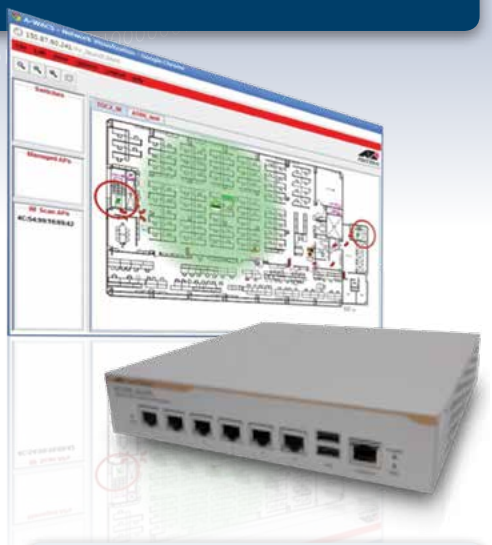
Unified Wireless Controller

WIRELESS LAN CONTROLLER SERIES FOR ENTERPRISES

The Allied Telesis Unified Wireless Controller (UWC) Series has been designed specifically to meet the requirements of enterprise organizations.



Wireless technology continues to advance as users look for ways to connect their ever-increasing array of devices. This evolution includes not only the increased bandwidth delivered by IEEE 802.11n, but also security and other functionality.

Within an enterprise environment, the rapid adoption of Bring Your Own Device (BYOD) has seen a significant increase in the number of devices that need to be supported.

The benefits of mobility and BYOD include greater flexibility, performance, and staff satisfaction, but these need to be carefully balanced with organizations' concerns around security. As the number of devices increases, so too does the size of the wireless network along with the burden of management.

Ensuring performance and staff satisfaction in a dynamic environment is particularly challenging and results in an increased Total Cost of Ownership (TCO) as a result of the Radio Frequency (RF) planning and management that is required.

An intelligent, unified control system is essential for reducing operational expenditure as it provides the ability to manage the infrastructure, security, mobility, and services — with many of these being updated automatically in real time.

The Allied Telesis UWC Series has been designed specifically to meet the requirements of enterprise organizations and addresses key concerns about mobility, security, and TCO.

The UWC Series controls a number of Allied Telesis TQ Series wireless access points and centralizes the provisioning, operation, administration, and maintenance for the entire enterprise wireless infrastructure. As a complete solution, this reduces the headaches involved with managing, upgrading, and troubleshooting, thereby improving the experience for users and IT staff.

The Allied Telesis Unified Wireless solution delivers a rich feature set that includes seamless mobility, client location tracking, and extensive security safeguards.

The UWC Series provides flexible deployment options and is available as a hardware appliance or a software-based solution.

Features

- Simplified Plug and Play
- RF management and control
- Flexible data forwarding
- Wireless IPS
- Enterprise class security
- Guest access
- End-to-end Quality of Service
- Seamless mobility
- Resilience
- Wireless controller grouping
- Graphic network visualization

The AT-UWC-Install software-based solution may be installed on any industry-standard server or on a virtual machine as a Cloud-based application. This Software-as-a-Service (SAAS) model provides a number of advantages including a simpler set-up resulting in a more cost-effective deployment.

As a hardware-based appliance, the AT-UWC-60-APL conforms to the traditional dedicated server model.

Key Features

Simplified Plug and Play

The Allied Telesis Unified Wireless Controller (UWC) detects, authenticates, and automatically configures the access points as they are installed. The discovery mechanism works at Layer 2 and Layer 3 and dramatically simplifies the task of deployment.

RF Management and Control

One of the biggest challenges with wireless solutions is the dynamic nature of the environment and the highly mobile nature of client devices. The UWC continuously monitors the RF coverage from access points and dynamically reconfigures the radios to minimize interference and improve performance. Load balancing is performed automatically to distribute clients among the available access points, which further improves the user experience. In addition, the automated management enables the UWC to alter the configuration of surrounding radios should an access point fail—ensuring no loss of coverage for client devices.

Flexible Data Forwarding

The UWC can be configured for either centralized or distributed data forwarding, enabling the solution to be tailored to meet the requirements of specific applications or environments. For environments with highly mobile clients, data traffic is encapsulated in tunnels to maintain the client's permanent IP address when the client is roaming through different subnets.

When deployed for centralized data forwarding, the UWC is responsible for the forwarding of all traffic. This allows the application of strong security policies as all traffic must traverse the UWC, where it can be forwarded or filtered as required.

In the distributed scenario, the access points are fully responsible for determining how and where to forward data — including the application of Quality of Service (QoS) or security policies.

The choice of data forwarding scheme may be applied dynamically, based on WLAN/SSID:

» Employee access should use centralized data forwarding to ensure that an organization's corporate security policies are being adhered to.

» Guest access may be provided, using distributed data forwarding as the guest data traffic is isolated from the corporate network and it is not necessary to enforce any specific security policy.

Wireless IPS

An integrated Intrusion Prevention System (IPS) is included as part of the comprehensive security features of UWC. The wireless IPS monitors the airspace and protects the network from rogue or unauthorized access points and other rogue devices. Countermeasures are taken automatically to mitigate any intrusion attempts.

Enterprise-class Security

A secure wireless network guarantees data confidentiality, integrity, mutual authentication and availability. In order to deliver the highest level of confidentiality and integrity, the UWC and controlled access points employs WPA2 (IEEE 802.11i). WPA2 is an advanced set of security features that satisfies the policy requirements for both large scale and residential networks. WPA2-Enterprise provides a centralized security model through the use of RADIUS for managing authentication and inter-operates with the IEEE 802.1x framework, supporting multiple EAP modes.

Guest Access

Guests and contractors can connect directly to the Internet without compromising network security, because they are segregated within dedicated VLANs that have no access to corporate resources. Guest access is controlled through the use of a captive portal, which provides Web-authentication for unauthorized users. The captive portal can be customized per SSID, enabling different Web portal pages to be provided for each SSID.

End-to-end Quality of Service

With the growing number of devices utilizing wireless connectivity, and the increasing prevalence of multi-media services, guaranteeing an end user's experience while using wireless is crucial. The UWC manages the QoS across the entire wireless LAN and optimizes resource use on an application by application basis. The UWC is able to prioritize each application based on its requirements for bandwidth, latency, and jitter.

Seamless Mobility

One of the benefits of a wireless solution is the mobility and freedom it delivers. As clients become increasingly mobile, maintaining connectivity while roaming from one part of the network to another becomes challenging. Seamless roaming enables a client to move an established wireless network association from one access point to another, maintaining the wireless connection and delivering constant network connectivity. Fast roaming minimizes the time required to transition between the access points, so that time-sensitive applications like Voice over WLAN (VoWLAN), or highly mobile applications like handheld data scanners don't lose information or connectivity. The UWC delivers fast roaming and seamless mobility at Layer 2 and Layer 3, so regardless of network topology, the UWC will deliver the best mobility experience possible.

Resilience

The UWC can be configured in a highly redundant topology to ensure that no single failure will result in an interruption to network coverage. If the UWC is unavailable for any reason, the associated access points will first try to connect to a redundant controller. If they are unable to locate a redundant controller, they will switch to stand-alone mode—maintaining services on a best-effort basis.

Wireless Controller Grouping

Multiple wireless controllers can be configured as a "peer group" or cluster. The resulting cluster becomes the single point for provisioning, firmware upgrade, maintenance, RF, and mobility operations.

Graphic Network Visualization

In addition to the benefits around provisioning and maintenance, the UWC provides a single user interface to monitor the performance of the wireless network. The dashboard provides an intuitive view of RF coverage, the position of wireless devices and their performance metrics—even when deployed in a multi-floor environment. The location tracking facility populates the map, giving immediate visibility of the wireless network and thereby simplifying the survey of unauthorized entities along with simplifying the task of troubleshooting.

Product Specifications

Management
Graphical User Interface (HTTP, HTTPS)
Profiling (AP, WLAN, Network)
Peer grouping (controller cluster)
Simple Network Management Protocol (SNMPv1, v2c)
Extended MIB set
Database import (.cvs)
- » Access point list
- » Peer group member list
- » Wireless client list

Firmware upgrade facility for:
- » AP operations
- » Controller operations
- » Licensing

Radio Management and Control
AP Plug and Play
- » Device detection
  - » Layer 3/IP discovery
  - » Layer 2/VLAN discovery
- » Authentication
- » Configuration

RF coverage
- » Planning (automatic/manual)
- » Continuous, adaptive monitoring
- » Interference mitigation (automatic/manual)
  - » Dynamic channel assignment
  - » Transmission power control

Data rate setting (automatic/manual)

Bridging
VLAN tagging

Wireless Distribution System
Bridging
Repeating

Mobility
Layer 2/Layer 3 seamless mobility
Fast roaming
- » Dynamic key caching/forwarding

Data forwarding (WLAN/SSID basis)
- » Centralized
- » Distributed

Security
L2 ACLs
IEEE 802.1x framework
Local RADIUS
Captive portal (Web authentication)
- » Per WLAN/SSID web pages
- » Fully customizable web pages

Wireless IDS
- » RF scanning
- » Rogue AP detection
- » Rogue client detection
- » DoS protection/mitigation

Quality of Service
Client load balancing
Bandwidth limiting
CoS-based (Class of Service) prioritization

Resilience
N-to-N high availability
AP management auto-arrangement (standalone/controlled mode switch)

Monitoring
WLAN analysis
- » Location tracking

Graphical network visualization
- » Layered design
- » Multiple maps
- » AP configuration context
- » AP performance metrics
- » Alarm display

Local/remote logging (syslog)
System status

Utilities
DHCP client
DNS client
NTP client
Logging
Statistics/metrics gathering
Troubleshooting
- » Ping
- » Traceroute

Wireless Features
Regulatory domain compliance
IEEE 802.11a/b/g
IEEE 802.11n
IEEE 802.11d
IEEE 802.11e (WMM)
IEEE 802.11h (DFS/TCP)
IEEE 802.11i (Enhanced Security)
- » WPA2-Personal
- » WPA2-Enterprise

Extended Authentication Protocol (EAP)
- » 3rd Generation Authentication and Key Agreement (EAP-AKA)
- » Flexible Authentication via Secure Tunneling (EAP-FAST)
- » GSM Subscriber Identity (EAP-SIM)
- » Transport Layer Security (EAP-TLS)
- » Tunnelled Transport Layer Security (EAP-TTLS/MSCHAPv2)
- » Protected Extensible Authentication Protocol (PEAP)
- » Generic Token Card (PEAPv0/EAP-MSCHAPv2)
- » Microsoft CHAP v2 (PEAPv1/EAP-GTC)

Scalability
Profiling
- » AP profiles ≤ 64
- » WLAN/SSID profiles ≤ 255
- » Captive portal ≤ 10

Peer grouping
- » Group ID ≤ 255
- » Group members ≤ 64

Management capability
- » Peer group:
  - » Managed APs ≤ 2.000
  - » Managed clients ≤ 8.000
- » Single controller:
  - » Managed clients ≤ 200
  - » Managed APs:
    - » AT-UWC-BaseST ≤ 210
    - » AT-UWC-210-APL ≤ 210
    - » AT-UWC-60-APL ≤ 60

WDS AP members ≤ 2

Interoperability
Web browser
- » Microsoft Internet Explorer 7
- » Microsoft Internet Explorer 8

External RADIUS
- » Microsoft Windows Server 2008 R2 onward
- » AlliedWare Plus v5.4.2-0.2 onward
- » Soliton Net Attest EPS v4.4.0 onward

Virtualization platform [1]
- » VMware vSphere (v5.1)
- » Microsoft Windows Server 2008 R2 (Hyper-V 2.0)
- » Microsoft Windows 8 (Hyper-V 2.0)

Hardware platform [1] [2]
- » CPU board x86-based [3]
- » System memory ≥ 1 GB
- » Hard disk ≥ 80 GB
- » DVD ROM
- » Ethernet port 1 x 1GE
- » VGA
- » Keyboard

Compliance

Certificates
RCM
CCC
CE
FCC
EAC
KC
TUV-T

Electromagnetic Compatibility (EMC)
CISPR22
EN 55022
EN 55024
EN 61000-3-2
EN 61000-3-3
FCC 47 CFR Part 15, Subpart B
ICES-003
IEC 61000-4-2
IEC 61000-4-3
IEC 61000-4-4
IEC 61000-4-5
IEC 61000-4-6
IEC 61000-4-8
IEC 61000-4-11
IEC 61000-4-12

Safety
cUL, UL 60950-1
CSA C22.2 No. 60950-1-07
IEC 60950-1
EN 60950-1

[1] UWC as hosted software appliance
[2] Minimum requirements
[3] Must be compatible with Cent OS 5.x

Technical Specifications

		AT-UWC-INSTALL + AT-UWC-BASEST	AT-UWC-60-APL
TARGET DEPLOYMENT		Virtualization, SaaS	Small to mid-sized enterprise
FORM FACTOR		-	desktop, 1RU
SCALABILITY	Managed APs: Factory default	10	10
	Managed APs: Maximum	up to 210	up to 60
ENVIRONMENTAL SPECIFICATIONS	Operating temperature	-	5° C - 40° C (32° F - 104° F)
	Storage temperature	-	5° C - 40° C (32° F - 104° F)
	Relative humidity	-	20% - 90%
	MTBF	-	55,000 hrs
PHYSICAL SPECIFICATIONS	Dimensions (W x D x H)	-	210 x 210 x 42 mm (8.26 x 8.26 x 1.65 in)
	Weight	-	1.5 Kg (3.3 lb)
	Case	-	Metal
POWER CHARACTERISTICS	Powering	-	AC/DC adapter
	Input voltage	-	100 V - 240 V
	Frequency	-	47Hz – 63Hz
	Max consumption	-	≤35 W
INTERFACES	Type	NIC	Ethernet
	Standard	-	IEEE 802.3 / IEEE 802.3u / IEEE 802.3ab
	Ports	1	6
	Connectors	-	RJ-45 female
	Type	-	Serial console
	Standard	-	RS232
	Ports	-	1
	Connectors	-	RJ-45 female
	Type	-	USB 2.0
	Standard	-	USB-IF (host controller class)
	Ports	-	2
	Connectors	-	Type A receptacle

Ordering Information

AT-UWC-60-APL
Wireless LAN controller for enterprises (hardware appliance)

AT-UWC-Install [4]
Wireless LAN controller for enterprises (software appliance installer)

AT-UWC-BaseST [5]
Basic license, supporting 10 managed access points

AT-UWC-TrialST [4]
Free 30-day trial license, supporting 10 managed access points

Associated Products

AT-UWC-NN-Lic
License upgrade, adding "NN" of managed access points; "NN" may be 10, 20, 50, 100, and 200

AT-RKMT-APL1
19 in rackmount kit for AT-UWC-60-APL

AT-CONSOLE-CABLE-RJ45
Console cable with DB9 female, and RJ-45 connectors, pack of 10 pieces

AT-TQ2450
Enterprise-class, wireless access point with IEEE 802.11a/b/g/n dual radio

[4] The item can be obtained from the Allied Telesis website, at alliedtelesis.com/support

[5] This item is required to enable the operation and full feature set of hosted software appliance. Upgrading of managed APs via AT-UWC-NN-Lic may be done after the basic license has been loaded.

Allied Telesis
the solution : the network

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

617-000486 Rev A