NETGEAR® PROSAFE®

ProSafe® 16-AP Wireless Management System Data Sheet
WMS5316

Central Configuration for up to 16 Wireless Access Points

Utilizing multiple wireless access points throughout the network provides the performance, coverage, and reliability required by businesses of all sizes. However, individually configuring, deploying, and managing multiple standalone devices can quickly become resource intensive, creating a significant burden on scarce IT resources. The NETGEAR ProSafe WMS5316 Wireless Management System resolves this quandary. With support for up to 16 wireless access points, it provides a single location to configure and manage all wireless access points in the network.

One Configuration

Mimicking the set up process of a single access point, the NETGEAR ProSafe WMS5316 Wireless Management System supports up to 16 wireless access points to provide a single location with which to centrally configure the entire wireless network. The WMS5316 is the ideal solution for businesses and schools with 50-200 users delivering centralized management via an intuitive interface – without the costs that accompany full-service wireless controllers. With a single entry of wireless parameters and security settings that can be simultaneously pushed to all wireless access points on the network, the system dramatically simplifies the deployment and daily management of the wireless network.

Automatic Management

The WMS5316 Wireless Management System monitors the wireless network to ensure optimal performance and respond to changes in the RF environment. Once a day, based on a schedule it will automatically re-assign channels and adjust RF parameters for maximum connectivity. WMS5316 can ensure that no single access point is overloaded continuously, by limiting the maximum number of clients per access point.

Access Points

Supporting a wide portfolio of standard NETGEAR access points, the WMS5316 Wireless Management System enables customers to select the right access points for their needs, even mixing models to provide the right coverage, as well as an upgrade path as technology changes. Supported models include 802.11g access points as well as professional caliber dual band 802.11n access points.

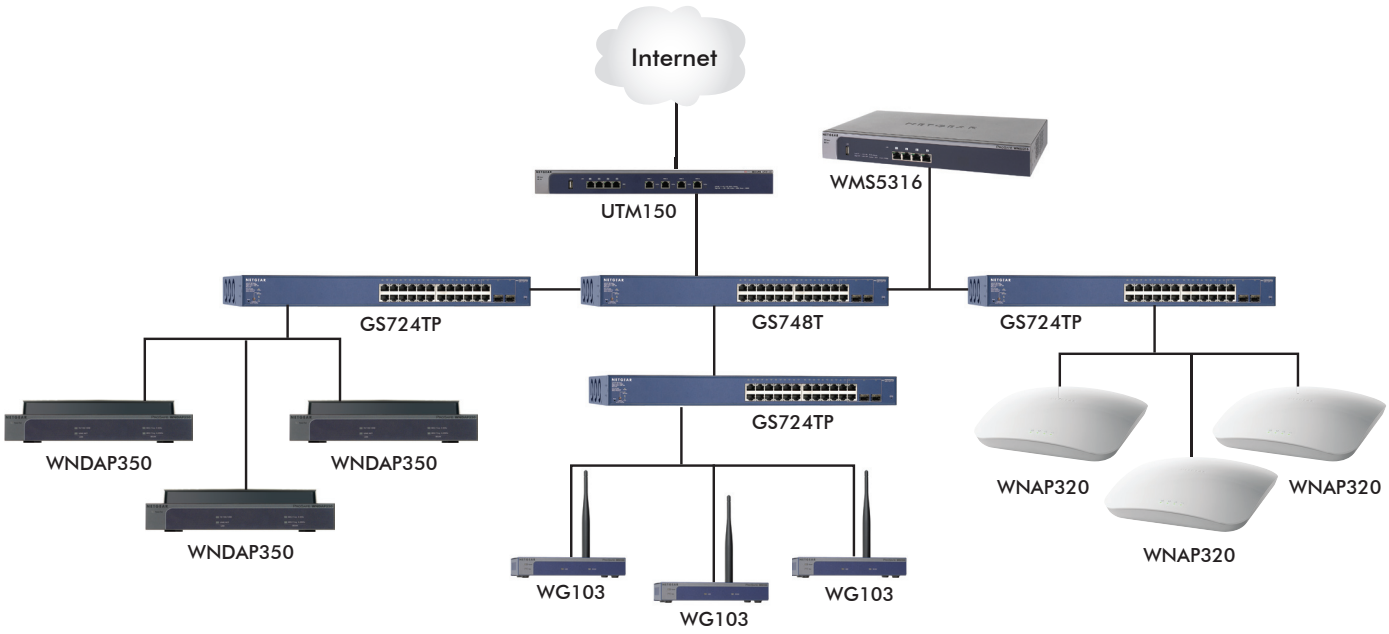
DIFFERENCES BETWEEN WMS5316 AND A FULL SERVICE WIRELESS CONTROLLER WC7520

	WMS5316	WC7520
Main functionality	Wireless Management	Wireless Controller
Number of access points	Up to 16	Up to 50 per Controller - Up to 150 per Stack
Central configuration	Yes	Yes
Multiple SSIDs, VLANs	Yes	Yes
Automatic RF management	Yes - Once a day (schedule)	Yes - Continuous healing
Limitation of number of clients per AP	Yes	Yes
RF Planning before deployment	No	Yes - Based on Floor plans and computed coverage
Dynamic RF with heat map after deployment	No	Yes - Real time view of wireless connectivity
Self Healing Wireless network	No	Yes - Automatic WLAN healing after loss of AP or due to RF interferences
Dynamic Load Balancing	No	Yes - Based on number of clients per AP or client Signal strength/Data rate threshold
L2 and L3 Fast Roaming support	No	Yes
Built-in AAA server, LDAP support	No	Yes
Captive portal with Guest management	No	Yes
Summary	Access Points configuration	Dynamic RF capabilities

24/7 TECHNICAL SUPPORT*

1-888-NETGEAR (638-4327)
Email: info@NETGEAR.com

NETGEAR PROSAFE LIFETIME WARRANTY*



FEATURES AND BENEFITS

SUPPORTED ACCESS POINT MODELS		MINIMUM FIRMWARE VERSION REQUIRED
Up to 16 mixed access points are simultaneously supported by the Wireless Management System (WMS5316)	WNDAP360 Prosafe Dual Band 802.11n Wireless Bccess Point	WNDAP360_V2.0.7
	WNDAP350 ProSafe Dual Band 802.11n Wireless Access Point	WNDAP350_V2.0.27
	WNAP320 ProSafe 802.11n Wireless Access Point	WNAP320_V2.0.3
	WNAP210 ProSafe 802.11n Wireless Access Point	WNAP210_V2.0.27
	WG103 ProSafe 802.11g Wireless Access Point	WG103_V2.0.37

WMS5316 KEY FEATURES	BENEFITS
Access Point Discovery	Discovers NETGEAR Wireless Access Points everywhere on the LAN
Wireless Performance Optimization	Allows centralized RF management, Quality of Service (QoS)
Wireless Security Configuration	Streamlines security configuration tasks
Wireless Network Monitoring	Summarizes managed access point status, rogue access points, wireless clients status, and wireless network usage
Maintenance Operations	Provides remote management, and firmware updates for the managed access points on the LAN

NETWORK CONFIGURATION LEVELS	EASE OF USE EVEN FOR NON-PROFESSIONAL USERS
Basic Settings for a Typical Network	The basic settings fit the most common network configurations. All wireless access points belong to the same organization or business.
Advanced Settings for Access Point Groups	If completely separate networks share a single LAN, advanced settings allow set up of access point groups. For example, a shopping mall might need access point groups if several businesses share a LAN, but each business has its own network.

TECHNICAL SPECIFICATIONS

IP AND VLAN CONFIGURATION	
Own IP Address	Fixed IP address only (no DHCP client mode for the Wireless Management System itself)
DHCP Server	The Wireless Management System can function as a DHCP server. Multiple DHCP server pools can be added for different VLANs.
VLANs for the Wireless Management System	Untagged Management VLAN (default) or dedicated management VLAN (tagged)
VLANs for the Access Points - Multiple SSIDs	For each access point group, up to 8 tagged VLANs can be configured per radio, a maximum of 16 SSIDs per group for both the radios (2.4 GHz and 5 GHz).
ACCESS POINT DISCOVERY	
Automatic Discovery	Layer 2 discovery method if the Wireless Management System and all the wireless access points on the LAN are in the same IP subnet
IP Discovery	Layer 3 discovery method if the the Wireless Management System and the wireless access points use different IP subnets. IP discovery can be used to find the access points for each subnet, one subnet at a time.
ACCESS POINT MANAGEMENT	
Managed Access Point Assignment	After the Wireless Management System discovers the access points, they can be “added” and set “managed” by the Wireless Management System
Access Point Information Edition	Name (modifiable), model (cannot be modified), user name for logging in to the access point (cannot be modified), password (modifiable)
Access Point Groups	Initially all the wireless access points belong to the same access point group. Up to 8 independent groups of managed access points can be configured and each access point can belong to only one group.

TECHNICAL SPECIFICATIONS	
WIRELESS CONFIGURATION - RF	
Centralized Automatic RF Management	Automatically allocates access points channel and RF power based on each access point performance in the local environment. For example, if an access point experiences interference on a channel, the Wireless Management System allocates a different channel to that access point.
Selectable Corporate Channel List for Auto Channel Selection	For channel list, the administrator will be able to select what are the allowed corporate channels for 2.4GH and 5GHz band. The Channel allocator will assign the access points within the corporate allowed channels.
RF Management Schedule	Channel allocation can be scheduled on a daily/weekly basis, once a day at a specified time
Client Aware RF Management	If enabled, the Wireless Management System will not modify the channel for an access point with associated clients that would be impacted by the channel change. The Wireless Management System will wait for the next scheduled channel allocation to adjust the channel.
Usage-aware RF Management	If enabled, the Wireless Management System will not modify the channel for an access point that is switching more than 1 Mbps of wireless data traffic
Custom RF Settings	Radio mode preference and 2.4 GHz or 5 GHz band selection for each access point group
Advanced Wireless Settings for Access Point Groups	If centralized automatic RF management disabled, for each radio band (802.11 b/bg/ng and 802.11 a/na) the Wireless Management System can centrally configure each access point group with common settings: turn radio on, wireless mode, MCS index/data rate, channel width (11n only), guard interval (11n only), output power, RTS threshold (0-2347), fragmentation length (256-2346), beacon interval (100-1000), aggregation length (1024-65535, 11n only), AMPDU (11n only), RIFS transmission (11n only), enable Wi-Fi Multimedia™ (WMM), DTIM interval (1 and 255), preamble type (11b/bg only), access point channel
WIRELESS CONFIGURATION - QOS	
WMM Quality of Service	WMM automatically prioritizes traffic for both upstream traffic from the stations to the access points (station EDCA parameters) and downstream traffic from the access points to the client stations (AP EDCA parameters). Basic QoS settings for all the access points or advanced QoS settings for each access point group are available.
WMM Queues in Decreasing Order of Priority	• Voice: The highest priority queue with minimum delay, which makes it ideal for applications like VOIP and streaming media • Video: The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue • Best Effort: The medium priority queue with medium delay is given to this queue. Most standard IP application will use this queue • Background: Low priority queue with high throughput. Applications, such as FTP, which are not time-sensitive but require high throughput can use this queue.
WMM Power Save option	WMM Power Save helps conserve battery power in small devices such as phones, laptops, PDAs, and audio players using IEEE 802.11e mechanisms.
Max Number of Clients per Access Point	Allows the Wireless Management System to set maximum number of client's limitation per access point or per radio – ensuring that no single access point is overloaded continuously.
WIRELESS CONFIGURATION - SECURITY	
Security Profiles Lists	Up to eight (8) security profiles per radio can be configured for all the managed access points. If several access point groups have been defined, then up to eight (8) security profiles per access point group can be centrally configured.
Security Profiles settings	Name, wireless network name (SSID), broadcast wireless network name, network authentication (open, Shared Key, legacy 801.1X WPA and WPA2 with RADIUS, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK), data encryption (none, WEP, TKIP, AES, TKIP+AES), Wireless client security separation (wireless clients can't communicate each other), VLAN ID
MAC Authentication	Block the network access privilege of the specified stations through all managed access points or through one or several specific access point group.
Local MAC Address Database	The managed access points use the local MAC address table for access control.
Remote MAC Address Dabase (Radius)	The managed access points use the MAC address table on an external 802.1x Radius server on the LAN for access control.
801.1x RADIUS Server Settings	Four types of 801.x RADIUS server can be configured per access point group: • Primary authentication server (main RADIUS server used for authentication) • Secondary authentication server: for use if the primary authentication server fails or is unreachable • Primary accounting server: used for accounting on the network • Secondary accounting server: for use if the primary accounting server fails or is unreachable
Guest Access	Guest access settings are useful when configuring a public wireless network (preferably secured VLAN-SSID). The guest access feature is not a captive portal. Guest access settings aim to: • Redirect the user to a specified internal Guest web page, or external guest portal • Allow users to enter simple information such as an email address • Identify sessions and track usage When guest access is configured, it redirects the first HTTP (TCP, port 80) request to the default guest access page. The last 512 IP access and entered email address are recorded.
Rogue Access Point Detection	Unidentified access points that use the SSID of a legitimate network can present a serious security threat. Rogue access point detection is enabled by default on all the managed access points. To detect rogue access points, the managed access points scan the wireless environment on all available channels, looking for unidentified access points.
WIRELESS NETWORK MONITORING	
Monitoring Summary	Summary of the managed access points status, rogue access points detected, wireless stations connected, wireless management system information and wireless network usage
Managed Access Point Status	Displays status for the managed access points and details per managed access point/group that includes configuration settings, current wireless settings, current clients and current traffic statistics
Rogue Access Points	Basic status displays the count of rogue or neighboring access points discovered by the managed access points (instantly and in the last 24 hours): • Rogue access points reported • Rogue access points in same channel • Rogue access points in interfering channels

TECHNICAL SPECIFICATIONS	
WIRELESS NETWORK MONITORING	
Wireless Client Status	The client status list specifies detailed information about each client node currently associated with managed access points
Wireless Network Usage	Network usage statistics display plots of average received/transmitted network traffic per managed access point. Three different plots show Ethernet, Wireless 802.11 b/bg/ng and 802.11 a/na mode traffic separately.
Wireless Network Topology	• Display topology graph of the managed access points (connectivity graph). The managed access points icons can be moved on the topology background and their locations saved for later displays. • Background image file: a floor map jpg/gif image of size 800 x 600 can be uploaded and displayed as the topology background.
DHCP Leases	Displays DHCP details for wireless clients which have been allocated IP addresses by the integrated DHCP server or the multiple DHCP server pool (VLANs)
MANAGEMENT	
Management Interface	HTTP, SNMP v1/v2c, telnet, Secure Shell (SSH)
Log Delivery	If available Syslog server on the network, the wireless management system and managed access points can send all logs. Logs are also available on the GUI and ready to download (log export file).
Diagnostics	Managed Access Points Ping
Maintenance	Save/restore configuration, restore to factory defaults, admin password change, add user (read-only), firmware upgrade via Web browser for the wireless management system and the managed access points.
SNMP (Wireless Management System)	SNMP v1/v2c
SNMP (Access Point Groups)	SNMP v1/v2c
HARDWARE	
Gigabit RJ45 Ports LAN	Switch 4-port 10/100/1000
Flash Memory/RAM	64 MB/512 MB
USB Port	1
Major Regulatory Compliance	FCC Class A, CE, WEEE, RoHS
Storage and Operating Temperatures	Operating Temperature 0°-45° C (32°-113° F), Storage Temperature -20°-70° C (-4°-158° F)"
Humidity	Operation 90% Maximum Relative, Storage 95% Maximum Relative
Electrical Specifications	100-240V, AC/50-60 Hz, Universal Input, DC 5V/5A (internal power supply)
Dimensions (W x H x D) cm	33 x 4.3 x 20.9
Dimensions (W x H x D) in	13 x 1.7 x 8.2
Weight kb/lb	2.1/4.6
System Requirements	Internet Explorer® 5.0 or higher or Mozilla Firefox® 1.0 or higher
Package Contents	Wireless Management System (WMS5316), Ethernet cable, power cord, installation guide, resource CD
Warranty	ProSafe Lifetime
ORDERING INFORMATION	
North America	WMS5316-100NAS
Europe	WMS5316-100EUS
Asia	WMS5316-100AUS
PROSUPPORT SERVICE PACKS	
OnCall 24x7, Category 1	PMB0331-100 (US), PMB0331 (non-US)
XPressHW, Category 1	PRR0331

NETGEAR®

350 E. Plumeria Drive
San Jose, CA 95134-1911
1-888-NETGEAR (638-4327)
E-mail: info@NETGEAR.com
www.NETGEAR.com

© 2010 NETGEAR, Inc. NETGEAR, the NETGEAR Logo, NETGEAR Digital Entertainer Logo, Connect with Innovation, FrontView, IntelliFi, PowerShift, ProSafe, ProSecure, RAIDar, RAIDiator, RangeMax, ReadyNAS, Smart Wizard, X-RAID, and X-RAID2, are trademarks and/or registered trademarks of NETGEAR, Inc. and/or subsidiaries in the United States and/or other countries. Mac and the Mac logo are trademarks of Apple Inc., registered in the U.S. and other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. All rights reserved.

*Free basic installation support provided for 90 days from date of purchase. Advanced product features and configurations are not included in free basic installation support; optional premium support available.