Clean wireless

High-performance clean wireless solutions

The demands on organizations' wireless networks—such as increased connection counts, bandwidth consumption, need for seamless roaming and extended perimeters—are all taxing on network performance, and complicate the management of existing 802.11 wireless network infrastructures. The challenge facing many businesses is how to preserve compatibility with legacy 802.11 technologies; enhance and optimize wireless networks through centralized management and control across all nodes of the WLAN while at the same time, maintaining maximum security.

The Dell™ SonicWALL™ Clean Wireless™ solutions combine high-performance 802.11n technology with enterprise-class network security appliances to deliver unparalleled wireless network security and performance, while dramatically simplifying the set-up and management of any 802.11-based wireless network.

The solution is based on Dell SonicWALL SonicPoint-N Series (SonicPoint-Ni Dual-Band, SonicPoint-Ne Dual-Band and SonicPoint-N Dual-Radio) wireless access points, which support the IEEE 802.11 a/b/g/n standards, to provide secure, higher speed access to data, voice and video over high-bandwidth wireless LANs. Scalable to networks of any size, SonicPoint-N wireless access points require no pre-configuration, as they are centrally configured and managed by any current Dell SonicWALL firewall – no additional wireless access controller is required.

The seamless integration of wireless access points with best-in-class Next-Generation Firewall or Unified Threat Management Firewall security featuring advanced application intelligence and control technology ensures that wireless traffic is scrutinized with the same intensity as wired network traffic. As a result, IT administrators can build and easily manage high-performance, distributed wireless networks with unified policy management across both the wireless and wired networks.

- **Comprehensive wireless security**
- **Exceptional wireless performance**
- **Central WLAN management**
- **Enhanced wireless reliability**
- **Flexible wireless deployment options**
- **Virtual Access Point (VAP) segmentation**
- **Broad protocol support**
- **Granular security policy enforcement**
- **Discreet wireless access point deployment**
- **FairNet wireless bandwidth allocation**

Features and benefits

Comprehensive wireless security features include Wireless Intrusion Detection Services (WIDS), wireless firewalling, secure Layer 3 wireless roaming, IEEE 802.11d multi-country roaming, and integrated Wireless Guest Services (WGS) to enforce password access for customers and other third-party guests.

Exceptional wireless performance features include 40 MHz channels and packet aggregation to support data rates of up to 600 Mbps. Dual-Radio and Dual-Band supports operation on either 2.4 GHz or 5.0 GHz networks.

Central WLAN management can be administered using Dell SonicWALL SuperMassive™ E10000, E-Class Network Security Appliance (NSA) , NSA and TZ Series firewalls, and requires no pre-configuration of the SonicPoint-N devices.

Enhanced wireless reliability is delivered using Multiple-Input Multiple-Out (MIMO) technology that uses multiple antennas as both the transmitter and the receiver to enhance throughput and reliability.

Flexible wireless deployment options include wall or ceiling mounting. SonicPoint-N Series wireless access points can receive power from a Dell SonicWALL Power over Ethernet (PoE) Injector or third party device for easy deployment where electrical outlets are not readily accessible. (SonicPoint-Ni Dual-Band and SonicPoint-Ne Dual-Band require IEEE 802.3af PoE; SonicPoint-N Dual-Radio requires IEEE 802.3at PoE.) SonicPoint-N Dual-Radio and SonicPoint-Ne Dual-Band access points can also be powered directly through an AC adapter.

Virtual Access Point (VAP) segmentation enables up to eight SSIDs to have dedicated authentication and privacy settings while sharing the same physical infrastructure, providing logical segmentation of secure wireless network traffic and secure customer access.

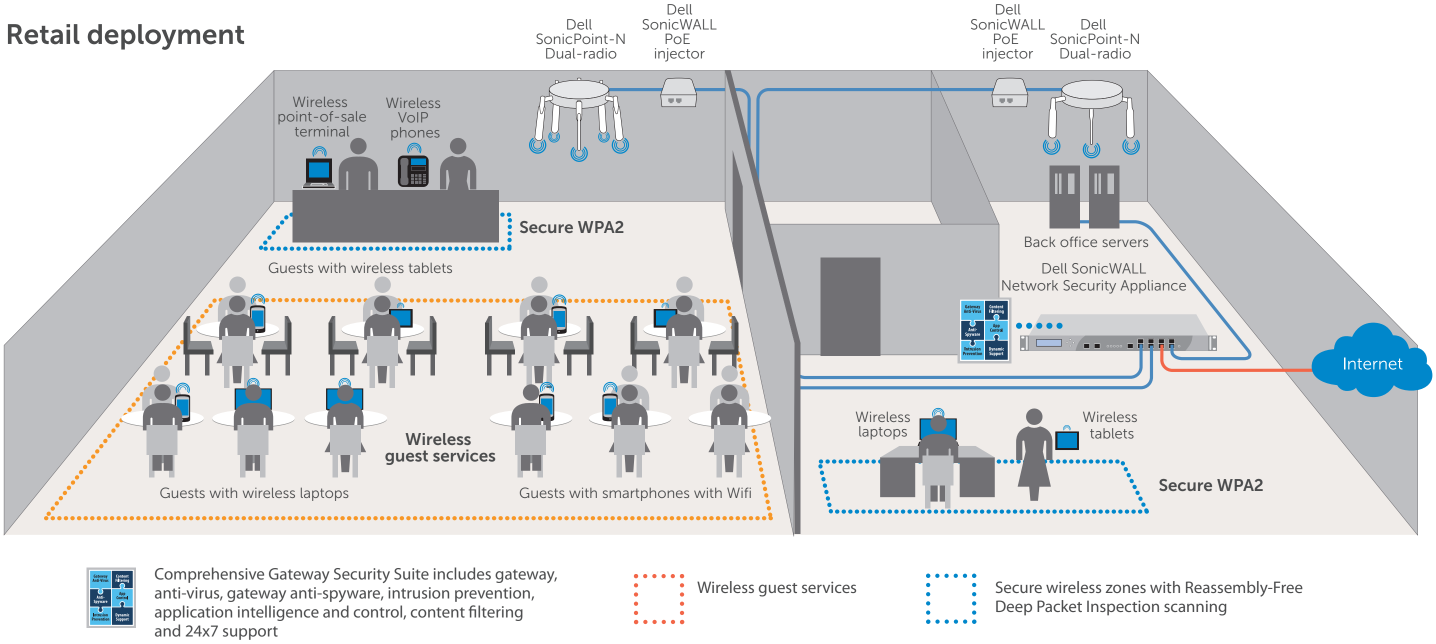
Broad protocol support includes 802.11 a/b/g/n, WPA2 and WPA, allowing businesses to leverage prior investments in devices that are incapable of supporting higher encryption standards, while easing migration to 802.11n.

Granular security policy enforcement allows the implementation of firewall rules to all wireless traffic, and controls all wireless client communications to any host on the network—wired or wireless.

Discreet wireless access point deployment features light and logo covers, controllable LED (except power) and internal antennas (on SonicPoint-Ni models).

FairNet wireless bandwidth allocation guarantees a minimum amount of bandwidth to each wireless client in order to prevent disproportionate bandwidth consumption by a single user.

Scenario 1: Small retail shop/ medical or dental office

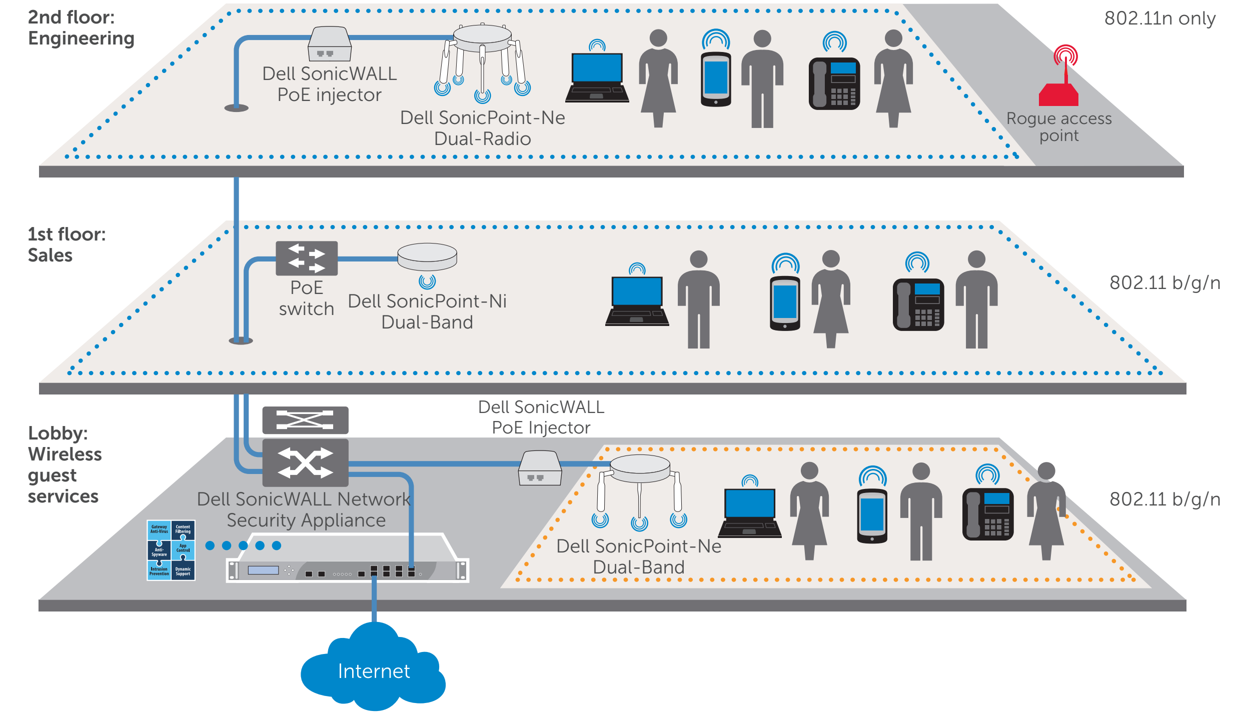

Retail deployment
Dell SonicPoint-N Dual-radio
Dell SonicWALL PoE injector
Dell SonicWALL PoE injector
Dell SonicPoint-N Dual-radio
Wireless point-of-sale terminal
Wireless VoIP phones
Secure WPA2
Back office servers
Dell SonicWALL Network Security Appliance
Guests with wireless tablets
Internet
Wireless guest services
Wireless laptops
Wireless tablets
Secure WPA2
Guests with wireless laptops
Guests with smartphones with Wifi
Comprehensive Gateway Security Suite includes gateway, anti-virus, gateway anti-spyware, intrusion prevention, application intelligence and control, content filtering and 24x7 support
Wireless guest services
Secure wireless zones with Reassembly-Free Deep Packet Inspection scanning

Retail, medical or dental businesses can combine SonicPoint-N Series wireless access points with Dell SonicWALL firewall solutions to quickly extend wireless network access, while providing Dell SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) for both wired and wireless traffic at the gateway, before allowing access to sensitive resources. Dell SonicWALL Wireless Guest Services (WGS) offers password-enforced customer access to the Internet, while Dell SonicWALL Virtual Access Points (VAPs) provide logical segmentation of secure wireless network traffic and in-the-clear customer access.

- SonicPoint-N Series wireless access points with 802.11n provide faster wireless access with greater range and better reliability
- SonicPoint-N Series wireless access points enable employees to securely access network resources from the wireless network using SSL VPN or WPA2
- VAPs create secure segmentation between trusted and un-trusted wireless users by allowing the broadcast of up to eight unique SSIDs
- Dell SonicWALL RFDPI scans all wireless traffic for vulnerabilities and threats
- Dell SonicWALL WGS allows customers to take advantage of wireless network access
- Provides auto-provisioning and centralized management for all SonicPoint-N Series wireless access points deployed in the network
- SonicPoint-N Dual-Radio wireless access points allow the dedication of one radio to rogue access detection while the other supports users, helping meet regulatory compliance

Scenario 2: Clean wireless solution

Enterprise deployment


2nd floor:
Engineering
Dell SonicWALL PoE injector
Dell SonicPoint-Ne Dual-Radio
802.11n only
Rogue access point
1st floor:
Sales
PoE switch
Dell SonicPoint-Ni Dual-Band
802.11 b/g/n
Lobby:
Wireless guest services
Dell SonicWALL PoE Injector
Dell SonicWALL Network Security Appliance
Dell SonicPoint-Ne Dual-Band
802.11 b/g/n
Internet

▦ Comprehensive Gateway Security Suite includes gateway, anti-virus, gateway anti-spyware, intrusion prevention, application intelligence and control, content filtering and 24x7 support

⬚ Wireless guest services

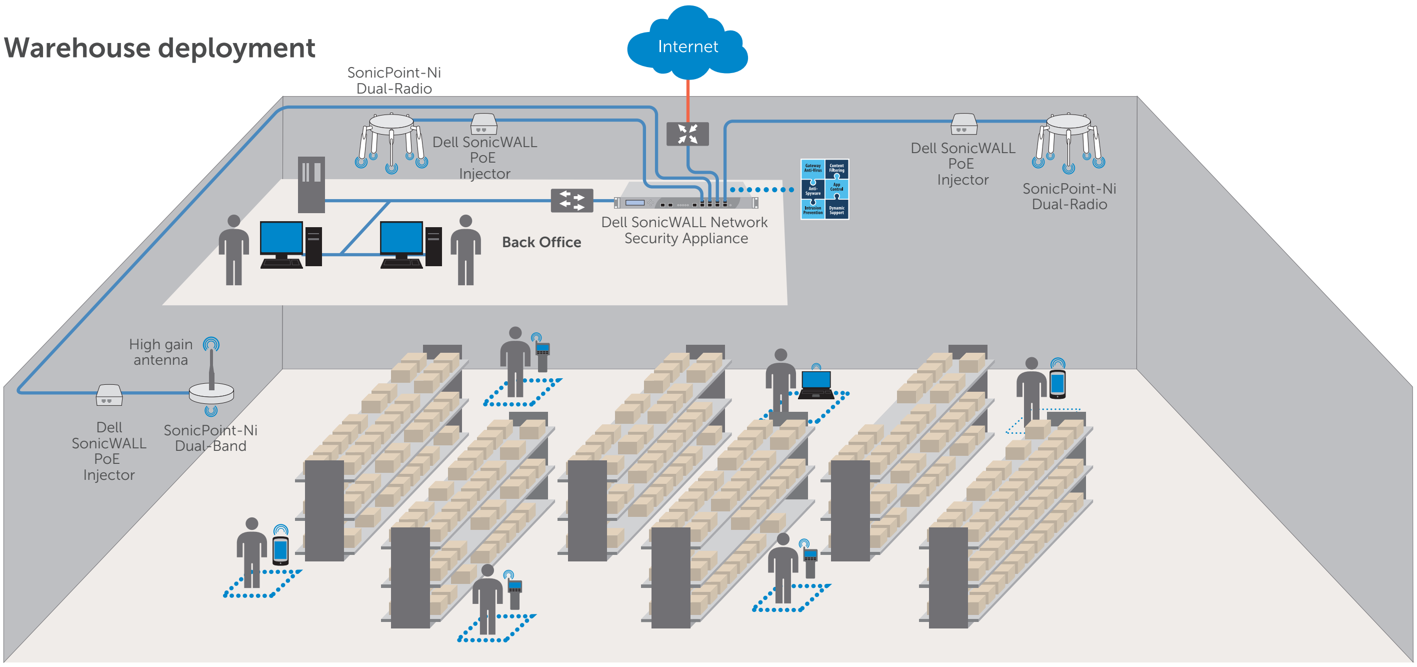
⬚ Secure wireless zones with Reassembly-Free Deep Packet Inspection scanning

In distributed organizations, SonicPoint-N Series wireless access points automatically contact Dell SonicWALL firewalls to auto-provision the latest firmware and configurations, easing rapid deployment. Dell SonicWALL firewalls offer a single point of wireless monitoring and management, lowering total cost of infrastructure ownership. The SonicPoint-N Series provides built-in wireless Intrusion Detection Systems (IDS) to scan for rogue access points and prevent unauthorized access.

- SonicPoint-N Series wireless access points with 802.11n provide faster wireless access with greater range and better reliability
- SonicPoint-N Series wireless access points auto-discover the central management gateway, easing deployment
- SonicPoint-N Series enable employees to securely access network resources from the wireless network using SSL VPN or WPA2
- Dell SonicWALL RFDPI comprehensively scans all wireless traffic for vulnerabilities and threats
- VAPs create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs

Scenario 3: Warehouse deployment

Warehouse deployment


Internet
SonicPoint-Ni Dual-Radio
Dell SonicWALL PoE Injector
Dell SonicWALL Network Security Appliance
Back Office
Dell SonicWALL PoE Injector
SonicPoint-Ni Dual-Radio
High gain antenna
Dell SonicWALL PoE Injector
SonicPoint-Ni Dual-Band

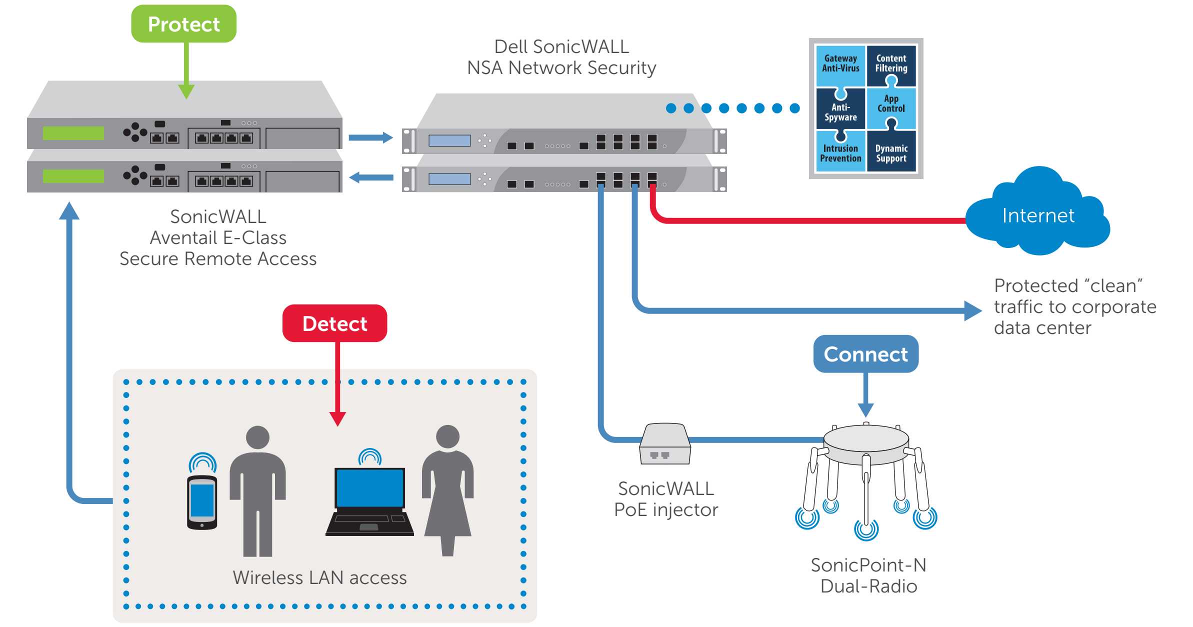
▦ Comprehensive Gateway Security Suite includes gateway, anti-virus, gateway anti-spyware, intrusion prevention, application intelligence and control, content filtering and 24x7 support

⬚ Secure wireless zones with Reassembly-Free Deep Packet Inspection scanning

In warehouse deployments, SonicPoint-N Series wireless access points automatically contact a Dell SonicWALL firewall to auto-provision the latest firmware and configurations, simplifying rapid wireless deployment. Dell SonicWALL firewalls offer a single point of wireless monitoring and management, lowering total cost of infrastructure ownership. SonicPoint-Ni Dual-Band and SonicPoint-Ne Dual-Band come with built-in wireless IDS to scan for rogue access points and prevent unauthorized access.

- SonicPoint-N Series wireless access points with 802.11n provide faster wireless access with greater range and better reliability
- SonicPoint-N Series wireless access points auto-discover the central management gateway, easing deployment
- SonicPoint-N Series wireless access points allow employees to securely access network resources from the wireless network using SSL VPN or WPA2
- Dell SonicWALL RFDPI comprehensively scans all wireless traffic for vulnerabilities and threats
- VAPs create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs
- Dell SonicWALL firewalls provide auto-provisioning and central management for all SonicPoints deployed in the network

Scenario 4: Enterprise wireless and Dell SonicWALL Aventail E-Class Secure Remote Access



Detect **SonicWALL Aventail's Endpoint Control** continually detects the identity and security state of the end device

Protect **SonicWALL Aventail Unified Policy** enforces devices access control, ensuring users access only to authorized applications

Connect **SonicWALL Aventail Smart Access and Smart Tunneling** ensure easy, secure user access to all network resources

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, application intelligence and control, content filtering and 24x7 support

Secure wireless zone with Reassembly-Free Deep Packet Inspection scanning

In distributed wireless environments where there is a need to support additional endpoint security and Network Access Control (NAC), network administrators can deploy SonicPoints in conjunction with a SuperMassive E10000 or E-Class NSA Series appliance and a Dell SonicWALL Aventail E-Class Secure Remote Access (SRA) appliance. The combined solution not only provides distributed wireless connectivity and centralized SonicPoint management, but also endpoint enforcement and interrogation ensuring that all wireless users systems have the proper system configuration before gaining access to secure network resources.

- Enforces policy across disparate points of entry, allowing granular access control for collaboration and compliance
- Easy-to-use, providing the core elements of NAC today and a foundation for NAC initiatives for the future
- Dell SonicWALL 802.11n solutions provide fast wireless access with greater range and better reliability
- VAPs create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs
- Dell SonicWALL firewalls provide auto-provisioning and central management for all SonicPoints deployed in the network

Specifications

Hardware Specifications	SonicPoint-N Dual-Radio	SonicPoint-Ni Dual-Radio	SonicPoint-Ne Dual-Radio
Dimensions	7.5 (L) x 7.5 (W) x 1.5 (H) in 19.1 (L) x 19.1 (W) x 3.8 (H) cm	4.9 (L) x 4.9 (W) x 1.18 (H) in 15 (L) x 15 (W) x 3 (H) cm	
Weight	0.87 lbs/0.39 kg	0.595 lbs/0.27 kg	
PoE Power Requirements	802.3at/0.35A	802.3af/0.35A	
Power Supply	PoE and AC Adapter	PoE	PoE and AC Adapter
Status Indicators	Six (6) LED (WLAN, Link/Act) (LAN, Link/Act) Power, Wrench		
Antennas	3 External SMA and 3 External RP-TNC antennas	Fully internal	3 External SMA antennas
Wired Network Ports	1 10/100/1000 auto-sensing RJ-45 port for Ethernet and Power over Ethernet (PoE); 1 RJ-45 console port		
Mechanical	Wall or ceiling mount kit, Logo and LED Cover		
Virtual Access Points	Up to 8 per SonicPoint		

Maximum Managed Devices		
Security Appliance	Per WLAN Interface	Per Appliance
TZ 105/105 Wireless-N	1	1
TZ 205/205 Wireless-N	2	2
TZ 215/215 Wireless-N	16	16
NSA 220/250M	16	16
NSA 2400/2400MX	32	32
NSA 3500	48	48
NSA 4500	64	64
NSA 5000	64	64
NSA E5500	96	96
NSA E6500	128	128
NSA E8500	128	128
NSA E8510	128	128
SuperMassive™ E10000 Series	128	128

Standards	
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n draft 2.0, IEEE 802.11i, IEEE 802.3af
Regulatory	FCC/ICES CE, C-Tick, RoHS, WEEE
Safety	UL, cUL, TUV-GS, CB, CE
Environmental	
Temperature range	32 to 104°F, 0 to 40°C
Radio Specifications	
Frequency band	802.11a: 5.180-5.825GHz; 802.11b/g: 2.412-2.472GHz; 802.11n: 12-2.472Ghz, 5.180-5.825Ghz
Operating channels	802.11a: US and Canada 9 , Europe 15, Japan 8, Singapore 9, Taiwan 4 channels 802.11b/g/n: US and Canada 1-11, Europe 1-13, Japan 1-14
Dynamic frequency selection	Capable
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: 6,9,12,18,24,36,48,54, 72, 84, 150 300 Mbps per channel
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM), BPSK, QPSK, 1-QAM, 64-QAM; 802.11b: Direct Sequence Spread Spectrum (DSSS), CCK, DBPSK, DQPSK; 802.11g: Orthogonal Frequency Division Multiplexing (OFDM), BPSK, QPSK, 16-QAM, 64-QAM; 802.11n: 802.11n draft 2.0
Security	
Data encryption	WPA2; IPSec, 802.11i, WPA; 64/128/152-bit WEP, TKIP, AES, SSL VPN*
Authentication	
Authentication	RADIUS, Active Directory, Novell e-Directory, SAMBA, Single Sign-on (SSO)

Hardware specifications	PoE Injector		
Number of ports	2: (1) Data In; (1) data and power out		
Dimensions	1.22(H) x 2.30(W) x 5.71(D) in; 31(H) x 58.5(W) x 145(D) mm		
Weight	1.0 lbs/(450g)		
Connectors	Shielded RJ-45, EIA 568A and 568B		
Indicators	System indicator: AC power (Green); User indicator: Channel power active (Green)		
Data rates	10/100/1000 Mbps		
Power over LAN output			
Pin assignment and polarity	4/5 (+), 7/8 (-)		
Output power voltage	-48 VDC		
User port power	15.4 W minimum	16.4 W minimum	15.4 minimum
Input power requirements			
AC input voltage	90 to 264 VAC		
AC frequency	47 to 63 Hz		
AC Input currency	0.5A at 100-240 VAC		
Standards and compliance			
Regulatory compliance	CE, RoHS, WEEE; Electromagnetic emission and immunity; EN 55022, CISPR 22, FCC Part 15, (Class B with FTP cabling); EN 55024, CISPR 24		
Safety approvals	UL 60950-1; EN 60950; IEC 60950-1		
Environmental conditions			
Operating ambient temperature	32 to 104 °F, 0 to 40 °C		
Operating humidity	Maximum 90%, non-condensing		
Storage temperature	-4 to 158 °F, -20 to 70 °C		
Storage humidity	Maximum 93%, non-condensing		
Operating altitude	-1,000 to 10,000 ft. (-304.8 to 3,048 m)		

*When used with Dell SonicWALL Secure Remote Access Series appliance.

Dell SonicWALL SonicPoint-N Dual-Radio with PoE Injector
01-SSC-9289

4-pack Dell SonicWALL SonicPoint-N Dual-Radio without PoE Injector
01-SSC-9291

8-pack Dell SonicWALL SonicPoint-N Dual-Radio without PoE Injector
01-SSC-9293

Dell SonicWALL SonicPoint-Ni Dual-Band with PoE Injector
01-SSC-8575

Dell SonicWALL SonicPoint-Ni Dual-Band 4-Pack Bundle without PoE Injector
01-SSC-8588

Dell SonicWALL SonicPoint-Ni Dual-Band 8-Pack Bundle without PoE Injector
01-SSC-8592

Dell SonicWALL SonicPoint-Ne Dual-Band with PoE Injector
01-SSC-8577

Dell SonicWALL SonicPoint-Ne Dual-Band 4-Pack Bundle without PoE Injector
01-SSC-8590

Dell SonicWALL SonicPoint-Ne Dual-Band 8-Pack Bundle without PoE Injector
01-SSC-8579

PoE Injector 802.3af Gigabit N
01-SSC-5544

For more information on Dell SonicWALL secure wireless networking solutions, please visit **www.sonicwall.com**.

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit **www.dell.com/secureworks**