

Refurbished CISCO LIC-CT5520-1A Datasheet

CISCO > WIRELESS

Cisco 5500 Series Wireless Controllers

Features and benefits	
Feature	
Feature	Benefits
Cisco DNA SD-Access Wireless	<p>SD-Access Wireless is Cisco's next-generation architecture for enterprise networks. It is the industry's first policy-based automation from the edge to the cloud. It enables network access in minutes for any user or device to any application without compromising on security.</p> <p>SD-Access Wireless enables policy-based automation for wired and wireless, automated provisioning of wired and wireless networks, group-based policy for users and connected devices, and a distributed wireless data plane for campus deployments. In addition, all clients roams are treated as Layer 2 roams across the network for distributed traffic.</p> <p>Learn more at https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html.</p>
Cisco DNA Analytics and Assurance	<p>Cisco DNA Analytics and Assurance offers comprehensive network visibility. It collects data from users, devices, and applications to proactively identify problems. Network analytics and automation help IT quickly resolve issues, so you can increase availability and deliver a better user experience.</p> <p>Learn more at https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-analytics-assurance.html.</p>
Scalability and performance	<p>Optimized to enable 802.11ac Wave 2 next-generation networks, supporting:</p> <ul style="list-style-type: none"> 20-Gbps throughput 1500 access points 20,000 clients 4096 VLANs
RF management	<p>Proactively identifies and mitigates signal interference for better performance</p> <p>Provides both real-time and historical information about RF interference affecting network performance across controllers, through systemwide integration with Cisco CleanAir technology</p>
Multimode with indoor, outdoor mesh access points	<p>Versatile controller with support for centralized, distributed, and mesh deployments to be used at different places in the network, offering maximum flexibility for medium-sized campus, enterprise, and branch networks</p> <ul style="list-style-type: none"> Centralized control, management, and client troubleshooting Seamless client access in the event of a WAN link failure (local data switching) Highly secure guest access Efficient access point upgrade that optimizes the WAN link utilization for downloading access point images Cisco OfficeExtend technology that supports corporate wireless service for mobile and remote workers with secure wired tunnels to indoor Cisco Aironet access points supporting OfficeExtend mode
Comprehensive end-to-end security	<p>Offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant Datagram Transport Layer Security (DTLS) encryption on the control plane between access points and controllers across remote WAN links</p> <ul style="list-style-type: none"> Management frame protection detects malicious users and alerts network administrators Rogue detection for Payment Card Industry (PCI) compliance Rogue access point detection and detection of denial-of-service attacks
End-to-end voice	<p>Supports Cisco Unified Communications for improved collaboration through messaging, presence, and conferencing</p> <p>Supports all Cisco Unified IP Phones for cost-effective, real-time voice services</p>
Fault tolerance and high availability	<p>Subsecond access point and client failover for uninterrupted application availability</p> <ul style="list-style-type: none"> Redundant 1 Gigabit Ethernet or 10 Gigabit Ethernet connectivity Solid-state device-based storage - no moving parts Optional redundant, hot-swappable power supply with no incremental system downtime Enhanced system uptime with fast system restarts
Cisco Enterprise Wireless Mesh	<p>Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network</p> <p>Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing</p>

WLAN express setup	Simplified GUI wizard for quick setup and intuitive dashboards for monitoring and troubleshooting
High-performance video	Cisco VideoStream technology optimizes the delivery of video applications across the WLAN
Mobility, security, and management for IPv6 and dual-stack clients	Highly secure, reliable wireless connectivity and consistent end-user experience Increased network availability through proactive blocking of known threats Equips administrators for IPv6 planning, troubleshooting, and client traceability from Cisco Prime Infrastructure
Environmentally responsible	Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours

Product specifications

Item	
Item	Specifications
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2, Wi-Fi 6 (802.11ax)
Wired/switching/routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T, 1000BASE-SX, 1000BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Data Request For Comments (RFC)	RFC 768 UDP RFC 791 IP RFC 2460 IPv6 RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 1122 Requirements for Internet Hosts RFC 1519 CIDR RFC 1542 BOOTP RFC 2131 DHCP RFC 5415 CAPWAP Protocol Specification RFC 5416 CAPWAP Binding for 802.11
Security standards	Wi-Fi Protected Access (WPA) IEEE 802.11i (WPA2, RSN) RFC 1321 MD5 Message-Digest Algorithm RFC 1851 ESP Triple DES Transform RFC 2104 HMAC: Keyed Hashing for Message Authentication RFC 2246 TLS Protocol Version 1.0 RFC 2401 Security Architecture for the Internet Protocol RFC 2403 HMAC-MD5-96 within ESP and AH RFC 2404 HMAC-SHA-1-96 within ESP and AH RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV RFC 2407 Interpretation for ISAKMP RFC 2408 ISAKMP RFC 2409 IKE RFC 2451 ESP CBC-Mode Cipher Algorithms RFC 3280 Internet X.509 PKI Certificate and CRL Profile RFC 4347 Datagram Transport Layer Security RFC 5246 TLS Protocol Version 1.2
Encryption	Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) Data Encryption Standard (DES): DES-CBC, 3DES Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit DTLS: AES-CBC IPsec: DES-CBC, 3DES, AES-CBC 802.1AE MACsec encryption
Authentication, Authorization, and Accounting (AAA)	IEEE 802.1X RFC 2548 Microsoft Vendor-Specific RADIUS Attributes RFC 2716 PPP EAP-TLS RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 2867 RADIUS Tunnel Accounting RFC 2869 RADIUS Extensions RFC 3576 Dynamic Authorization Extensions to RADIUS RFC 5176 Dynamic Authorization Extensions to RADIUS RFC 3579 RADIUS Support for EAP RFC 3580 IEEE 802.1X RADIUS Guidelines RFC 3748 Extensible Authentication Protocol (EAP) Web-based authentication TACACS support for management users

Management	<p>Simple Network Management Protocol (SNMP) v1, v2c, v3 RFC 854 Telnet RFC 1155 Management Information for TCP/IP-Based Internets RFC 1156 MIB RFC 1157 SNMP RFC 1213 SNMP MIB II RFC 1350 TFTP RFC 1643 Ethernet MIB RFC 2030 Sntp RFC 2616 HTTP RFC 2665 Ethernet-Like Interface Types MIB RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions RFC 2819 RMON MIB RFC 2863 Interfaces Group MIB RFC 3164 Syslog RFC 3414 User-Based Security Model (USM) for SNMPv3 RFC 3418 MIB for SNMP RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs Cisco private MIBs</p>
Management interfaces	<p>Web-based: HTTP/HTTPS Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port Cisco Prime Infrastructure</p>
Interfaces and indicators	<p>2 x 10 Gigabit Ethernet interfaces or 2 x 1 Gigabit Ethernet interfaces Small Form-Factor Pluggable Plus (SFP+) options (only Cisco SFP+s supported), including S-Class Optics Small Form-Factor Pluggable (SFP) options (only Cisco SFPs supported), including S-Class Optics 1 x service port: 1 Gigabit Ethernet port (RJ-45) 1 x redundancy port: 1 Gigabit Ethernet port (RJ-45) 1 x Cisco Integrated Management Controller port: 10/100/1000 Ethernet (RJ-45) 1 x console port: Serial port (RJ-45) LED indicators: Network Link, Diagnostics</p>
Physical dimensions	<p>Dimensions (WxDxH): 18.98 x 30.98 x 1.70 in. (48.2 x 78.7 x 4.32 cm) including handles Weight: 30 lb (13.6 kg) with 1 power supply</p>
Environmental conditions	<p>Air temperature: Appliance operating: 41° to 104°F (5° to 40°C), derate the maximum temperature by 1.0°C per every 1000 ft. (305m) of altitude above sea level Appliance nonoperating: -40° to 149°F (-40° to 65°C) Humidity: Appliance operating: 10% to 90%; noncondensing at 82°F (28°C) Appliance nonoperating: 5% to 93% at 82°F (28°C) Altitude: Appliance operating: 0 to 3000m (0 to 10,000 ft.) Appliance nonoperating: 0 to 12,192m (0 to 40,000 ft.) Electrical input: AC input frequency range: 47 to 63 Hz Input voltage range: Minimum: 90 VAC Maximum: 264 VAC Maximum Power 190W Input kilovolt-amperes (kVA), approximately: Minimum: 0.090 kVA Maximum: 0.700 kVA Heat dissipation: 650 BTU/hr Sound power level measure: A-weighted per ISO 7779 LpAm (dBA), operation at 77°F (25°C): 49.3</p>
Regulatory compliance	<p>CE Markings per directives 2004/108/EC and 2006/95/EC Safety: UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition AS/NZS 60950-1 GB4943 2001 EMC - Emissions: 47CFR Part 15 (CFR 47) Class A AS/NZS CISPR22 Class A EN55022 Class A ICES003 Class A VCCI Class A EN61000-3-2 EN61000-3-3 KN22 Class A CNS13438 Class A EMC - Immunity: EN55024 CISPR24 EN300386 KN24</p>

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com