

Alcatel-Lucent OmniAccess Wireless Base Software

WIRELESS LAN SOFTWARE



Standard with every Alcatel-Lucent OmniAccess Wireless LAN (WLAN) switch, the base wireless software provides unprecedented control over the entire wireless environment with centralized wireless LAN switching and advanced services.

The base feature set of Alcatel-Lucent OmniAccess WLAN software, detailed below, includes sophisticated authentication and encryption, protection against rogue APs, seamless mobility with fast roaming, RF management and analysis tools, centralized configuration, location tracking, and more.

OmniAccess Wireless LAN base software can be complemented with optional modules including Wireless Intrusion Protection, Policy Enforcement Firewall, VPN Server, Client Integrity, Remote AP, External Services Interface, and xSec Advanced L2 Encryption.



FEATURES

- Secure authentication, encryption and access control
- Seamless mobility
- RF management, RF planning and troubleshooting

BENEFITS

- 802.1x authentication with WPA, WPA2 and 802.11i
- Programmable hardware-based encryption engine upgradeable to latest security standards
- Web-based Captive Portal for SSL browser-based authentication
- Automatic detection, classification, and containment of rogue access points
- Roaming cutover times of 2-3 milliseconds enable ultra-fast handoffs for delay sensitive applications
- Proxy mobile IP and proxy DHCP allows users to roam seamlessly between APs and WLAN switches
- Automatic Radio Management (ARM) for simple self-configuration of all RF parameters
- Live Site Survey for real-time monitoring and display of RF coverage and interference
- Automatic modeling, planning and placement of APs and RF monitors based on capacity, coverage and security requirements
- Packet capture tools provide detailed snapshot of entire wireless environment

FEATURES

- Network management high availability
- QoS, VoIP support and location tracking

BENEFITS

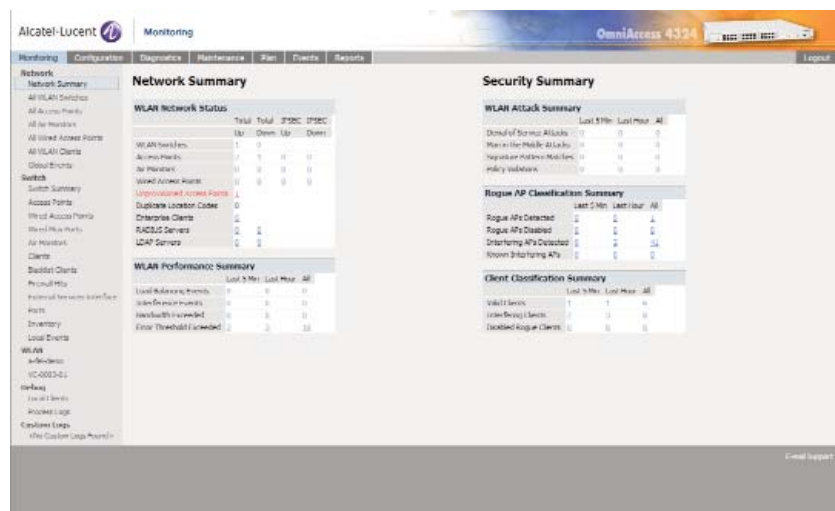
- All WLAN switches and APs are centrally controlled and managed
- Redundant WLAN switch arrays using VRRP
- Automatic RF fault tolerance avoids radio dead spots and provides AP back-up
- 802.11e, WMM and 802.1p support
- Call admission control and voice aware RF monitoring
- Location of any 802.11 device with real-time display

Secure Authentication, Encryption and Access Control

The OmniAccess WLAN software delivers industry-leading capabilities for securing the air, devices, users and data on the enterprise wireless network. A wide range of authentication methods are supported, including the industry standard WPA2 and 802.11i protocols widely recognized as state-of-the-art for wireless security. The OmniAccess WLAN software provides the latest layer 2 encryption technologies and with its programmable hardware encryption processor, the OmniAccess WLAN switch can be instantly upgraded to support emerging encryption standards.

For clients without WPA, VPN, or other security software, the OmniAccess wireless system supports a web-based captive portal that provides standard browser-based authentication. Captive portal authentication is encrypted using industry-standard SSL (Secure Sockets Layer), and can support both registered users with a login and password or guest users who supply only an email address. Through integration with back-end systems, captive portal can provide a secure guest access solution, permitting front-desk reception staff to issue and track authentication credentials for visitors.

Figure 1



To protect against unsanctioned wireless devices, the OmniAccess WLAN rogue AP classification algorithms allow the system to accurately differentiate between threatening "rogue" APs installed on the local network and nearby "interfering" APs. Once classified as rogue, these APs are automatically disabled through both the wireless and wired networks. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floor plan, so that they may be removed from the network.

Seamless Mobility

The OmniAccess WLAN software provides seamless wireless connectivity as users move throughout the network. With roaming cutover times of 2-3 milliseconds, delay-sensitive and persistent applications such as voice and Citrix experience uninterrupted performance. OmniAccess WLAN software integrates proxy mobile IP and proxy DHCP functions letting users roam between subnets, APs and WLAN switches without special client software. With VLAN pooling, user membership of VLANs is load-balanced to maintain optimal network performance as large groups of users move about the network.

RF Management, RF Planning & Troubleshooting

The OmniAccess WLAN Automatic Radio Management (ARM) feature takes the guesswork out of AP deployments. Once APs are brought up, they immediately begin monitoring their local environment for interference, noise, and signals being received from other APs. This information is reported back to the central WLAN switch, which is then able to control the optimal channel assignment and power levels for each AP in the network.

Once the network is deployed, the OmniAccess WLAN Live Site Survey feature provides a real-time, color display of the RF environment showing signal strength, coverage and interference. Live Site Survey enables WLAN coverage and capacity planning, and precludes the need for frequent and expensive manual site surveys.

Working with OmniAccess access points and air monitors to constantly scan across all the channels in the 2.4 Ghz and 5 Ghz bands, the OmniAccess wireless software collects aggregate and raw statistics on a per station, per channel and per user basis. All statistics can be displayed within the OmniAccess wireless intuitive troubleshooting tools, and are also available via SNMP for easy integration into third-party management or analysis applications. Live packet capture is available that can turn any OmniAccess AP or Air Monitor into a packet capture device, able to stream live 802.11-level frames back to monitoring stations such as Ethereal, Air Magnet Laptop Analyzer, or WildPackets AiroPeek NX. With this detailed information, administrators can quickly troubleshoot user problems, determine top wireless talkers and diagnose congested APs.

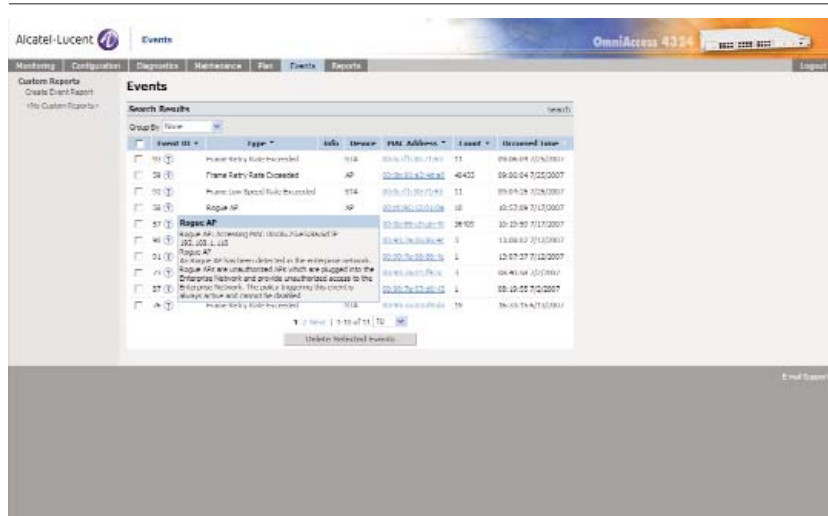
QoS, VoIP Support and Location Tracking

Support for 802.11e and WMM ensures wireless QoS for delay-sensitive applications with mapping between 802.11e tags and internal hardware queues. OmniAccess WLAN switches also support mapping of 802.1p and DiffServ tags to hardware queues for wired-side QoS. Layer-2 QoS capabilities are easily enhanced to layer-3+flow management and DiffServ using the add-on Policy Enforcement Firewall module.

For voice over WLAN (VoWLAN) deployments, the OmniAccess wireless automatic Voice Flow Classification (VFC) identifies and automatically prioritizes voice calls to ensure low-latency transmission. Call admission control manages voice device associations and active off-hook calls to ensure bandwidth availability for voice calls at each AP. For uninterrupted performance, voice-aware RF scanning ensures that APs don't cycle to optional monitoring-mode when a voice client is in the vicinity.

The OmniAccess WLAN software includes advanced location visualization and tracking of 802.11z devices. RF signature-based location triangulation allows administrators to physically locate any 802.11 user or device within one meter of accuracy. OmniAccess' wireless real-time location tracking capabilities, multiple devices can be continuously located and tracked simultaneously.

Figure 2



Secure Authentication, Encryption & Access Control

AUTHENTICATION TYPES

- IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST)
- RFC 2548 Microsoft Vendor-Specific RADIUS Attributes
- RFC 2716 PPP EAP-TLS
- RFC 2865 RADIUS Authentication
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 3579 RADIUS Support for EAP
- RFC 3580 IEEE 802.1X RADIUS Guidelines
- RFC 3748 Extensible Authentication Protocol
- MAC Address authentication
- Web-based captive portal authentication

AUTHENTICATION SERVERS

- Internal database
- LDAP/ SSL Secure LDAP
- RADIUS
- TACACS+
- Third-party Authentication Servers Tested Interoperability: Microsoft Active Directory, Microsoft IAS RADIUS
- Server, Cisco ACS Server, Funk Steel Belted RADIUS Server, RSA ACEserver, Infoblox, Interlink RADIUS
- Server, FreeRADIUS, A-10 Networks IDSentrie

ENCRYPTION TYPES

- WEP: 64 and 128 bit
- WPA-TKIP, WPA-PSK-TKIP, WPA-AES, WPA-PSK-AES
- WPA2/802.11i: WPA2-AES, WPA2-PSK-AES, WPA2-TKIP, WPA2-PSK-TKIP
- Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit
- Programmable hardware upgradeable to new encryption mechanisms

Rogue AP Detection: Yes

Rogue AP Classification: Yes

Rogue AP Containment: Wired and Wireless

Seamless Mobility

- Fast Roaming: 2-3 msec intra-switch; 10-15 msec inter-switch
- Roaming across subnets and VLANs: Yes
- Mobile IP support: Yes
- Proxy Mobile IP: Yes
- Proxy DHCP: Yes
- VLAN Pooling: Yes

RF Management, RF Planning and Troubleshooting

- Adaptive Radio Management (ARM): Yes
- Multiple ESSIDs per AP: Up to 16
- Automatic AP calibration: Yes
- Self-healing around failed APs: Yes
- Load balancing — number of users: Yes
- Load balancing — utilization based: Yes
- Timer-based AP access control: Yes
- RF Planning and Deployment Tool: Yes
- Wireless RMON/packet capture: Yes
- Plug-ins for third-party analysis tools: Ethereal, AiroPeek, AirMagnet
- 802.11h 5GHz extensions for Europe: Yes
- 802.11d additional regulatory domains: Yes

Network Management and High Availability

- Web-based Configuration: Yes
- Command Line: Console, telnet, SSH
- Syslog: Yes
- SNMP v2c: Yes
- SNMP v3: Yes
- Aruba private MIB: Yes
- MIB-II: Yes
- Centralized configuration of local WLAN switches: 128
- Centralized image upgrade for WLAN switches and all APs: Yes
- VRRP: Yes
- Redundant datacenter support: Yes

Quality of Service, VoIP Support and Location Tracking

- 802.1p support: Yes
- 802.11e support: Yes
- T-SPEC/TCLAS: Yes
- WMM: Yes
- Voice-aware RF monitoring /scanning: Yes-session based
- Call Admission Control: Yes
- Automatic Voice Flow Classification (VFC): SIP, SVP, SCCP
- U-APSD (Unscheduled Automatic Power Save Delivery): Yes
- IGMP Snooping for efficient multicast delivery: Yes
- Real-time location tracking and monitoring: Yes
- Location tracking API for external integration: Yes

General Switching

- RFC 1812 Requirements for IP Version 4 Routers RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2338 VRRP
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- IEEE 802.1D - 1998 Spanning Tree Protocol (STP) IEEE 802.1Q -1998 Virtual Bridged Local Area Networks

Wireless

- IEEE 802.11a/b/g 5GHz, 2.4GHz, 2.4GHz High-Rate
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e Quality of Service
- IEEE 802.11h Spectrum and TX Power Extensions for 5GHz in Europe
- IEEE 802.11i MAC Security Enhancements

VLANS

- IEEE 802.1Q VLAN Tagging
- Port-based VLANs

Quality of Service and Policies

- IEEE 802.1D -1998 (802.1p) Packet Priority
- IEEE 802.11e - Quality of Service Enhancements
- RFC 2474 Differentiated Services

Management and Traffic Analysis

- RFC 2030 - SNMP, Simple Network Time Protocol v4
- RFC 854 - Telnet client and server
- RFC 783 - TFTP Protocol (revision 2)
- RFC 951, 1542 - BootP
- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 1591 - DNS (client operation)
- RFC 1155 - Structure of Mgmt Information (SMIv1)
- RFC 1157 - SNMPv1
- RFC 1212 - Concise MIB definitions.
- RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets - MIB-II
- RFC 1215 - Convention for defining traps for use with the SNMP
- RFC 1573 - Evolution of Interface
- RFC 2011 - SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 - SNMPv2 Management Information
- RFC 2013 - SNMPv2 Management Information
- RFC 2578 - Structure of Management Information Version 2 (SMIv2)
- RFC 2579 - Textual Conventions for SMIv2
- RFC 2863 - The Interfaces Group MIB
- RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

- RFC 959 - File Transfer Protocol (FTP)
- RFC 2660 - The Secure HyperText Transfer Protocol (HTTPS)
- RFC 1901 - 1908 SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2570 - 2575 SNMPv3, user based security, encryption and authentication
- RFC 2576 - Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2233 - Interface MIB
- RFC 2251 - Lightweight Directory Access Protocol (v3)
- RFC 1492 - An Access Control Protocol, TACACS+
- RFC 2865 - Remote Access Dial In User Service (RADIUS)
- RFC 2866 - RADIUS Accounting
- RFC 2869 - RADIUS Extensions
- RFC 3576 - Dynamic Authorization Extensions to Remote RADIUS
- RFC 3579 - RADIUS Support For Extensible Authentication Protocol (EAP)
- RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 - Microsoft RADIUS Attributes
- RFC 1350 - The TFTP Protocol (Revision 2)
- Secure Shell (SSHv2) server
- Configuration logging
- Multiple Images, Multiple Configs

- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers

Security/Encryption

- RFC 1661 - The Point-to-Point Protocol (PPP)
- RFC 2406 - IP Encapsulating Security Payload (ESP)
- RFC 2661 - Layer Two Tunneling Protocol "L2TP"
- RFC 3193 - Securing L2TP using IPsec
- RFC 2451 - The ESP CBC-Mode Cipher Algorithms
- RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
- RFC 2401 - Security Architecture for the Internet Protocol
- RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 - The Internet Key Exchange (IKE)
- RFC 2405 - ESP DES-CBC cipher algorithm with explicit IV
- RFC 2403 - Use of HMAC-SHA1-96 with ESP and AH
- RFC 3602 - The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 4017 - Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
- RFC 3706 - A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3947 - Negotiation of NAT-Traversal in the IKE
- RFC 3748 - Extensible Authentication Protocol (EAP)
- RFC 3079 - Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
- RFC 4137 - State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 2716 - PPP EAP TLS Authentication Protocol
- RFC 2246 - The TLS Protocol (SSL)
- RFC 2407 - Internet IP Security Domain of Interpretation for ISAKMP
- RFC 3948 - UDP encapsulation of IPsec packets
- Internet Draft - EAP-TTLS
- Internet Draft - EAP-PEAP
- Internet Draft - EAP-POTP
- Internet Draft - XAuth for ISAKMP

To learn more, contact your dedicated Alcatel-Lucent representative, authorized reseller, or sales agent. You can also visit our Web site at www.alcatel-lucent.com.

This document is provided for planning purposes only and does not create, modify, or supplement any warranties, which may be made by Alcatel-Lucent relating to the products and/or services described herein. The publication of information contained in this document does not imply freedom from patent or other protective rights of Alcatel-Lucent or other third parties.

www.alcatel-lucent.com

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.
© 2007 Alcatel-Lucent. All rights reserved. 031901-00 Rev. B 8/07