NETGEAR® PROSAFE®

ProSafe® 5-AP Wireless Management Software WMS105

Data Sheet

Easy to use wireless network management for small networks

The NETGEAR ProSafe 5-AP Wireless Management Software is an easy to use tool to simplify the set up and maintenance of small wireless networks. Supporting up to five access points, the WMS105 Software provides a single location to configure and upgrade the entire wireless network. Priced less than a single access point, the WMS105 software provides significant time savings and simplifies the deployment of a wireless network.

Deployment

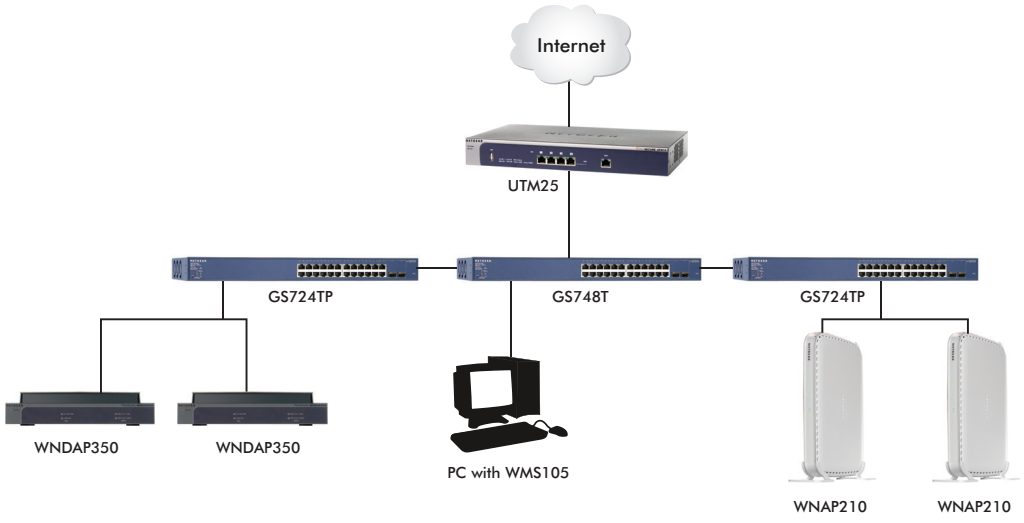
Mimicking the set up process of a single access point, the easy to use WMS105 Software enables even novice users to adopt a centralized management architecture. With automatic discovery of all supported access points in the network, the WMS105 Software speeds the configuration of a multiple access point network.

Security

By centrally configuring all access points in the network, the WMS105 Software ensures identical wireless parameters and security settings throughout the coverage area so that clients, guests and unwanted intruders all get appropriate access to network resources. Setting up WPA2 encryption keys to keep traffic safe from prying eyes and MAC authentication lists to only allow approved devices on the wireless network can be done once and sent out to the entire network. When used with ProSafe Access Points, the WMS105 software can configure a guest SSID for the wireless network to allow visitors safe access to the Internet without allowing visibility to company files or resources. Additionally, 802.1x network authentication can be applied for further verification of clients' rights to be on the network.

Access Points

Supporting a wide portfolio of standard NETGEAR access points, the WMS105 Software 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. The access points retain their standalone capabilities and do not require a conversion to be managed by the WMS105 software. Supported models include SOHO-class 802.11G access points as well as professional caliber dual band 802.11N access points.



24/7 TECHNICAL SUPPORT*

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

FEATURES AND BENEFITS

SUPPORTED ACCESS POINT MODELS		MINIMUM FIRMWARE VERSION REQUIRED
Up to 5 mixed access points are simultaneously supported by the Wireless Management Software WMS105	WNDAP350 ProSafe Dual Band 802.11n Wireless Access Point	WNDAP350_V2.0
	WNDAP330 ProSafe Dual Band 802.11n Wireless Access Point	WNDAP330_V3.0.4
	WNAP210 ProSafe 802.11n Wireless Access Point	WNAP210_2.0.8
	WG302v2 ProSafe 802.11g Wireless Access Point	5.2.3
	WG103 ProSafe 802.11g Wireless Access Point	WG103_2.0
	WN802Tv2 802.11n Wireless Access Point	WN802Tv2_V3.1.2
	WG602v4 802.11g Wireless Access Point	V1.1.0

	RF AND QOS CONFIGURATION		SECURITY CONFIGURATION					MANAGEMENT AND MONITORING			
ACCESS POINTS "MANAGED" FEATURES	AUTO CHANNEL	QOS / WMM	SECURITY PROFILES PER RADIO	VLAN CONFIG	ROGUE ACCESS POINTS	GUEST ACCESS	CLIENT SEPARATION	REMOTE ACCESS SSH/TELNET	TOPOLOGY	SYSLOG	NTP (TIME SERVER)
WNDAP350	Yes	Yes	8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WNDAP330	Yes	Yes	8	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
WNAP210	Yes	Yes	8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WG302v2	Yes	Yes	8	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
WG103	Yes	Yes	8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WN802Tv2	Limited	No	1	No	No	No	No	No	No	No	No
WG602v4	Limited	No	1	No	No	No	No	No	No	No	No

WMS105 KEY FEATURES	BENEFITS
Access Point Discovery	Discovers NETGEAR Wireless Access Points everywhere on the LAN
Single Location to Configure Everything	Simplifies wireless deployment
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 firmware updates for the managed access points on the LAN

TECHNICAL SPECIFICATIONS

ACCESS POINT DISCOVERY	
Automatic Discovery	MAC address automatic discovery method if the Wireless Management Software and all the wireless access points on the LAN are in the same IP subnet
IP Discovery	If the Wireless Management Software and the wireless access points are in different IP networks, then 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 Software discovers the access points, they can be "added" and set " managed" by the Wireless Management Software
Access Point Information Edition	Name (modifiable), model (cannot be modified), user name for logging in to the access point (cannot be modified), password (modifiable)
WIRELESS CONFIGURATION - RF	
Centralized RF Management*	Allocates access point channels 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 Software allocates a different channel to that access point
RF Management Schedule	Channel allocation can be scheduled on a per day/per week basis, once a day at a specified time
Client-aware RF Management*	If enabled, the Wireless Management Software will not modify the channel for an access point with associated clients that would be impacted by the channel change. The Wireless Management Software will wait for the next scheduled channel allocation to adjust the channel
Usage-aware RF Management	If enabled, the Wireless Management Software 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
Advanced Wireless Settings	If centralized automatic RF management disabled, for each radio band (802.11b/bg/ng and 802.11a/na) the Wireless Management Software can centrally configure each access point 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)

TECHNICAL SPECIFICATIONS	
WIRELESS CONFIGURATION - SECURITY	
Security Profile Lists	Up to 8 (eight) security profiles per radio can be configured for all the managed access points.
Security Profile 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 cannot communicate each other), VLAN ID
MAC Authentication*	Block the network access privilege of the specified stations through all managed access points
Local MAC Address Database*	The managed access points use the local MAC address table in WMS105 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: • 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. The guest access feature is not a captive portal. Guest access settings aim to: • Redirect the user to a specified external guest portal • Allow users to enter simple information such as an email address When guest access is configured, it redirects the first HTTP (TCP, port 80) request to the external default guest access page
Rogue Access Points 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, and WMS105 system information
Managed Access Points Status	Displays status of the managed access points that includes total number of access points, number of down access points, and healthy/major/ critical status of pingable access points. Advanced monitoring per access point provides complete read-only status of current settings and associated wireless clients
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): • Reported rogue access points • Rogue access points in same channel • Rogue access points in interfering channels
Wireless Client Status	The client status list specifies detailed information about each client node currently associated with managed access points
MANAGEMENT	
Management Interface	Windows® user interface, SNMP v1/v2c for external SNMP monitoring, telnet and Secure Shell (SSH) for remote access
Log Delivery*	Logs are available for manual download (log export file)
Diagnostics	Managed access points ping
Maintenance	Save/restore configuration, WMS105 admin password change, firmware upgrade via Web browser for the Wireless Management Software and the managed access points, access points reboot
SNMP (Wireless Management Software)	SNMP v1/v2c
SOFTWARE SPECIFICATIONS	
System Requirements	• Windows XP 32 bit and 64 bit versions • Windows 7 32 bit and 64 bit versions
Software Utilization	• Wireless Management Software (WMS105) does not need to be used all the time • WMS105 can be shut down when no configuration tasks or no monitoring actions are needed
Warranty	NETGEAR 90-day Warranty (media)
Package Content	Wireless Management Software (WMS105) Resource CD
ORDERING INFORMATION	
All regions	WMS105-10000S

* Please refer to the Access Points "Managed" Features Matrix

NETGEAR®

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

*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.