

Wieso OmniAccess Wireless ?

- Einfach aufzubauen
- Einfach zu managen
- Herausragende Security-Funktionen
- Preisgekrönte Performance und Skalierbarkeit
- Einfache Unterstützung von neuen Services z.B. VoIP
- 802.11n (Draft) Unterstützung mit bis zu 300 MBit
- Leistungstarker 802.11n AP mit geringer Leistungsaufnahme und Gewicht kann von Standard PoE Systemen wie OmniSwitch 6850 ohne zusätzliche Netzteile versorgt werden
- Explosionsgeschützte Outdoor AP85 mit Anschluss für Solarpanel
- Unterstützung von Meshed Topology, Voice over Wireless und Location Tracking
- Geringes Risiko durch Migrationsfähigkeit
- Beste Testergebnisse unabhängiger Institute

Performance

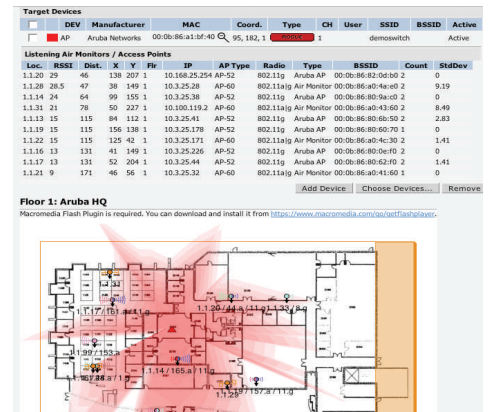
- Ultra Fast Roaming—weniger als 10ms
- Einsatz in Netzwerken mit hunderten Controllern und tausenden APs
- Erweiterter VoIP/Mobile Application Support
- Unterstützung von Voice und Data im gleichen Netzwerk (gleiche SSID) ohne Einschränkung der Performance oder der Zuverlässigkeit
- High-Speed Redundanz- und Recovery Funktionen
- Integrierter VPN Server
- Ultra Thin AP mit hoher Leistungsfähigkeit

Einfache Nutzung

- 100% Netzwerk Transparent. OmniAccess Wireless läuft als Overlay Infrastruktur und erfordert keine Eingriffe in das bestehende Netz
- Höchste Kompatibilität mit bestehendem Equipment
- Plug & Play mit single Point of Control für die gesamte WLAN Security, das Funkmanagement, IDS, Rechtevergabe etc.
- No Touch automatisches Upgrade der APs
- RF Live Software im Controller integriert überwacht und zeigt kontinuierlich den Status des WLAN an

Security

- Eingebaute Application- und Identity-basierende stateful Firewall sichert jedes Device, jeden User und jeden Verkehrsfluss
- Durchgängige Sicherheitsrichtlinien im gesamten Netzwerk durch Client-basierte Rollenzuweisung durch 802.1x, MAC Adresse, SSID und Gastportal
- Echte Ende-zu-Ende Verschlüsselung nach neuesten Standards. Keine Schlüssel auf AccessPoints, daher kein Unberechtigtes Eindringen möglich.
- Unterstützt die ab 2009 geforderten rechtlichen Bestimmungen zur Protokollierung von Internetzugängen für Gastbenutzer (auch für LAN Benutzer nutzbar)
- Zusätzliche Verschlüsselung für Meshed WLAN und Remote AccessPoints
- Einzigartige Rogue-AccessPoint Erkennung und Ausschaltung



Die Funktionen von OmniAccess Wireless in der Übersicht

OAW-AOS Basis Software <ul style="list-style-type: none"> ■ WLAN Unterstützung für WPA/WPA2 ■ Automatisches RF Management 	<ul style="list-style-type: none"> ■ Location Tracking ■ Layer 3 Roaming ■ Rogue AP Erkennung
Policy Enforcement Firewall (PEF) <ul style="list-style-type: none"> ■ Stateful Firewall ■ Dynamisches Client-Policy Management 	<ul style="list-style-type: none"> ■ Captive Portal für Gastzugang ■ Rollenbasierende Rechtezuweisung ■ QoS für Daten und Voice Verkehr
Wireless Intrusion Protection (WIP) <ul style="list-style-type: none"> ■ Intrusion Detection ■ DoS Attacken Erkennung 	<ul style="list-style-type: none"> ■ Man-in-the-Middle Erkennung ■ Intrusion Prevention
Advanced AAA <ul style="list-style-type: none"> ■ External Captiv Portal Server Support 	<ul style="list-style-type: none"> ■ Auswahl des Authentication Servers aufgrund unterschiedlicher Zuweisungen ■ External Policy Control API
VPN Server <ul style="list-style-type: none"> ■ PPTP, L2TP, IPSec Terminierung 	External Services Interface (ESI) <ul style="list-style-type: none"> ■ Weiterleitung auf externe Schnittstellen ■ Load-Balancing und Health Checking
xSec Security <ul style="list-style-type: none"> ■ Zusätzliche Layer 2 AES Verschlüsselung ■ Zwischen Client-Server oder Server-Server 	Meshed Topology <ul style="list-style-type: none"> ■ Aufbau komplexer Netze über Funk ohne Anschluss an das Datennetz
Remote AccessPoint (RAP) <ul style="list-style-type: none"> ■ Terminierung von Remote AP mit L2TP/ IPSec 	<ul style="list-style-type: none"> ■ Verschlüsselung von Remote Client Verkehr und Steuerungsdaten

www.alcatel-lucent.com

