4ipnet®

BUYER'S GUIDE

WHG-SERIES FEATURE OVERVIEW

AP MANAGEMENT

- L2 / L3 AP Management
- Tunneled AP Management (CAPWAP-based)
- L2 / L3 Roaming between AP
- Automatic AP Discovery
- Automatic AP Provisioning
- AP Batch Upgrade & Firmware Management
- Configuration Backup & Restore
- Map View of Managed APs
- AP Load Balancing
- Rogue AP Detection
- Network Traffic & Hardware Performance Statistics
- Real-time Event Notifications & AP Status Report via E-mail

USER MANAGEMENT

- 802.1X, MAC/IP Address, or Browser-based User Authentication
- Multiple Authentication Servers (RADIUS, POP3, LDAP, etc.)
- Billable On-Demand Accounts
- User Blacklists
- Customizable Captive Portals with Walled Garden
- Simple Guest Access
- Role-based User Policies
- Schedule-based QoS, Firewall, Routing Profiles per Role
- User Session Control (e.g. Idle Timeout, Session Limit)
- User Activity Monitoring
- SMS & Payment Gateway Support

WHG

NETWORK MANAGEMENT

- Multiple Service Zones (Virtual Networks)
- IEEE802.1Q-in-Q Double-Tagged VLAN
- VLAN Tag / Port-based Configuration
- L2 / L3 Traffic Isolation
- Cross Gateway Roaming
- Built-in DHCP Server / Relay
- Built-in Proxy Server
- Built-in NAT with Conversion Log
- Local DNS Records
- VPN (Local, Site-to-Site, Remote)
- Zero Configuration IP Plug-and-Play
- HTTPS Redirect (User Login)
- Monitor IP List
- Direct Interface with Micros Opera Hotel PMS

SYSTEM MANAGEMENT

- High Availability / Redundancy
- Multiple-Tiered Administrator Access Privileges
- Configurable Management IP Address Range for Administrator Access
- Automatic Time Synchronization (NTP)
- Built-in Certificate Management
- Automatic Periodic System Backup
- Built-in Network Troubleshooting Utilities (e.g. packet capture, tracert)
- Detailed Logs and Reports (DHCP Lease Log, Session List, Configuration Change Log, RADIUS Log, etc.)
- External Logging via FTP or SMTP
- IPv4 and IPv6 Compatible

Note: Feature availability is subject to software version

BENEFITS

Lowered TCO and increased ROI

In addition to no license fees, the WHG appliance provides automatic AP discovery and template-based AP provisioning to simplify WLAN deployment, helping organizations minimize costs and maximize return on their WLAN infrastructure.

Reduced maintenance and troubleshooting efforts

Centralized management of both local and branch networks reduces the need for an army of IT personnel at each location, while real-time e-mail notifications reduces downtime and prevents lost revenue.

Complete visibility of network and user status

Detailed logs and statistics allow network operators to monitor network usage, analyze user behavior, and trace the source of any illegal or unsanctioned activity.

Flexible and caters to all deployment needs

In addition to providing multiple virtual networks under a single appliance, the WHG controller offers IEEE 802.1Q-in-Q for extremely large deployments that need to limit broadcast domains. Multiple authentication servers and methods can be simultaneously enabled depending on deployment needs, while customizable captive portals allow organizations to perform venue branding or serve important information.

Improved network performance and security

Comprehensive schedule and role-based user policies such as bandwidth control, QoS, and firewall profiles help guarantee that the network is not abused by certain individuals. Furthermore, fine-grained Layer 2 traffic isolation can be utilized to prevent communication in sensitive network environments.

FAQ

Who should buy the WHG controller?

The WHG controller appliance is designed for network operators and organizations that wish to provide reliable, secure, and high-performance Wi-Fi connectivity in the most cost-effective way. 4ipnet has distilled all the essential and commonly used features from the complex WLAN controller, and offers them at a much more competitive price point. Hotels, enterprises, campuses, and other public environments can leverage the WHG's features to protect critical network resources and manage network access, which in turn improves productivity and customer satisfaction.

How does the WHG differ from other "free" AP management solutions?

While the "free" AP management solutions offered by other vendors may be sufficient in managing APs and performing simple user authentication, they do not contain the fine-grained user policy enforcement, user analytics, and network management features needed by network operators in public Wi-Fi settings. These solutions also do not have the option of tunneling traffic back to the controller, and have limited authentication and deployment options.

Why should you invest in a WHG controller?

User management is critical in any public or enterprise network, and not only for security concerns. In an unmanaged network, individual users can consume the entire bandwidth through inappropriate usage, leading to poor connectivity for others. By enforcing role-based policies, user complaints can be reduced and long-term troubleshooting costs can be minimized, allowing organizations to easily recoup their initial investment. Furthermore, many countries have regulations that require operators of public Wi-Fi networks to keep track of all usage data, which can be accomplished through the WHG controller's detailed network and user statistics. Finally, the ongoing maintenance efforts required after initial deployment can be streamlined and made more efficient by the WHG's centralized and detailed management interface. In the long run, deploying the WHG controller can help organizations acheive much greater cost savings, some of which are not readily apparent.

What is the advantage over "controller-less" solutions?

There has been much hype regarding the "controller-less" architecture, which typically takes the form of controller functionality built into individual access points or a completely cloud-based/virtualized management interface. However, not all of this hype is exactly true. First and foremost, there is always a controller - the only difference being whether or not you control the actual hardware. By purchasing a physical appliance, you have total control over where the appliance is to be deployed (e.g. in a data center you specify), which is optimal from a corporate security standpoint. And aside from the free management solutions mentioned in the previous page, there is always a cost for the controller - it just is paid for in different ways. For vendors that build controller functionality into APs, the cost may be distributed into the cost of the APs, while other vendors (typically cloud-based systems) may charge license fees or subscriptions on an annual basis.

The following is a list of complications or issues that may arise when deploying controller-less WLAN solutions:

1. When most network elements are on-premise, a cloud-based controller will suffer in performance as it needs to traverse the Internet and all corporate firewall and security policies in order to communicate with other network elements, such as the authentication database.
2. By moving controller functionality to APs and using them as the point of handoff for untrusted traffic may degrade network performance, while inducing additional security risks. For example, in a controller-based WLAN, untrusted traffic can be tunneled back to the controller, where it can then be directed to other network segments for quarantine or analysis. However, in an AP-only infrastructure, preventing this traffic from traversing the secure network it is much more difficult and requires many workarounds.
3. Even though many cloud-based solutions are hosted in data centers with pristine uptime records, this does not necessarily mean that they are as reliable as on-premise controllers. One of the major deficiencies is revealed when there is a power outage or AP failure. Without the controller coordinating self-healing, a hole is created in the Wi-Fi coverage that ultimately leads to lost productivity. Furthermore, all user information would be lost during this service interruption, as all information is cached on the AP itself.

All in all, the controller-less architecture may provide some advantanges and flexibility in certain deployment cases, but the benefits are typically accompanied by some deficiencies or myths that may not be very obvious on first sight.

WHG MODELS

The table below lists the primary differences between each WHG model, including capacity, size, and other hardware characteristics. From the software standpoint, all of the WHG models contain the same feature set (most of which are listed in page 1 of this document), except for a specific few functions such as high availability. For detailed descriptions of the software features provided by the WHG models, please consult the product datasheets.

HARDWARE SPECIFICATIONS

	WHG311	WHG315	WHG405	WHG711	WHG801
					
Managed APs	30	50	150	500	1200
Local Accounts	3000	4000	6000	15000	30000
On-Demand Accounts	3000	4000	6000	15000	30000
Form Factor	Desktop	19" Rack-mount (1U)	19" Rack-mount (1U)	19" Rack-mount (1U)	19" Rack-mount (2U)
WAN Ports	2 x GbE	2 x GbE	2 x GbE	2 x GbE 2 x 1G SFP	2 x GbE 2 x 1G SFP 1 x 10G SFP
LAN Ports	8 x GbE	8 x GbE	4 x GbE	10 x GbE 2 x 1G SFP	6 x GbE 6 x 1G SFP 1 x 10G SFP
Dimensions (W x D x H; cm)	33.0 x 18.0 x 4.5	43.0 x 28.0 x 4.4	42.6 x 23.6 x 4.4	42.6 x 45.0 x 4.4	43.0 x 58.0 x 8.8
Weight	1.81 kg	5.99 kg	5.60 kg	8.00 kg	19.00 kg
High Availability / Redundancy	No	No	Yes (1+1)	Yes (1+1)	Yes (1+1)
Power Redundancy	No	No	No	No	Yes

Note: Capacity limits may vary depending on configuration parameters