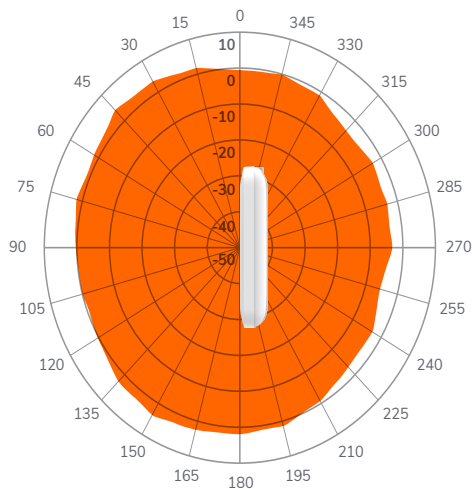




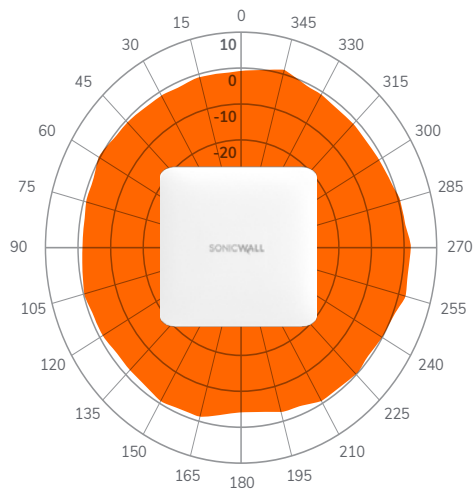


Antennencharakteristik

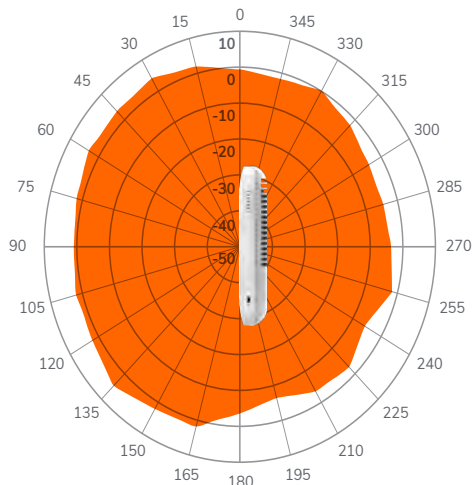
2,4 GHz, XY-Ebene



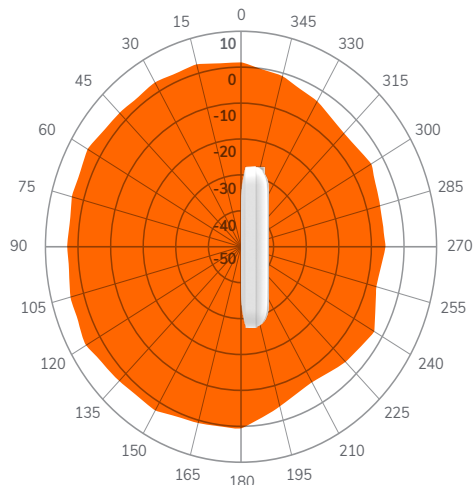
2,4 GHz, XZ-Ebene



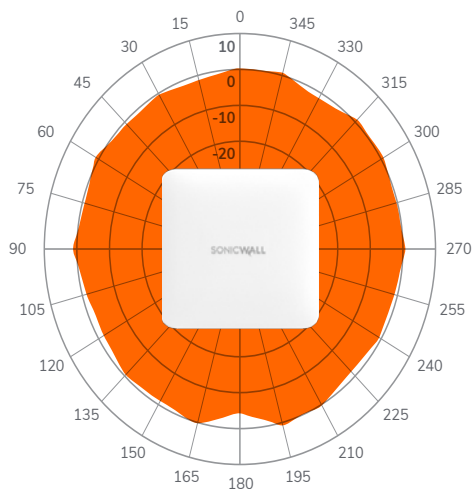
2,4 GHz, YZ-Ebene



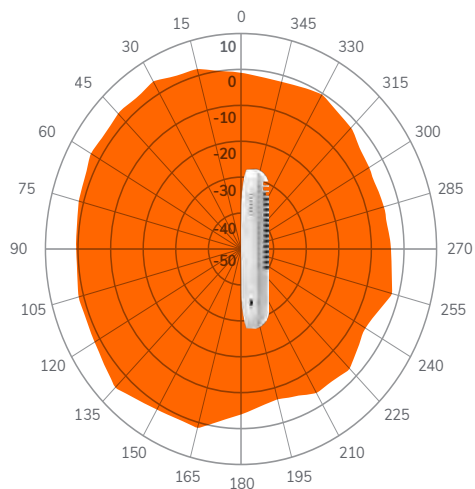
5 GHz, XY-Ebene



5 GHz, XZ-Ebene



5 GHz, YZ-Ebene



## Die SonicWave-Funktionen im Überblick

ÜBERRAGENDE BENUTZERERFAHRUNG	
Funktion	Beschreibung
Highspeed-Wireless-Performance und -Reichweite	Die WLAN-Netzwerkperformance hängt von der PHY-Datenrate (physikalische Schicht) des genutzten Chipsatzes bzw. Standards ab. In einem optimal gestalteten WLAN-Netzwerk genießen die Benutzer den größtmöglichen Durchsatz, den ihre Clients nutzen können.
Bessere Signalqualität	Der 802.11ax-Standard arbeitet sowohl mit dem 2,4-GHz-Band als auch mit dem 5-GHz-Band.
Verbesserte Wireless-Zuverlässigkeit	Die verbesserte Bandbreiten-Kapazität und die größere Menge räumlicher Streams in Verbindung mit MU-MIMO und der optimierten Datenverarbeitung durch 802.11ax sorgen für eine zuverlässigere Drahtlos-Netzabdeckung.
Target Wake Time	Durch Target Wake Time können Geräte selbst bestimmen, wann und wie oft sie sich aktivieren, um Daten zu senden bzw. zu empfangen. Dadurch halten die Akkus von mobilen Geräten länger.
MU-MIMO	Die MU-MIMO-Technologie (Multi-User, Multiple-Input, Multiple-Output) ermöglicht eine Übertragung vom Access-Point an mehrere Wireless-Clients gleichzeitig (und nicht nur an einen).
Bandsteering	Durch Bandsteering werden Dual-Band-Clients automatisch mit dem weniger belasteten 5-GHz-Frequenzband verbunden, während das 2,4-GHz-Frequenzband für veraltete Clients verwendet wird. Auf diese Weise wird die Benutzererfahrung deutlich verbessert.
Tx- und Rx-Beamforming	Beamforming verbessert die Wireless-Performance und -Reichweite durch die gezielte Ausrichtung des Funksignals auf einen einzelnen Client, anstatt die Datenübertragung gleichmäßig in alle Richtungen zu verteilen.
Airtime-Fairness	Airtime-Fairness teilt die Übertragungszeit gleichmäßig unter den verbundenen Clients auf und stellt sicher, dass schnellere Clients in derselben Zeit einen höheren Datendurchsatz erreichen als langsamere Clients.
Wireless Mesh (nur Client-Modus)	Ein Wireless-Mesh-Netzwerk bietet höhere Geschwindigkeiten und besseren Schutz für Geräte im Netzwerk.
FairNet-Wireless-Bandbreitenzuordnung	FairNet garantiert jedem Wireless-Client eine Mindestbandbreite, um zu verhindern, dass einzelne Benutzer überproportional viel Bandbreite beanspruchen.

UMFASSENDE WIRELESS-SICHERHEITSFUNKTIONEN	
Funktion	Beschreibung
Dritte Funkeinheit speziell zur Prüfung von Paketen	Die SonicWave-Access-Points der 600 Series umfassen eine spezielle Funkeinheit, die den drahtlosen Datenverkehr kontinuierlich auf unberechtigte Access-Points prüft und zusätzliche Sicherheitsfunktionen bietet, die die Einhaltung der PCI-Compliance fördern.
Erkennung und Vermeidung von Wireless-Angriffen	Im Rahmen der Erkennung und Vermeidung von Wireless-Angriffen wird das Wireless-Netzwerk auf unautorisierte (unberechtigte) Access-Points überprüft.
Wireless Guest Services	Mit Wireless Guest Services können Administratoren Gastbenutzern einen Zugriff nur für das Internet gewähren. Dieser Zugriff ist vom internen Zugriff getrennt. Gastbenutzer müssen sich sicher an einem virtuellen Access-Point authentifizieren, bevor sie einen Zugriff erhalten.
Lightweight Hotspot Messaging	Lightweight Hotspot Messaging erweitert das SonicWall Wireless Guest Services-Modell des differenzierten Internetzugriffs für Gastbenutzer und erlaubt so eine umfassende Personalisierung der Authentifizierungsfläche und eine Nutzung beliebiger Authentifizierungsverfahren.
Captive Portal	Captive Portal veranlasst Benutzergeräte dazu, eine Seite aufzurufen und sich über einen Webbrowser zu authentifizieren, bevor ein Internetzugang bereitgestellt wird.
Segmentierung mithilfe virtueller Access-Points	Administratoren können bis zu acht SSIDs auf demselben Access-Point mit eigenen Authentifizierungs- und Datenschutzeinstellungen erstellen. Dies ermöglicht eine logische Segmentierung des sicheren drahtlosen Netzwerkverkehrs und einen sicheren Kundenzugriff.
Cloud-Zugriffssteuerungsliste	Als Ergänzung zur lokalen ACL wird eine Cloud-ACL eingesetzt und über einen zentralisierten RADIUS-Server in der Cloud verwaltet. Dies löst Skalierbarkeitsprobleme mit der lokalen ACL und ermöglicht Organisationen die Konfiguration von Authentifizierungskonten basierend auf ihren spezifischen Anforderungen. Zusätzlich lässt sich eine MAC-Authentifizierung auf allen Wi-Fi-fähigen Geräten durchsetzen, auch wenn sie kein 802.11ax unterstützen. Dies sorgt für eine weitere Schutzschicht für das drahtlose Netzwerk.
Multi-RADIUS-Authentifizierung	Die Multi-RADIUS-Authentifizierung bietet Redundanz der Enterprise-Klasse, indem sie Unternehmen eine hohe Verfügbarkeit durch den Einsatz mehrerer RADIUS-Server im Aktiv- bzw. Passiv-Modus ermöglicht. Außerdem kann die Multi-RADIUS-Authentifizierung auf jedem virtuellen Access-Point unterstützt und für den WPA2-Enterprise- oder WPA2-Auto-Enterprise-Modus konfiguriert werden.

EINFACHE IMPLEMENTIERUNG UND ZENTRALE VERWALTUNG	
Funktion	Beschreibung
Einfachere Einrichtung und zentrale Verwaltung	Die SonicWave-Access-Points werden von der Cloud automatisch erkannt, bereitgestellt und aktualisiert.
Integriertes Switch-Management	Der SonicWall Wireless Network Manager bietet eine integrierte Steuerung von SonicWave-Access-Points und SonicWall-Switches für einheitliche Netzwerkverwaltung und -transparenz.
WiFi Planner	Um schon vor der Implementierung eine optimale Positionierung der Access-Points zu ermöglichen, bietet WiFi Planner eine umfassende Visualisierung des WLAN-Netzwerks, einschließlich Hindernissen, die das Signal stören, sowie abgedeckter und nicht abgedeckter Bereiche.
Floor Plan View	Bei Floor Plan View handelt es sich um ein Wi-Fi-Planungstool, mit dem Benutzer einen Raumplan hochladen oder erstellen und dann SonicWave-Access-Points entsprechend platzieren können, um die erforderliche Funkversorgung sicherzustellen.



## EINFACHE IMPLEMENTIERUNG UND ZENTRALE VERWALTUNG

Topology View	Topology View ist ein Wi-Fi-Tool, das automatisch Geräte und ihre Vernetzung in der drahtlosen Netzwerkarchitektur abbildet. Dies ist sehr nützlich für die Problembeseitigung.
Feuerfestigkeit	Die SonicWave-Access-Points sind feuerfest, sodass sie sich sicher in Lüftungskanälen oder innerhalb bzw. oberhalb abgehängter Decken installieren lassen.
Verschiedene Optionen für die Stromversorgung	Die SonicWave-Access-Points werden von SonicWall-PoE-Injektoren (Power over Ethernet) oder Fremdgeräten gespeist, um einen unkomplizierten Einsatz an Stellen zu gewährleisten, an denen Steckdosen schwer zugänglich sind.
Lichtsteuerung	Mit dimmbaren LEDs (außer Betriebsanzeige) eignen sich die SonicPoints perfekt für Umgebungen, in denen eine diskrete Wireless-Abdeckung erwünscht ist.
Umfassende Unterstützung für Standards und Protokolle	Die SonicWave-Access-Points unterstützen eine große Bandbreite an Wireless-Standards und Sicherheitsprotokollen, einschließlich 802.11 a/b/g/n/ac/ax, WPA2 und WPA3. Auf diese Weise können Organisationen Geräte, die keine höheren Verschlüsselungsstandards unterstützen, weiterhin nutzen.

## GERINGE GESAMTBETRIEBSKOSTEN

Funktion	Beschreibung
Niedrige Gesamtbetriebskosten	Die Lösung kommt ohne separate Wireless Controller aus, lässt sich einfach implementieren und ermöglicht die Verwaltung von Wireless- und Sicherheitsfunktionen über eine einzige Konsole. Dies reduziert die Kosten für die Implementierung einer Wireless-Lösung in eine neue oder bestehende Netzwerkinfrastruktur um ein Vielfaches.
MiFi-Extender	MiFi-Extender ermöglicht die Anbindung eines 3G-/4G-/LTE-Modems an einen SonicWave-Access-Point und kann entweder als primäres WAN oder als sekundäres Failover-WAN eingesetzt werden, um die Business-Continuity sicherzustellen.
Bluetooth Low Energy	Die SonicWave-Access-Points umfassen eine Bluetooth-Low-Energy-Funkinheit für die Nutzung von ISM-Anwendungen (ISM = industrial, scientific and medical) für Healthcare, Fitness, Beacons für den Einzelhandel, Sicherheit und Home-Entertainment über eine Bluetooth-Verbindung, die wenig Strom verbraucht.
USB-Port	Access-Points mit einem USB-Port unterstützen 3G-/4G-Failover. In den Port kann ein Dongle gesteckt werden, der im Falle eines WLAN-Ausfalls den Betrieb des Netzwerks über eine Mobilfunkverbindung aufrechterhält.
Green Access-Points	Die SonicWave-Access-Points unterstützen sogenannte Green Access-Points. Diese sorgen dafür, dass Funkheiten in den Sleep-Modus schalten, wenn keine Clients aktiv verbunden sind. So kann man Strom sparen und gleichzeitig auch die Kosten reduzieren. Der Access-Point beendet den Sleep-Modus, sobald ein Client versucht, eine Verbindung aufzubauen.

## MODELLNUMMERN (RICHTLINIEN)

SonicWave 681	APL66-106
SonicWave 641	APL67-107
SonicWave 621	APL68-108



Wenn Sie unsere sichere Wireless-Lösung testen möchten, besuchen Sie uns unter:

[www.sonicwall.com/products/secure-wireless/live-demo](http://www.sonicwall.com/products/secure-wireless/live-demo)

## Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter [www.sonicwall.de](http://www.sonicwall.de).

### SonicWall Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

Weitere Informationen erhalten Sie auf unserer Website.

[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

© 2023 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Haftung und keinerlei ausdrückliche, stillschweigende oder gesetzliche Gewährleistung für deren Produkte, einschließlich, aber nicht beschränkt auf die stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck und die Nichtverletzung von Rechten Dritter, soweit sie nicht in den Bestimmungen der Lizenzvereinbarung für dieses Produkt niedergelegt sind. SonicWall und/oder dessen Tochtergesellschaften haften nicht für irgendwelche unmittelbaren, mittelbaren, strafrechtlichen, speziellen, zufälligen oder Folgeschäden (einschließlich, aber nicht beschränkt auf Schäden aus entgangenem Gewinn, Geschäftsunterbrechung oder Verlust von Information), die aus der Verwendung oder der Unmöglichkeit der Verwendung dieses Dokuments entstehen, selbst wenn SonicWall und/oder dessen Tochtergesellschaften auf die Möglichkeit solcher Schäden hingewiesen wurden. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.