



WAH7003

3G Portable Router

Version 1.00
Edition 1, 06/2015

User's Guide

Default Login Details

LAN IP Address	http://192.168.0.254
User Name	admin/guest
Password	admin/guest

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the WAH7003 and access the Web Configurator.

Contents Overview

User's Guide	8
Introduction	9
The Web Configurator	13
Technical Reference	19
Home	20
WAN	24
Network	32
SMS	37
Wi-Fi	40
Firewall	59
System	63
Troubleshooting	72

Table of Contents

Contents Overview	3
Table of Contents	4
Part I: User's Guide	8
Chapter 1	
Introduction.....	9
1.1 Overview	9
1.2 Ways to Manage the WAH7003	9
1.3 Good Habits for Managing the WAH7003	10
1.4 Hardware Connections	10
1.5 Turn on/off the WAH7003	10
1.6 OLED Display and Icons	10
1.7 Resetting the WAH7003	11
1.7.1 How to Use the Physical Reset Button	11
Chapter 2	
The Web Configurator	13
2.1 Overview	13
2.2 Login Accounts	13
2.3 Access	13
2.4 Navigating the Web Configurator	14
2.4.1 Title Bar	15
2.4.2 Navigation Panel	16
Part II: Technical Reference.....	19
Chapter 3	
Home.....	20
3.1 Overview	20
3.2 Status	20
3.3 Wizard	21
3.3.1 LAN Settings	22
3.3.2 WAN Settings	22
3.3.3 Wi-Fi Settings	23

Chapter 4	
WAN	24
4.1 Overview	24
4.1.1 What You Can Do in this Chapter	24
4.2 Connection Operation Screen	25
4.3 User Profile Screen	26
4.4 2/3G Modem Settings Screen	27
4.5 2/3G Modem Information Screen	28
4.6 Unlock SIM Screen	28
4.7 SIM Lock/Unlock Configuration Screen	29
4.8 Change PIN Code Screen	29
4.9 PLMN 2G/3G Modem Screen	30
Chapter 5	
Network	32
5.1 Overview	32
5.1.1 What You Can Do in this Chapter	32
5.2 LAN IPv4 Screen	32
5.3 LAN DNS Name Screen	33
5.4 DHCP Server Screen	33
5.5 Static DHCP Screen	34
5.6 Leased Hosts Screen	35
Chapter 6	
SMS	37
6.1 Overview	37
6.1.1 What You Can Do in this Chapter	37
6.2 New Message > Send SMS Screen	37
6.3 Local Inbox Screen	37
6.4 Local Outbox Screen	38
Chapter 7	
Wi-Fi	40
7.1 Overview	40
7.1.1 What You Can Do in this Chapter	40
7.1.2 What You Need to Know	41
7.2 Wi-Fi Basic Screen	41
7.3 WPS Screen	44
7.4 MAC Filter Screen	45
7.5 Station List Screen	46
7.6 Technical Reference	47
7.6.1 Wireless Network Overview	47
7.6.2 Additional Wireless Terms	49

7.6.3 Wireless Security Overview	49
7.6.4 Signal Problems	51
7.6.5 WiFi Protected Setup (WPS)	52
Chapter 8	
Firewall	59
8.1 Overview	59
8.1.1 What You Can Do in this Chapter	59
8.2 IP Filter Screen	59
8.3 MAC Filter Screen	60
8.4 Content Filter Screen	61
Chapter 9	
System	63
9.1 Overview	63
9.1.1 What You Can Do in this Chapter	63
9.2 About Screen	63
9.3 Configuration Screen	64
9.3.1 Backup	64
9.3.2 Restore	64
9.3.3 Reset to Default	65
9.4 Firmware Upgrade Screen	65
9.5 Power Saving Screen	66
9.6 Password Screen	66
9.7 Date and Time Screens	67
9.7.1 Date Screen	67
9.7.2 Time Zone Screen	68
9.8 Language Screen	69
9.9 System Log Screens	70
9.9.1 Log Setting Screen	70
9.9.2 Log Display Screen	71
9.10 Reboot Screen	71
Chapter 10	
Troubleshooting.....	72
10.1 Overview	72
10.2 Power, and Hardware Installation	72
10.3 WAH7003 Access and Login	72
10.4 Internet Access	74
10.5 Wireless Connections	74
10.6 Getting More Troubleshooting Help	75
Appendix A Customer Support	76

Appendix B Legal Information..... 82

Index 88

PART I

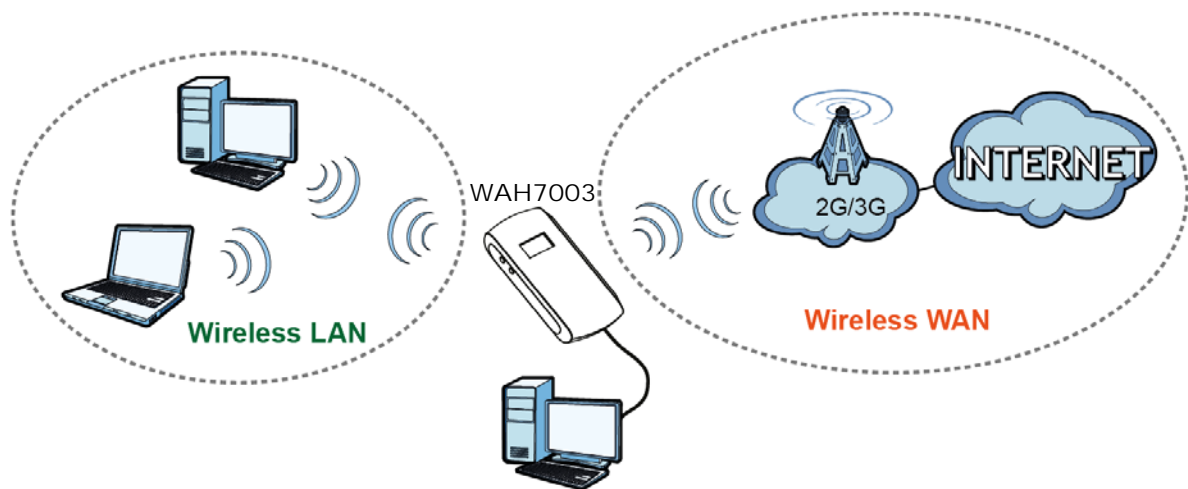
User's Guide

Introduction

1.1 Overview

This chapter introduces the main features and applications of the WAH7003.

The WAH7003 is a wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to mobile users without additional wiring. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.



A range of services such as a firewall are also available for secure Internet computing.

Optionally, you can insert a micro SD card up to 32GB in size to use the WAH7003 as a portal storage device at the same time.

Your WAH7003 is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance. See the Quick Start Guide for how to make hardware connections.

1.2 Ways to Manage the WAH7003

You can use the following way to manage the WAH7003.

Web Configurator

The Web Configurator allows easy WAH7003 setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

1.3 Good Habits for Managing the WAH7003

Do the following things regularly to make the WAH7003 more secure and to manage it more effectively.

- Change the password often. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WAH7003 to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the WAH7003; you can simply restore your last configuration.

1.4 Hardware Connections

See your Quick Start Guide for information on making hardware connections. You need to insert a SIM card before you can use the WAH7003.

1.5 Turn on/off the WAH7003

To turn on the device, press the power button and hold until the ZyXEL logo displays in the OLED screen.

To turn off the device, press the power button and hold until the word "BYE" displays in the OLED screen.

1.6 OLED Display and Icons

The OLED display is enabled by default when you turn on the WAH7003. You can check the icons display in the OLED screen to see the connection status, battery life and signal strength.

Note: To enable or disable the OLED display, press the power button and release after the WAH7003 is turned on.

Figure 1 WAH7003 OLED Display



The following table describes the OLED icons.

Table 1 WAH7003 OLED Icons

ICONS	DESCRIPTION
	The more bars that display, the stronger the signal strength.
	The type of the mobile network to which the WAH7003 is connecting.
	The Wi-Fi signal strength and the number of wireless clients which are currently connecting to the WAH7003.
	The Internet connection is up.
	The current battery level and charging state.
	The mode you configured in the WAN > Connection > Connection Operation screen. It shows how the WAH7003 connects to an available mobile network.
	There is no SIM card inserted.

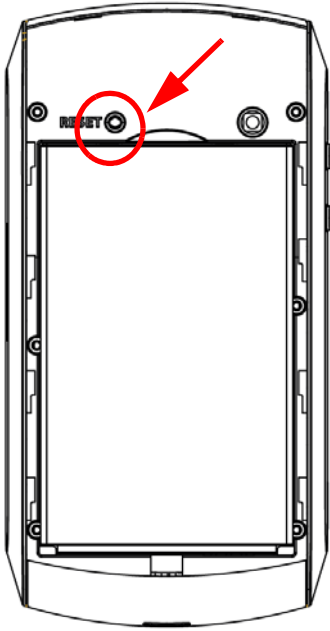
1.7 Resetting the WAH7003

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the physical **Reset** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to **admin** and the IP address will be reset to **192.168.0.254**.

1.7.1 How to Use the Physical Reset Button

- 1 Make sure the WAH7003 is turned on.

- 2 Remove the bottom cover and press the **Reset** button for longer than three seconds to set the WAH7003 back to its factory-default configurations.



The Web Configurator

2.1 Overview

The WAH7003 Web Configurator allows easy management using an Internet browser.

In order to use the Web Configurator, you must:

- Use Internet Explorer 7.0 and later versions, Mozilla Firefox 9.0 and later versions, Safari 4.0 and later versions, or Google Chrome 10.0 and later versions.
- Allow pop-up windows.
- Enable JavaScript (enabled by default).
- Enable Java permissions (enabled by default).
- Enable cookies.

The recommended screen resolution is 1024 x 768 pixels and higher.

2.2 Login Accounts

There are two system accounts that you can use to log in to the WAH7003: “**admin**” and “**guest**”. These two accounts have different privilege levels. The web configurator screens vary depending on which account you use to log in.

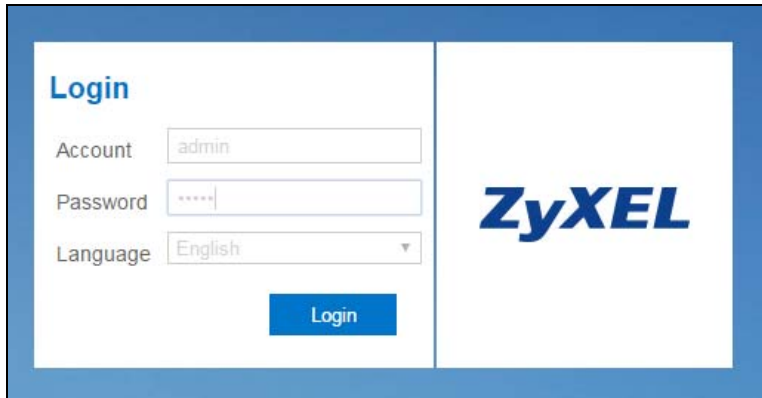
The **admin** accounts allows you full access to all system configurations. The default admin user name is “admin” and password is “admin”.

With the **guest** account, you cannot access the **WAN**, **Security** and **System** screens except for the **System > About** screen. The default username is “guest” and password is “guest”.

2.3 Access

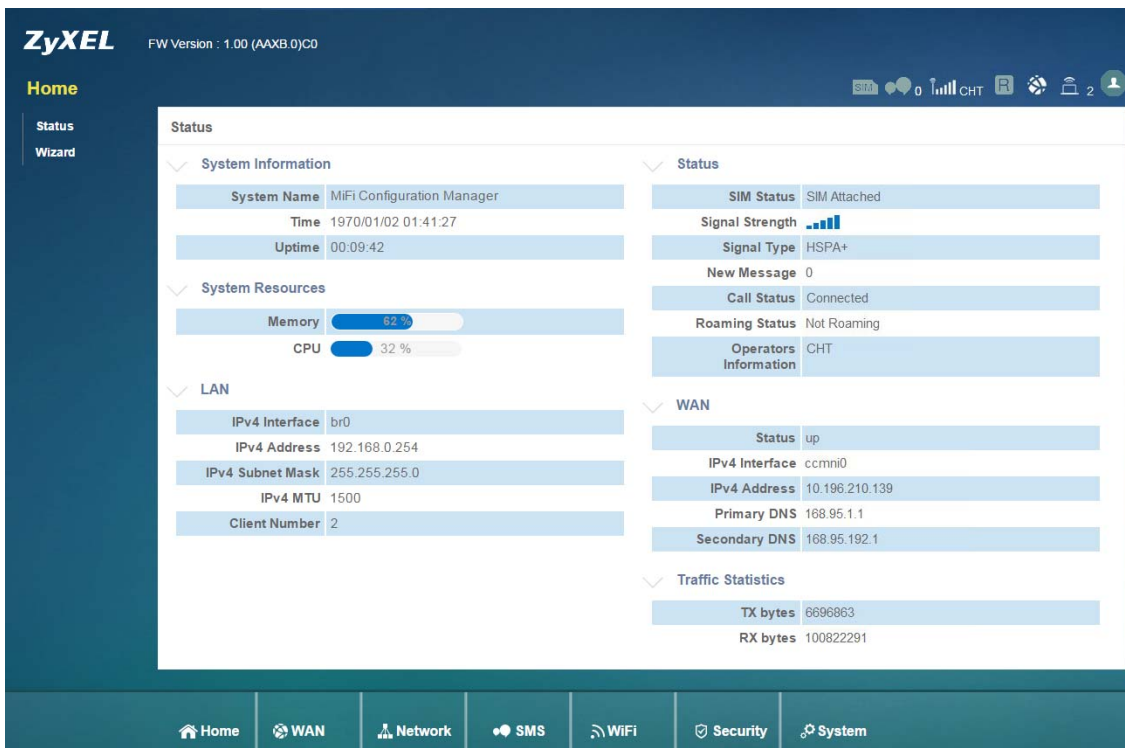
- 1 Make sure your WAH7003 hardware is properly connected. See the Quick Start Guide.
- 2 Launch your web browser.

- 3 Type "http://192.168.0.254" as the website address. The **Login** screen appears. Your computer must be in the same subnet in order to access this website address.



The image shows the ZyXEL login interface. On the left, there is a 'Login' section with three input fields: 'Account' containing 'admin', 'Password' with masked characters, and 'Language' set to 'English'. A blue 'Login' button is positioned below these fields. On the right, the ZyXEL logo is displayed in a large, blue, stylized font.

- 4 Enter the user name (default: "admin" or "guest") and password (default: "admin" or "guest"). See [Section 2.2 on page 13](#) for more information about login accounts.
- 5 Click **Login**, and the **Status** screen appears.



The image shows the ZyXEL web configurator's Status screen. The top left corner displays the ZyXEL logo and 'FW Version : 1.00 (AAXB.0)C0'. The top right corner shows various status icons including signal strength, battery, and network connectivity. The main content area is divided into several sections:

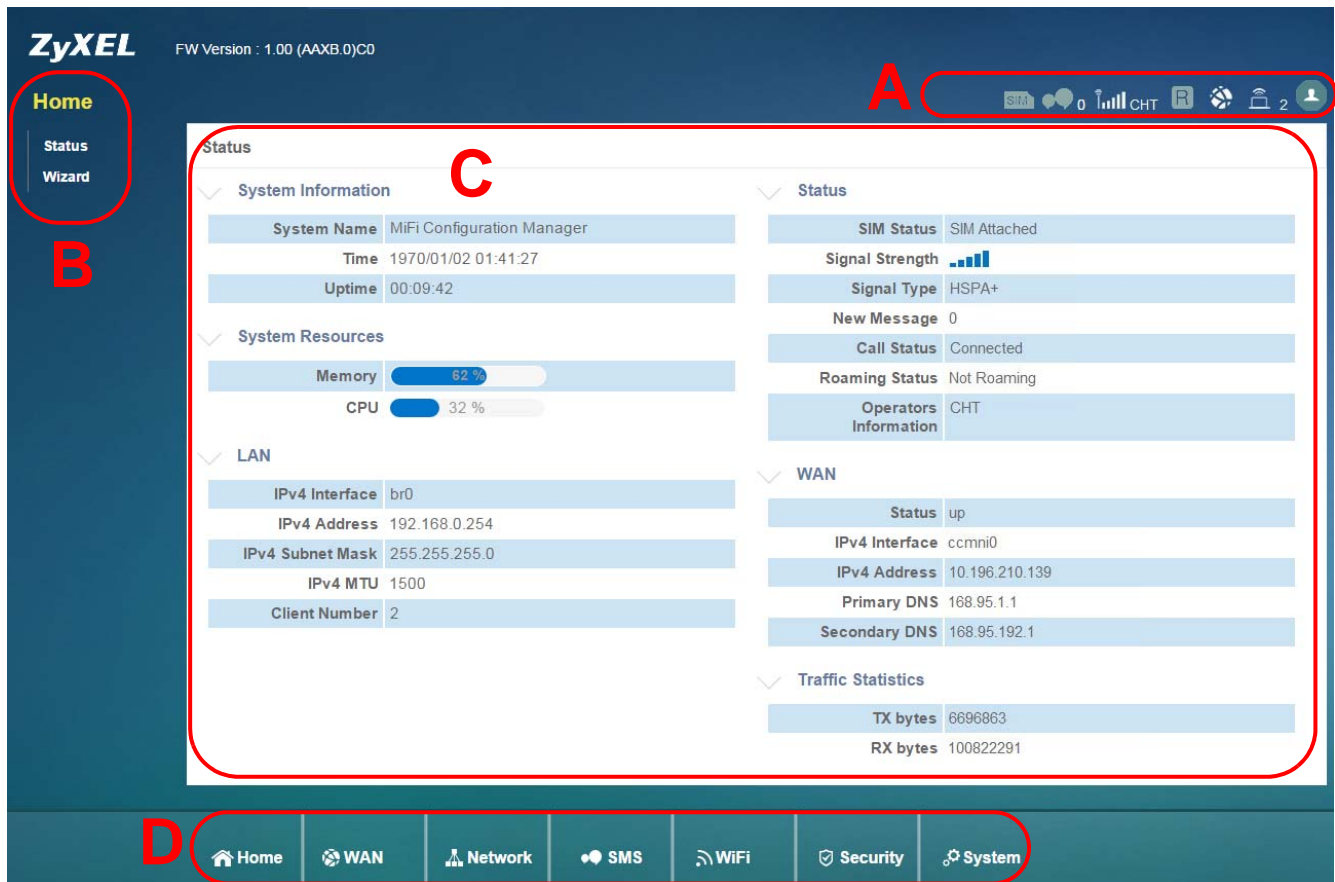
- System Information:** System Name: MiFi Configuration Manager, Time: 1970/01/02 01:41:27, Uptime: 00:09:42.
- System Resources:** Memory usage at 82% and CPU usage at 32%.
- LAN:** IPv4 Interface: br0, IPv4 Address: 192.168.0.254, IPv4 Subnet Mask: 255.255.255.0, IPv4 MTU: 1500, Client Number: 2.
- Status:** SIM Status: SIM Attached, Signal Strength: (visual bar), Signal Type: HSPA+, New Message: 0, Call Status: Connected, Roaming Status: Not Roaming, Operators Information: CHT.
- WAN:** Status: up, IPv4 Interface: ccmni0, IPv4 Address: 10.196.210.139, Primary DNS: 168.95.1.1, Secondary DNS: 168.95.192.1.
- Traffic Statistics:** TX bytes: 6696863, RX bytes: 100822291.

The bottom navigation bar includes icons for Home, WAN, Network, SMS, WiFi, Security, and System.

2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

Figure 2 The Web Configurator's Main Screen



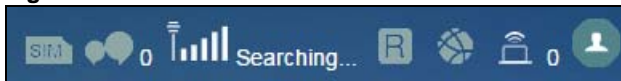
The Web Configurator's main screen is divided into these parts:

- A - Title Bar
- B - Navigation Panel_Sub-Menus
- C - Main Window
- D - Navigation Panel_Main Menu

2.4.1 Title Bar









The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

Figure 3 Title Bar



The icons provide the following functions.

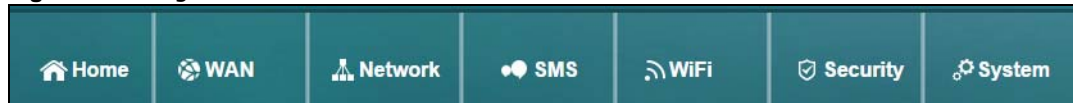
Table 2 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
SIM 	This shows whether a SIM card is inserted in the WAH7003. The icon is grayed out if there is no SIM card inserted.
SMS 	This shows the number of unread text messages in the SMS inbox. The icon is grayed out if there is no messages.
Signal Strength 	This shows the current signal strength to the mobile network. The icon is grayed out if the mobile data connection is not up.
Service Provider 	This shows the name of the service provider for the mobile network to which the WAH7003 is connected. This shows Searching... if the WAH7003 is not connected to a mobile network yet.
Roaming 	This shows whether the WAH7003 is connected to another service provider's mobile network using roaming. The icon is grayed out if roaming is disabled on the WAH7003.
Internet 	This shows whether the WAH7003 has an Internet connection. The icon is grayed out if the WAH7003 is not connected to the Internet.
Wi-Fi 	This shows whether the WAH7003's Wi-Fi network is active and the number of the connected wireless clients.
Logout 	Click this to log out of the Web Configurator.

2.4.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure WAH7003 features. The following sections introduce the WAH7003's navigation panel menus and their screens.

Figure 4 Navigation Panel



Home Menu

The dashboard displays general device information, system status, system resource usage, and interface status.

The Home menu screens display status and statistics information.

Table 3 Home Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
Home		
Status		Display general LAN interface information and packet statistics.
Wizard		Display information about the connected stations.

WAN Menu

Table 4 WAN Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
WAN		
Connection	Connection Operation	Configure the WAN settings on the WAH7003 for Internet access.
	User Profile	Configure user-defined connection profiles.
2/3G Modem	Settings	Set the mobile network type.
	Information	Display information about the WAH7003's mobile module.
SIM	SIM Lock/Unlock Configuration	Configure the PIN code when PIN code authentication is enabled.
PLMN	2G/3G Modem	Display available Public Land Mobile Networks and select a preferred network for roaming.

Network Menu

Table 5 Network Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
Network		
LAN	IPv4	Configure the management IP address for the WAH7003 LAN interface.
	DNS Name	Configure the WAH7003's host name.
DHCP	DHCP Server	Enable the DHCP server on the WAH7003.
	Static DHCP	Configure static DHCP entries.
	Leased Hosts	Display current DHCP client information.

SMS Menu

Table 6 SMS Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
SMS		
New Message	Send SMS	Send new SMS messages.
Local	Inbox	Display messages received on the WAH7003.
	Outbox	Display messages sent from the WAH7003.

WiFi Menu

Table 7 WiFi Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
WiFi		
Basic	Basic	Enable the wireless LAN and configure the basic wireless settings.
WPS	WPS	Enable or disable WPS.
MAC Filter	MAC Filter	Allow or deny wireless clients based on their MAC addresses from connecting to the WAH7003.
Station List	Station List	Display information about the associated stations.

Security Menu

Table 8 Security Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
Security		
Firewall	IP Filter	Configure IP filtering rules.
	MAC Filter	Configure MAC address filtering rules.
	Content Filter	Configure content filtering rules.

System Menu

Table 9 System Menu Screens Summary

MAIN MENU	SUB-MENU	FUNCTION
System		
About	About	Display the WAH7003's basic information.
Configuration	Configuration	Backup and restore device configurations, or reset your device settings back to the factory default.
Firmware Upgrade	Firmware Upgrade	Upload new firmware to the WAH7003.
Power Saving	Power Saving	Enable and configure the power saving settings in the WAH7003.
Password	Password	Configure the WAH7003's system password.
Date and Time	Date	Change the WAH3004's time and date.
	Time Zone	Select your time zone and configure daylight saving time.
Language	Language	Configure the web configurator language.
System Log	Log Setting	Configure to where the WAH7003 is to send logs.
	Log Display	View the logged messages.
Reboot	Reboot	Restart the WAH7003.

PART II

Technical Reference

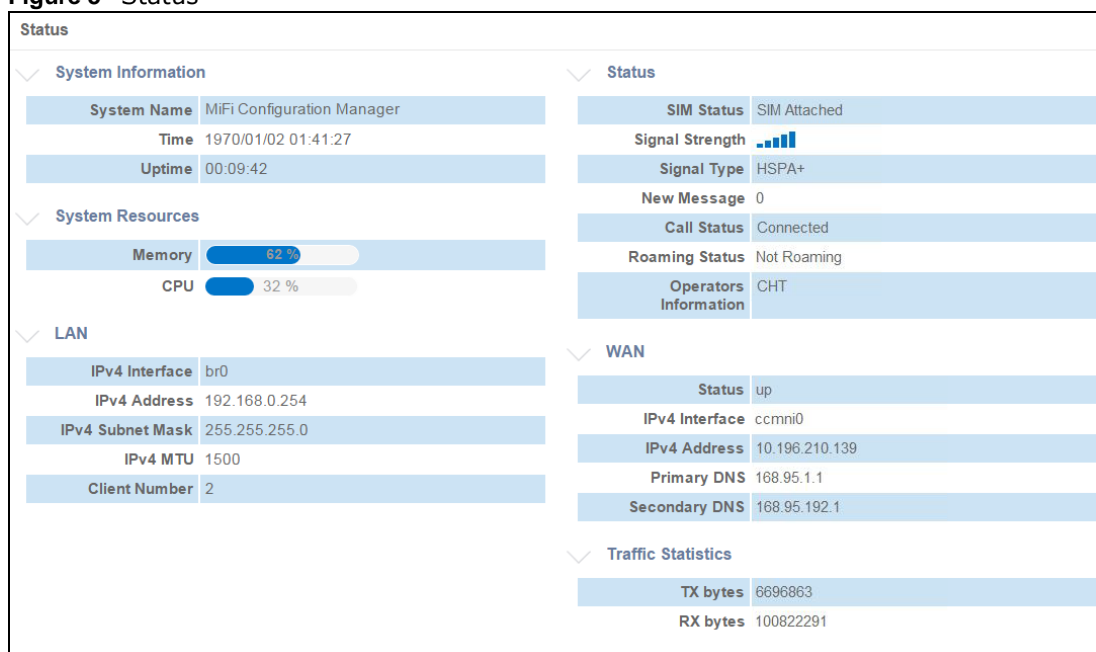
3.1 Overview

Use the **Status** screen to check status information about the WAH7003. Use the **Wizard** screens to configure the WAH7003's management IP address, basic Internet access, and wireless settings.

3.2 Status

This screen is the first thing you see when you log into the WAH7003. It also appears every time you click the **Home** icon in the navigation panel. The **Status** screen displays the WAH7003's general device information, system status, system resource usage, and interface status.

Figure 5 Status



The following table describes the labels in this screen.

Table 10 Status

LABEL	DESCRIPTION
System Information	
System Name	This field displays the name used to identify the WAH7003 on any network.
Time	This field displays the current date and time in the WAH7003. The format is yyyy-mm-dd hh:mm:ss.

Table 10 Status (continued)

LABEL	DESCRIPTION
Uptime	This field displays how long the WAH7003 has been running since it last restarted or was turned on.
System Resources	
Memory	This field displays what percentage of the WAH7003's RAM is currently being used.
CPU	This field displays what percentage of the WAH7003's processing capability is currently being used.
LAN	
IPv4 Interface	This field displays the name of the LAN/WLAN interface.
IPv4 Address	This field displays the current IP address assigned to the LAN/WLAN interface.
IPv4 Subnet Mask	This field displays the subnet mask assigned to the LAN/WLAN interface.
IPv4 MTU	This field displays the MTU (Maximum Transmission Unit) of each data packet, in bytes, that can move through the LAN/WLAN interface.
Client Number	This field displays the number of (wireless) clients that are currently connected to the LAN/WLAN interface.
Status	
SIM Status	This shows whether a SIM card is inserted in the WAH7003.
Signal Strength	This shows the current signal strength to the mobile network.
Signal Type	This shows the type of the mobile network (such as LTE, UMTS, GSM, HSPA+, etc.) to which the WAH7003 is connecting.
New Message	This shows the number of unread text messages in the SMS in-box.
Call Status	This shows the mobile data connection status.
Roaming Status	This shows whether the WAH7003 is connected to another service provider's mobile network using roaming.
Operators Information	This shows the name of the service provider for the mobile network to which the WAH7003 is connected. Searching... displays when the WAH7003 is looking for an available network.
WAN	
Status	This field displays whether the mobile data connection is up or down.
IPv4 Interface	This field displays the name of the WAN interface.
IPv4 Address	This field displays the current IP address assigned to the WAN interface.
Primary DNS	This field displays the first DNS server IP address assigned by the service provider.
Secondary DNS	This field displays the second DNS server IP address assigned by the service provider.
Traffic Statistics	
Tx bytes	This field displays the total amount of data in bytes that has been transmitted on the WAN interface since the WAH7003 last restarted.
Rx Bytes	This field displays the total amount of data in bytes that has been received on the WAN interface since the WAH7003 last restarted.

3.3 Wizard

Click **Home** > **Wizard** to open the wizard screen.

3.3.1 LAN Settings

Enter the WAH7003's LAN IP address and subnet mask. Click **Next** to configure the WAN settings.

Note: If you change the LAN IP address, use the new IP address to access the web configurator and manage the WAH7003.

Figure 6 Wizard > LAN Settings

Wizard

123

1. LAN Settings

2. WAN Settings

3. WiFi Settings

LAN Configuration

IP Address: 192.168.0.254

IP Subnet Mask: 255.255.255.0

Next

3.3.2 WAN Settings

Select a pre-defined profile and click **Set** to use the profile settings to connect to a mobile network. Click **Next** to configure the Wi-Fi settings.

Note: You should have a pre-configured connection profile in the **WAN > Connection > User Profile** screen. Check with your service provider for the APN, user name and password.

Figure 7 Wizard > WAN Settings

Wizard

123

2/3G Configuration
Please consult with service provider for these settings. If not sure, leave them with default value.

1. LAN Settings

2. WAN Settings

3. WiFi Settings

Type	Profile	
2/3G Data Connection	N/A	Set

Profile	Type	Name	APN	User	Password
Profile 1	U.S.	Profile 1	internet	user	1234

Total Num : 1

Back Next

3.3.3 Wi-Fi Settings

This screen shows the default Wi-Fi key and SSID for the WAH7003's wireless network. If you set up a new key and SSID, the wireless clients will lose their wireless connection and need to use new wireless settings. Click **Done** to save your changes. The WAH7003 will restart.

Figure 8 Wizard > WiFi Settings

Wizard

123

WiFi Configuration

1. LAN Settings

2. WAN Settings

3. WiFi Settings

Password Setting: 1234567890

SSID: ZYXEL_

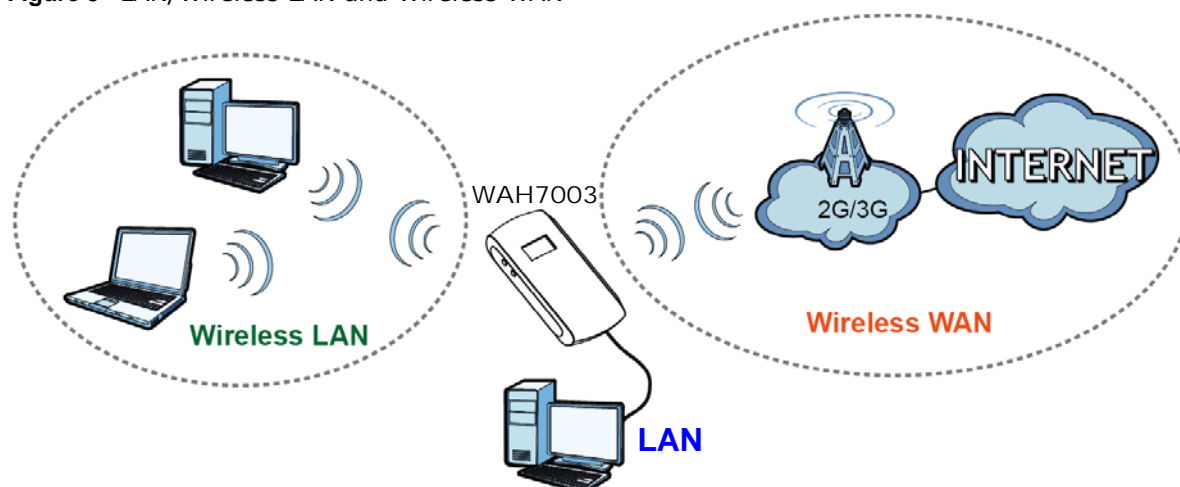
Back Done

4.1 Overview

This chapter discusses the WAH7003's **WAN** screens. Use these screens to configure your WAH7003 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 9 LAN/Wireless LAN and Wireless WAN



4.1.1 What You Can Do in this Chapter

- Use the **Connection Operation** screen to configure the WAN settings on the WAH7003 for Internet access ([Section 4.2 on page 25](#)).
- Use the **User Profile** screen to configure user-defined connection profiles ([Section 4.3 on page 26](#)).
- Use the **2/3G Modem Settings** screen to select the mobile network type ([Section 4.4 on page 27](#)).
- Use the **2/3G Modem Information** screen to display information about the WAH7003's mobile module ([Section 4.5 on page 28](#)).
- Use the **Unlock SIM** screen to enter the PIN code when PIN code authentication is enabled ([Section 4.6 on page 28](#)).
- Use the **SIM Lock/Unlock Configuration** screen to enable or disable PIN code authentication ([Section 4.7 on page 29](#)).
- Use the **Change PIN Code** screen to change the PIN code for the inserted SIM card ([Section 4.8 on page 29](#)).

- Use the **PLMN 2G/3G Modem** screen to display available Public Land Mobile Networks and select a preferred network for roaming ([Section 4.9 on page 30](#)).

4.2 Connection Operation Screen

Use this screen to change your WAH7003's Internet access settings. Click **WAN > Connection > Connection Operation**. The screen appears as shown next.

Figure 10 WAN > Connection > Connection Operation

Profile	Type	Name	APN	Protocol	User	Password
PID-1	User	Profile1	internet	IPv4	user	1234

Total Num : 1

The following table describes the labels in this screen.

Table 11 WAN > Connection > Connection Operation

LABEL	DESCRIPTION
Flight Mode	Select to enable or disable flight (airplane) mode on the WAH7003 and click Change to save your settings. When the WAH7003 is in flight mode, cellular services and signal transmitting functions (such as Wi-Fi) are turned off.
Preferred Cellular Network	Select how you want the WAH7003 to connect to an available mobile network using the applied profile settings and click Change to save your settings. Select Manual Mode to manually establish a connection to the mobile network. Select Auto Mode to have the WAH7003 automatically connect to the mobile network and the connection is always up until the WAH7003 is turned off. Select On Demand to have the WAH7003 connect to the mobile network only when there is traffic.
Roaming mode	Select to enable or disable roaming mode on the WAH7003 and click Change to save your settings. 3G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your WAH7003 is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Type	This field displays the connection type.
State	This field displays the connection status.
Signal	This field displays the current signal strength to the mobile network. The icon is grayed out if the mobile data connection is down.
Profile	This field displays the name of the profile used to connect to the mobile network.

Table 11 WAN > Connection > Connection Operation (continued)

LABEL	DESCRIPTION
	The summary table shows you the configured profiles on the WAH7003.
Profile	This field displays the profile index number.
Type	This field displays whether the profile is user-configured (User) via the WAN > Connection > User Profile screen or a system default profile (System).
Name	This field displays the name of the profile.
APN	This field displays the Access Point Name (APN) in the profile.
Protocol	This field displays Internet Protocol (IP) version used by the profile.
User	This field displays the user name in the profile.
Password	This field displays the password in the profile.
Total Num	This field displays the total number of profiles configured on the WAH7003.

4.3 User Profile Screen

Use this screen to view, add or remove a connection profile. A connection profile defines the parameters that you need to connect to a mobile network, such as the APN, user name and password. Click **WAN > Connection > User Profile**. The screen appears as shown next.

Figure 11 WAN > Connection > User Profile

Profile	Name	APN	Protocol	User	Password
PID-1	Profile1	internet	IPv4	user	1234

Total Num : 1



Apply

The following table describes the labels in this screen.

Table 12 WAN > Connection > User Profile

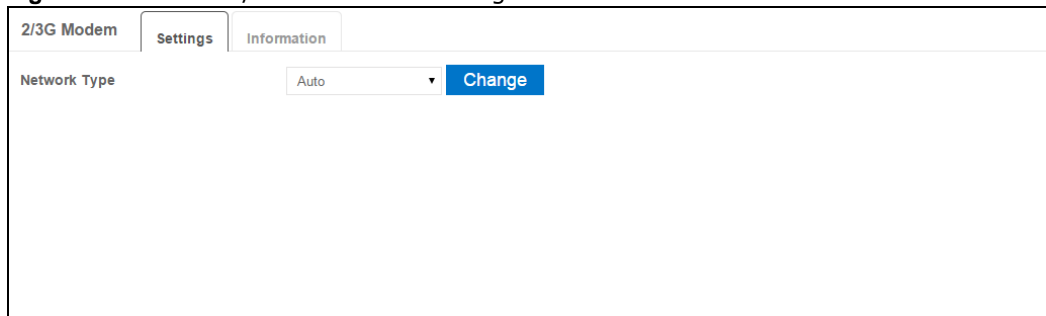
LABEL	DESCRIPTION
Profile	This field displays the profile index number. Click an entry to be able to modify the entry's settings.
Name	This field displays the name of the profile. Enter a descriptive name to identify the profile. You can enter up to 30 printable ASCII characters. Spaces are allowed.
APN	This field displays the Access Point Name (APN) in the profile. Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 30 printable ASCII characters. Spaces are allowed.
Protocol	This field displays Internet Protocol (IP) version used by the profile. Select IPv4 to connect to an IPv4 network, IPv6 to connect to an IPv6 network, or IPv4v6 to connect to either one.

Table 12 WAN > Connection > User Profile (continued)

LABEL	DESCRIPTION
User	This field displays the user name in the profile. Type the user name (of up to 31 printable ASCII characters) given to you by your service provider.
Password	This field displays the password in the profile. Type the password (of up to 31 printable ASCII characters) associated with the user name above.
	Click an entry's delete icon to remove the profile.
	Click the add icon to create a new entry. Click the OK icon to save the profile settings. Click the delete icon to remove all profiles.
Total Num	This field displays the total number of profiles configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

4.4 2/3G Modem Settings Screen

Use this screen to change your WAH7003's 2G/3G settings. Click **WAN > 2/3G Modem > Settings**. The screen appears as shown next.

Figure 12 WAN > 2/3G Modem > Settings


The following table describes the labels in this screen.

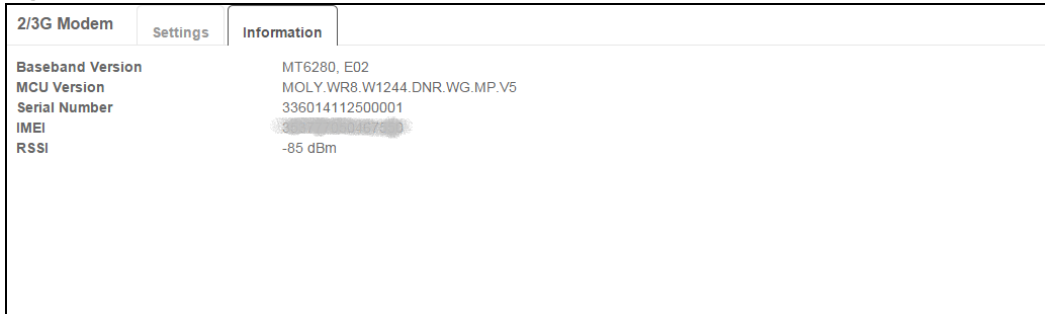
Table 13 WAN > 2/3G Modem > Settings

LABEL	DESCRIPTION
Network Type	Select the type of the network (3G Only , or 2G Only) to which you want the WAH7003 to connect and click Change to save your settings. Otherwise, select Auto to have the WAH7003 connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the WAH7003 switches to another available mobile network.

4.5 2/3G Modem Information Screen

Use this screen to view information about the WAH7003's mobile module. Click **WAN > 2/3G Modem > Information**. The screen appears as shown next.

Figure 13 WAN > 2/3G Modem > Information



The following table describes the labels in this screen.

Table 14 WAN > 2/3G Modem > Information

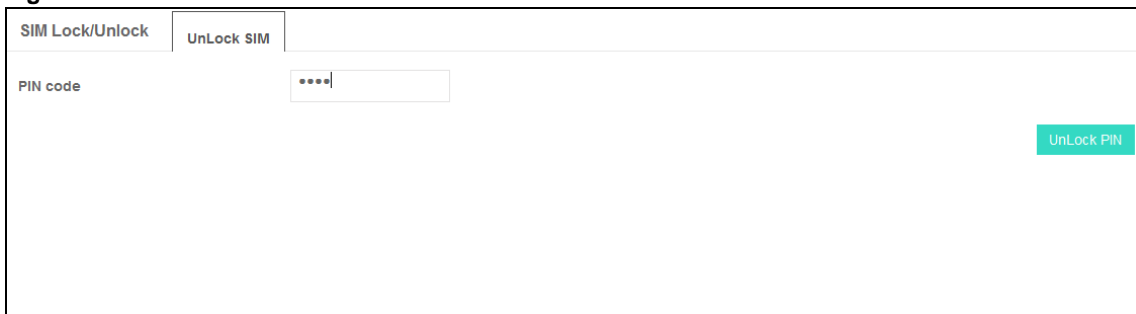
LABEL	DESCRIPTION
Baseband Version	This shows the version of the software for processing the baseband signals.
MCU Version	This shows the version of the Microcontroller Unit (MCU) for the mobile module.
Serial Number	This shows the serial number of the WAH7003's mobile module.
IMEI	This shows the International Mobile Equipment Number (IMEI) which is the serial number of a mobile device (the WAH7003). IMEI is a unique 15-digit number used to identify a mobile device.
RSSI	This shows the received signal strength indicator (RSSI), that is, the received signal strength in dBm.

4.6 Unlock SIM Screen

This screen displays if PIN code authentication is enabled on the inserted SIM card.

Use this screen to enter the correct PIN code. Click **WAN > SIM > Unlock SIM**. The screen appears as shown next.

Figure 14 WAN > SIM > Unlock SIM



The following table describes the labels in this screen.

Table 15 WAN > SIM > Unlock SIM

LABEL	DESCRIPTION
PIN Code	Enter the PIN code provided by your service provider for the inserted SIM card and click Unlock PIN so that you can use the SIM card to connect to an available mobile network.

4.7 SIM Lock/Unlock Configuration Screen

Use this screen to turn on or turn off PIN code authentication on the inserted SIM card. Click **WAN > SIM > SIM Lock/Unlock Configuration**. The screen appears as shown next.

Figure 15 WAN > SIM > SIM Lock/Unlock Configuration

The following table describes the labels in this screen.

Table 16 WAN > SIM > SIM Lock/Unlock Configuration

LABEL	DESCRIPTION
PIN Code	Enter the PIN code provided by your service provider for the inserted SIM card and click Enable to turn on PIN code authentication. Otherwise, click Disable to turn off PIN code authentication. A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.

4.8 Change PIN Code Screen

When there is a SIM card inserted in the WAH7003, you can use this screen to change your SIM card's existing PIN code. Click **WAN > SIM > Change PIN Code**. The screen appears as shown next.

Figure 16 WAN > SIM > Change PIN Code

The following table describes the labels in this screen.

Table 17 WAN > SIM > Change PIN Code

LABEL	DESCRIPTION
PIN Code	Enter the default or existing PIN code for the inserted SIM card.
New PIN Code	Configure a new PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code.
Please Enter New PIN Code Again	Enter the new PIN code again for confirmation.
Apply	Click this button to save your changes back to the WAH7003.

4.9 PLMN 2G/3G Modem Screen

This screen allows you to view available Public Land Mobile Networks (PLMNs) and select your preferred network when the WAH7003 is outside the geographical coverage area of the network to which you are registered and roaming is enabled.

Click **WAN > PLMN > 2G/3G Modem**. The screen appears as shown next.

Figure 17 WAN > PLMN > 2G/3G Modem

Status	PLMN number	Operator Name	Access Technology
Current	46692	CHT	GSM
Available	46601	FET	GSM
Available	46697	TWN	GSM

Total Num : 3

The following table describes the labels in this screen.

Table 18 WAN > PLMN > 2G/3G Modem

LABEL	DESCRIPTION
Mode	<p>Select Automatic to have the WAH7003 automatically connect to the first available mobile network using roaming when it is outside the coverage area of the original service provider's network.</p> <p>Select Manual or Manual failed then Automatic to display the network list and manually select a preferred network.</p>
Status	This field displays whether the mobile network is the preferred network (Current) or not (Available).
PLMN Number	This field displays the PLMN code of the mobile network.
Operator Name	This field displays the mobile network name.
Access Technology	This field displays the mobile telecommunications technology used by the mobile network.
Update	Select a network and click this button to use it as the preferred network when the WAH7003 is in roaming mode.
Query	<p>This button is available only when you select Manual or Manual failed then Automatic in the Mode field.</p> <p>Click this button to update the network list in this screen.</p>

5.1 Overview

This chapter describes how you can configure the management IP address and DHCP settings of your WAH7003.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

5.1.1 What You Can Do in this Chapter

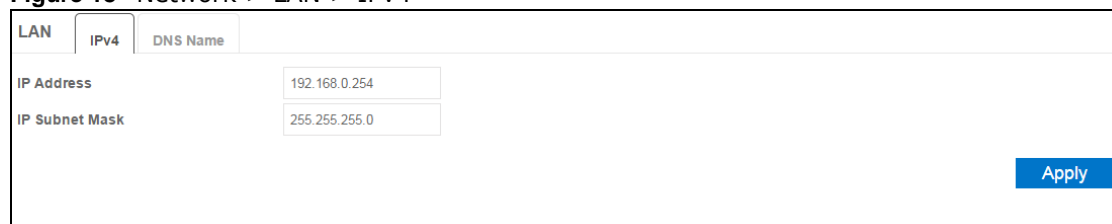
- Use the **LAN IPv4** screen to configure the WAH7003's LAN IP address ([Section 5.2 on page 32](#)).
- Use the **LAN DNS Name** screen to configure the WAH7003's host name ([Section 5.3 on page 33](#)).
- Use the **DHCP Server** screen to enable the DHCP server on the WAH7003 ([Section 5.4 on page 33](#)).
- Use the **Static DHCP** screen to configure static DHCP entries ([Section 5.5 on page 34](#)).
- Use the **Leased Hosts** screen to view current DHCP client information ([Section 5.6 on page 35](#)).

5.2 LAN IPv4 Screen

Use this screen to view or configure the management IP address for your WAH7003. To access this screen, click **Network > LAN > IPv4**.

Note: If you change the WAH7003's IP address, you need to use the new IP address to access the WAH7003's web configurator.

Figure 18 Network > LAN > IPv4



LAN	IPv4	DNS Name
IP Address	192.168.0.254	
IP Subnet Mask	255.255.255.0	

Apply

The following table describes the labels in this screen.

Table 19 Network > LAN > IPv4

LABEL	DESCRIPTION
IP Address	This shows the default LAN IP address. Enter the new IP address for the WAH7003's LAN interface if you want to change it.
Subnet Mask	This shows the default subnet mask. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Apply	Click this button to save your changes back to the WAH7003.

5.3 LAN DNS Name Screen

Use this screen to view or modify the WAH7003's host name. To access this screen, click **Network > LAN > DNS Name**.

Figure 19 Network > LAN > DNS Name

The following table describes the labels in this screen.

Table 20 Network > LAN > DNS Name

LABEL	DESCRIPTION
DNS Device Name	This shows the default name used to identify the WAH7003 on the network. Enter a new host name for the WAH7003 if you want to change it.
Apply	Click this button to save your changes back to the WAH7003.

5.4 DHCP Server Screen

The WAH7003 has built-in DHCP server capability that assigns IP addresses to systems that support DHCP client capability. Use this screen to enable the DHCP server. To access this screen, click **Network > DHCP > DHCP Server**.

Figure 20 Network > DHCP > DHCP Server

The following table describes the labels in this screen.

Table 21 Network > DHCP > DHCP Server

LABEL	DESCRIPTION
DHCP Mode	Select what type of DHCP service the WAH7003 provides to the network. Choices are: None - the WAH7003 does not provide any DHCP services. There is already a DHCP server on the network. Server - the WAH7003 assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The WAH7003 is the DHCP server for the network.
Start IP	The WAH7003 is pre-configured with a pool of 100 IP addresses starting from 192.168.0.100 to 192.168.0.199. This field specifies the first of the contiguous addresses in the IP address pool.
End IP	This field specifies the last of the contiguous addresses in the IP address pool.
Lease Time	Specify how long (in seconds) each computer can use the information (especially the IP address) before it has to request the information again.
Apply	Click this button to save your changes back to the WAH7003.

5.5 Static DHCP Screen

You can assign IP addresses on the LAN to specific individual computers based on their MAC addresses. Use this screen to view, add or remove a static DHCP entry. To access this screen, click **Network > DHCP > Static DHCP**.





Figure 21 Network > DHCP > Static DHCP

#	Status	MAC Address	IP Address
1	Disabled	00:00:00:00:00:00	192.168.0.0

Total Num : 1

The following table describes the labels in this screen.


Table 22 Network > DHCP > Static DHCP

LABEL	DESCRIPTION
per page	Select how many entries you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of entries.
#	This field displays the index number of the static DHCP entry. Click an entry to be able to modify the entry's settings.
Status	This field displays whether the entry is active or not. Click to select Enabled or Disabled .
MAC Address	This field displays the MAC address of the device to which the WAH7003 assigns the entry's IP address. Click to enter or change the MAC address.
IP Address	This field displays the IP address that the WAH7003 assigns to a device with the entry's MAC address. Click to enter or change the IP address.
	Click an entry's delete icon to remove the profile.
  	Click the add icon to create a new entry. Click the OK icon to save the entry settings. Click the delete icon to remove all entries.
Total Num	This field displays the total number of entries configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

5.6 Leased Hosts Screen

This screen displays current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the WAH7003 DHCP servers. To access this screen, click **Network > DHCP > Leased Hosts**.

Figure 22 Network > DHCP > Leased Hosts



#	Host Name	MAC Address	IP Address	Remaining Time
1	TWPC	00:10:58:00:02:AC	192.168.0.100	15:56:35

Total Num : 1

Refresh

The following table describes the labels in this screen.

Table 23 Network > DHCP > Leased Hosts

LABEL	DESCRIPTION
per page	Select how many entries you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of entries.

Table 23 Network > DHCP > Leased Hosts (continued)

LABEL	DESCRIPTION
#	This field displays the index number of the host computer.
Host Name	This field displays the computer host name.
MAC Address	This field displays the MAC address of the host computer.
IP Address	This field displays the IP address that the WAH7003 assigns to the host computer.
Remaining Time	This field displays how long the host computer can use the assigned IP address before it has to request the information again.
Total Num	This field displays the total number of entries in the DHCP table.
Refresh	Click this button to update the information in this screen.

6.1 Overview

SMS (Short Message Service) allows you to send and view the text messages that the WAH7003 received from mobile devices or the service provider.

When the SMS box is full the WAH7003 will begin to delete older entries as it adds new ones.

6.1.1 What You Can Do in this Chapter

- Use the **New Message > Send SMS** screen to send new messages ([Section 6.2 on page 37](#)).
- Use the **Local > Inbox** screen to view messages received on the WAH7003 ([Section 6.3 on page 37](#)).
- Use the **Local > Outbox** screen to view messages sent from the WAH7003 ([Section 6.4 on page 38](#)).

6.2 New Message > Send SMS Screen

Use this screen to send messages using the WAH7003. To access this screen, click **SMS > New Message > Send SMS**.

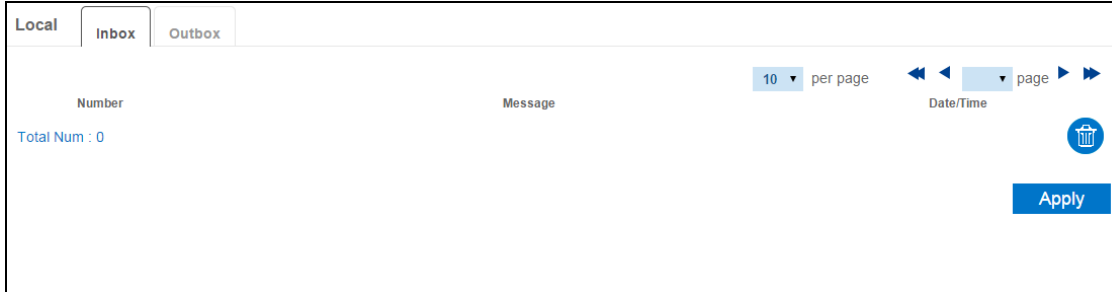
Type a phone number and message content. You can type up to 70 characters in one message. If the message exceeds 70 characters, more than one SMS will be sent. The maximum number of SMS that can be sent is 20 (1400 characters total). Click **Send** to send the message.

Figure 23 SMS > New Message > Send SMS

The screenshot shows a mobile application interface for sending an SMS. At the top, there is a header bar with 'New Message' on the left and 'Send SMS' on the right. Below the header, there is a 'Send To' label followed by a text input field. Underneath that is a 'Messages' label followed by a larger text area for composing the message. In the bottom right corner of the screen, there is a blue button labeled 'Send'.


6.3 Local Inbox Screen

Use this screen to view messages received on the WAH7003. To access this screen, click **SMS > Local > Inbox**.

Figure 24 SMS > Local > Inbox

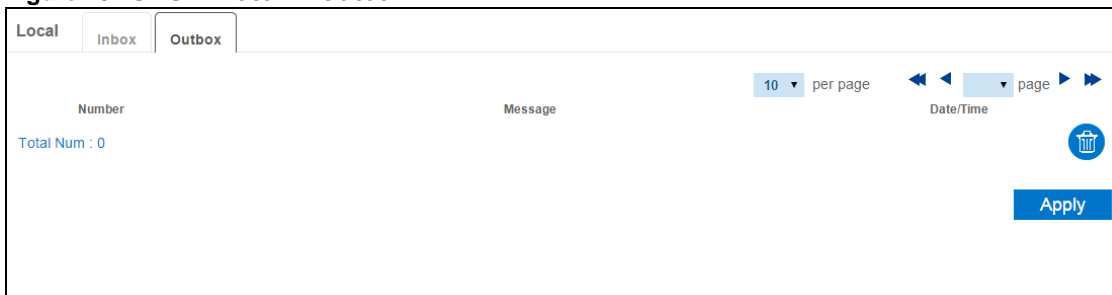
The following table describes the labels in this screen.

Table 24 SMS > Local > Inbox

LABEL	DESCRIPTION
per page	Select how many messages you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of messages.
#	This field displays the index number of the message.
Number	This field displays the mobile phone number from which the message is sent.
Message	This field displays the content of the message.
Date/Time	This field displays the date and time the message was received.
	Click the delete icon to remove the message record.
Total Num	This field displays the total number of messages.
Apply	Click this button to save your changes to the WAH7003.

6.4 Local Outbox Screen

Use this screen to view messages sent from the WAH7003. To access this screen, click **SMS > Local > Outbox**.


Figure 25 SMS > Local > Outbox

The following table describes the labels in this screen.

Table 25 SMS > Local > Outbox

LABEL	DESCRIPTION
per page	Select how many messages you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of messages.
#	This field displays the index number of the message.

Table 25 SMS > Local > Outbox (continued)

LABEL	DESCRIPTION
Number	This field displays the mobile phone number the message is sent to.
Message	This field displays the content of the message.
Date/Time	This field displays the date and time the message was sent.
	Click the delete icon to remove the message record.
Total Num	This field displays the total number of messages.
Apply	Click this button to save your changes to the WAH7003.

7.1 Overview

This chapter describes the WAH7003's **Wi-Fi** screens. Use these screens to set up your WAH7003's wireless LAN connection.

7.1.1 What You Can Do in this Chapter

- Use the **Basic** screen to enable the wireless LAN, enter the SSID and select the wireless security mode ([Section 7.2 on page 41](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.3 on page 44](#)).
- Use the **MAC Filter** screen to allow or deny wireless clients based on their MAC addresses from connecting to the WAH7003 ([Section 7.4 on page 45](#)).
- Use the **Station List** screen to view information about the associated stations (or "wireless clients") ([Section 7.5 on page 46](#)).

7.1.2 What You Need to Know

Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See [Section 7.6 on page 47](#) for advanced technical information on wireless networks.

7.2 Wi-Fi Basic Screen

Use this screen to enable the wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the WAH7003 from a computer connected to the wireless LAN and you change the WAH7003’s SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAH7003’s new settings.

To access this screen, click **Wi-Fi > Basic**.

Figure 26 Wi-Fi > Basic

Basic	
Enable	<input checked="" type="checkbox"/> On
Mode	802.11 B/G/N mixed
Channel	channel 11
802.11N Channel Width	HT20
TxPower	10 dBm
Beacon Interval (20 ~ 1024)	100
DTIM Period (1 ~ 255)	1
SSID	ZYXEL_
Hide SSID	<input type="checkbox"/> off
Encryption Type	WPA Personal
WPA Mode	Auto(WPA or WPA2)
Cipher Type	TKIP and AES
Pre-shared Key	1234567890

[Apply](#)

The following table describes the labels in this screen.

Table 26 Wi-Fi > Basic

LABEL	DESCRIPTION
Enable	Select On to enable the wireless LAN of the WAH7003. Otherwise, select Off .
Mode	<p>Select 802.11 B Only to allow only IEEE 802.11b compliant WLAN devices to associate with the WAH7003.</p> <p>Select 802.11 G Only to allow only IEEE 802.11g compliant WLAN devices to associate with the WAH7003.</p> <p>Select 802.11 N Only to allow only IEEE 802.11n compliant WLAN devices to associate with the WAH7003.</p> <p>Select 802.11 B/G mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the WAH7003. The transmission rate of the WAH7003 might be reduced when an 802.11b wireless client is associated with it.</p> <p>Select 802.11 B/G/N mixed to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the WAH7003. The transmission rate of the WAH7003 might be reduced when an 802.11b or 802.11g wireless client is associated with it.</p> <p>Select 802.11 G/N mixed to allow IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the WAH7003. The transmission rate of the WAH7003 might be reduced when an 802.11g wireless client is associated with it.</p>
Channel	<p>Set the channel depending on your particular region.</p> <p>Select a channel or use Auto to have the WAH7003 automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the WAH7003 is currently using then displays next to this field.</p>
802.11N Channel Width	<p>This field is available only when you set Mode to 802.11 N Only, 802.11 B/G/N mixed or 802.11 G/N mixed.</p> <p>Select whether the WAH7003 uses a wireless channel width of 20MHz or 40MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select HT20 if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Select HT20/40 Mixed to allow the WAH7003 to choose the channel bandwidth (20 or 40 MHz) that has least interference.</p>
TxPower	Set the output power of the WAH7003. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs.
Beacon Interval	<p>When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.</p> <p>The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1024ms. A high value helps save current consumption of the access point.</p>
DTIM Period	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network.

Table 26 Wi-Fi > Basic (continued)

LABEL	DESCRIPTION
SSID	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p>
Hide SSID	<p>Select On to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Otherwise, select Off.</p>
Encryption Type	<p>Select WEP or WPA Personal to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the WAH7003. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select None to allow any client to associate this network without any data encryption or authentication.</p>
The following fields are available if you set Encryption Type to WEP .	
Authentication Method	<p>This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network.</p> <p>Select SHARED KEY to force the clients to provide the WEP key prior to communication.</p> <p>Select OPEN SYSTEM if you do NOT want to force a key verification before communication between the wireless client and the WAH7003 occurs.</p> <p>Select AUTO to have the WAH7003 automatically determine a WEP authentication method to use according to the connected wireless clients.</p>
WEP Encryption Length	<p>Select 64-bit or 128-bit. This dictates the length of the security key that the network is going to use.</p>
Key 1 ~ Key 4	<p>The WEP keys are used to encrypt data. Both the WAH7003 and the wireless clients must use the same WEP key for data transmission.</p> <p>If you chose 64-bit, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure at least one password, only one password can be activated at any one time. The default password is Key 1.</p> <p>Select ASCII in order to enter ASCII characters as WEP key. Select HEX in order to enter hexadecimal characters as a WEP key.</p>
The following fields are available if you set Encryption Type to WPA Personal .	
WPA Mode	<p>Select Auto(WPA or WPA2) to allow wireless devices that support either WPA or WPA2 to connect to your WAH7003's wireless network.</p> <p>Select WPA to allow only wireless devices that support WPA to connect to your WAH7003's wireless network.</p> <p>Select WPA2 to allow only wireless devices that support WPA2 to connect to your WAH7003's wireless network.</p>
Cipher Type	<p>Select the encryption type (TKIP, AES or TKIP and AES) for data encryption.</p> <p>Select AES if your wireless clients can all use AES.</p> <p>Select TKIP if your wireless clients can all use TKIP.</p> <p>Select TKIP and AES to allow the wireless clients to use either TKIP or AES.</p>
Pre-shared Key	<p>Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.</p>
Apply	<p>Click Apply to save your changes.</p>

7.3 WPS Screen

Use this screen to configure Wi-Fi Protected Setup (WPS) on your WAH7003.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 7.6.5.3 on page 54](#) for more information about WPS.

Note: To use the WPS feature, make sure you have wireless enabled in the **Wi-Fi > Basic** screen.

Note: If you want to use the WPS feature set the security type to **WPA** or **None**.

Click **Wi-Fi > WPS**. The following screen displays. Select **On** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 27 Wi-Fi > WPS

The following table describes the labels in this screen.

Table 27 Wi-Fi > WPS

LABEL	DESCRIPTION
Enable	Select On to activate WPS on the WAH7003. Otherwise, select Off .
Configure State	The default WPS status is configured. Select Unconfigure to remove all configured wireless and wireless security settings for WPS connections on the WAH7003.
Configure Method	<ul style="list-style-type: none"> Select PCB to set up a WPS wireless network using Push Button Configuration (PBC). If you select PCB, click Apply to add another WPS-enabled wireless device (within wireless range of the WAH7003) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the Connect button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button. Select PIN to set up a WPS wireless network by either entering the PIN of the client into the WAH7003 or entering the PIN of the WAH7003 into the client.

Table 27 Wi-Fi > WPS (continued)

LABEL	DESCRIPTION
Current PIN	<p>This field is available only when you select Unconfigure in the Configure State field and set Configure Method to PIN.</p> <p>The PIN (Personal Identification Number) of the WAH7003 is shown here. Select this option, click Apply and then enter this PIN in the configuration utility of the device you want to connect to using WPS.</p> <p>The PIN is not necessary when you use WPS push-button method.</p> <p>Click the Generate Pin button to have the WAH7003 create a new PIN.</p>
Enrollee PIN	<p>This field is available only when you set Configure Method to PIN.</p> <p>Select this option and enter the PIN of the device that you are setting up a WPS connection with and click Apply to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the WAH7003.</p>
Current State	This shows the current status of the WPS connection.
Apply	Click Apply to save your changes or start WPS on the WAH7003.

7.4 MAC Filter Screen





This screen allows you to configure the WAH7003 to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the WAH7003 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your WAH7003's MAC filter settings and add new MAC filter rules. Click **Wi-Fi > MAC Filter**. The screen appears as shown.

Figure 28 Wi-Fi > MAC Filter

The following table describes the labels in this screen.

Table 28 Wi-Fi > MAC Filter

LABEL	DESCRIPTION
Enable MAC Address Filter	Select Off to disable MAC filtering. Select On to enable MAC filtering.
Mode	Define the filter action for the list of MAC addresses. Select Deny listed stations to block access to the WAH7003. MAC addresses not listed will be allowed to access the WAH7003. Select Allow listed stations to permit access to the WAH7003. MAC addresses not listed will be denied access to the WAH7003.
per page	Select how many entries you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of entries.
#	This field displays the index number of the MAC address entry. Click an entry to be able to modify the entry's settings.
Active	This field displays whether the entry is active or not. Click to enable or disable the entry.
Name	This field displays the name of the MAC address entry. Click to enter a descriptive name to identify the MAC address entry. You can enter up to 20 printable ASCII characters. Spaces are allowed.
MAC Address	This field displays the MAC addresses of the wireless devices that are allowed or denied access to the WAH7003. Click to enter or change the MAC address of the wireless devices that are allowed or denied access to the WAH7003 in this field. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
	Click an entry's delete icon to remove the MAC address entry.
  	Click the add icon to create a new entry. Click the OK icon to save the entry settings. Click the delete icon to remove all entries.
Total Num	This field displays the total number of entries configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

7.5 Station List Screen

Use this screen to view information about the associated stations (or "wireless clients"). Click **Wi-Fi > Station List** to access this screen.

Figure 29 Wi-Fi > Station List



The following table describes the labels in this screen.

Table 29 Wi-Fi > Station List

LABEL	DESCRIPTION
per page	Select how many stations you want to display on each page.
page	Select a page number to go to or use the arrows to navigate the pages of stations.
#	This is the station's index number in this list.
MAC Address	This is the station's MAC address.
Total Num	This field displays the total number of the associated stations.

7.6 Technical Reference

This section discusses wireless LANs in depth.

7.6.1 Wireless Network Overview

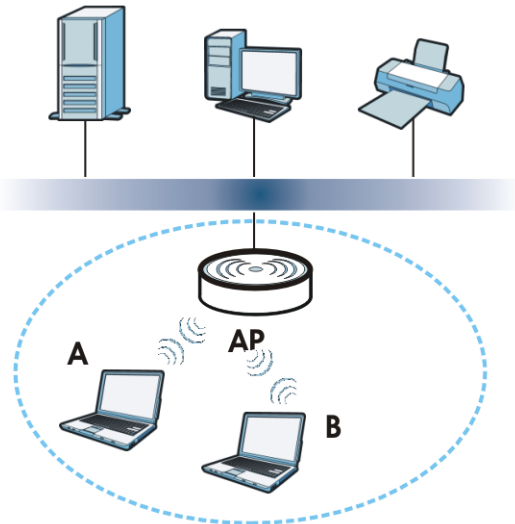
Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 30 Example of a Wireless Network

The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your WAH7003 is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.6.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the WAH7003's Web Configurator.

Table 30 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the WAH7003. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the WAH7003.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the WAH7003 does, it cannot communicate with the WAH7003.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.6.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random

and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

7.6.3.1 SSID

Normally, the WAH7003 acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the WAH7003 does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.6.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the WAH7003 which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.6.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.


-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

7.6.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 7.6.3.3 on page 50](#) for information about this.)

Table 31 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest 	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the WAH7003 and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your WAH7003, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the WAH7003.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.6.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.6.5 WiFi Protected Setup (WPS)

Your WAH7003 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.6.5.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the WAH7003, see [Section 7.3 on page 44](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the WAH7003 you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.6.5.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated

on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

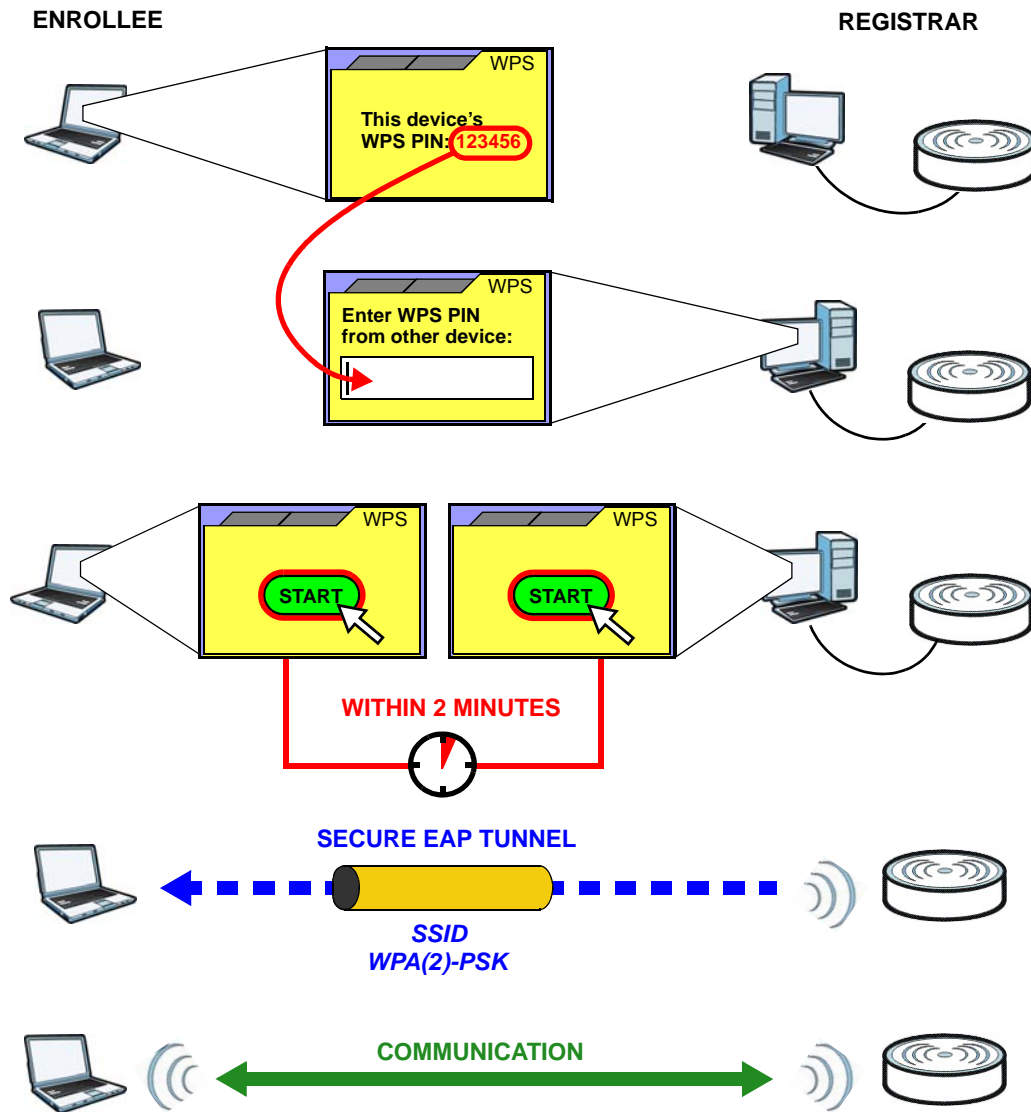
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the WAH7003, see [Section 7.3 on page 44](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 31 Example WPS Process: PIN Method

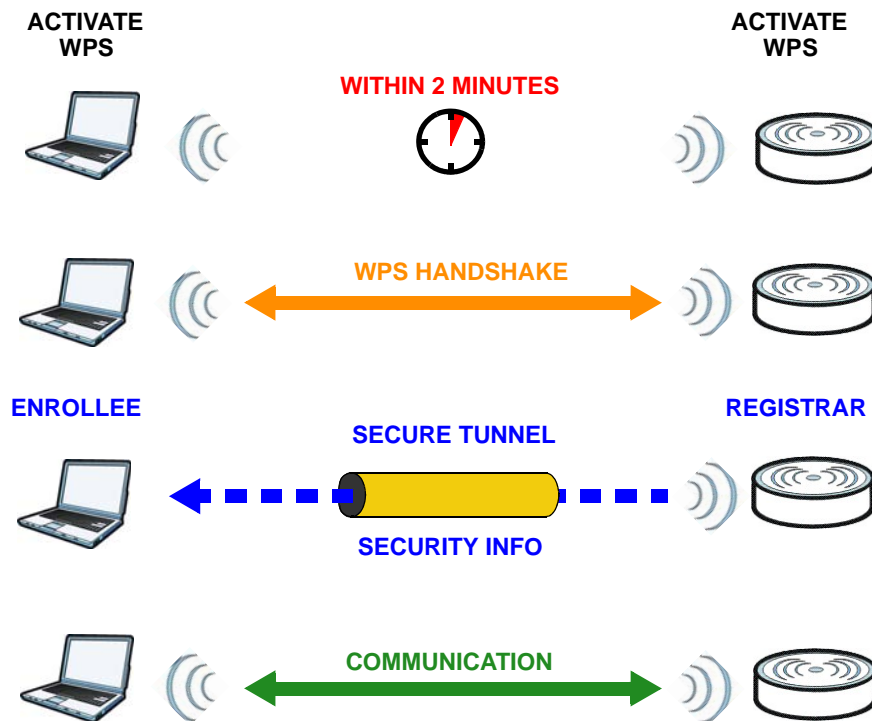


7.6.5.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 32 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

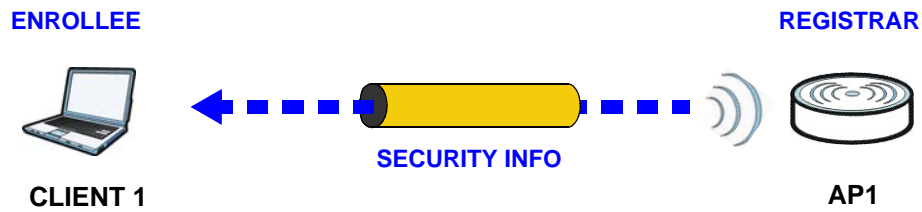
By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.6.5.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

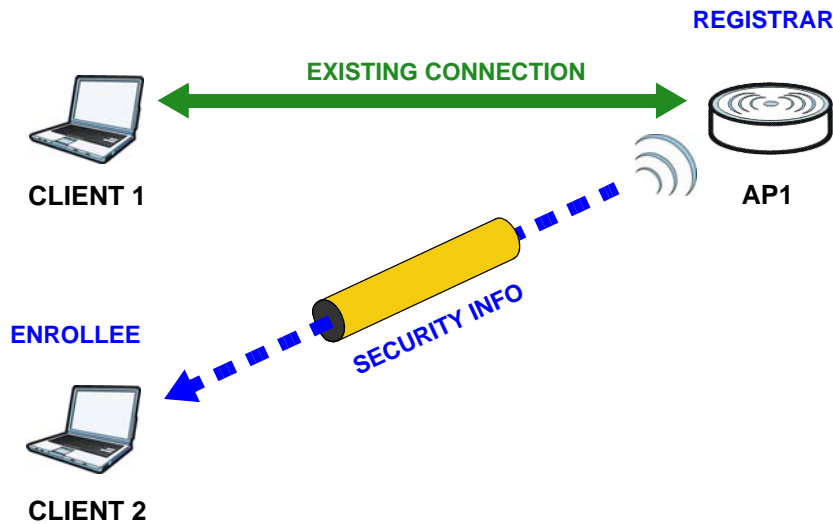
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 33 WPS: Example Network Step 1



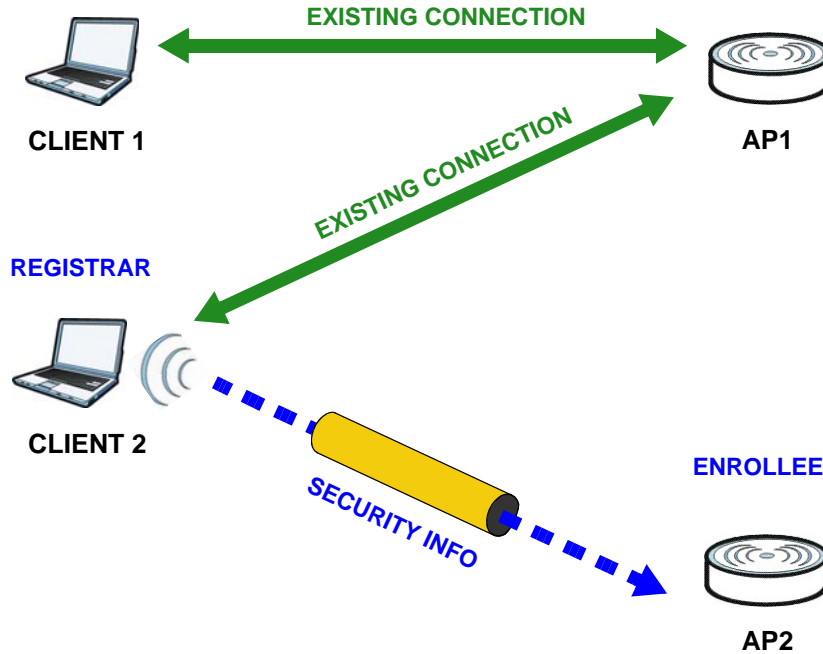
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 34 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 35 WPS: Example Network Step 3



7.6.5.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the

access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

8.1 Overview

This chapter shows you how to configure the IP filtering, MAC filtering and content filtering settings.

8.1.1 What You Can Do in this Chapter

- Use the **IP Filter** screen to view and configure IP filtering rules ([Section 8.2 on page 59](#)).
- Use the **MAC Filter** screen to view and configure MAC address filtering rules ([Section 8.3 on page 60](#)).
- Use the **Content Filter** screen to view and configure content filtering rules ([Section 8.4 on page 61](#)).

8.2 IP Filter Screen

The WAH7003 firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application. Use this screen to configure IP filtering rules. To access this screen, click **Security > Firewall > IP Filter**.

Figure 36 Security > Firewall > IP Filter

#	Active	Source IP	Source from Port	Source to Port	Destination IP	Destination from Port	Destination to Port	Protocol
1	<input checked="" type="checkbox"/>		0	0		0	0	TCP





Total Num : 1

The following table describes the labels in this screen.

Table 32 Security > Firewall > IP Filter

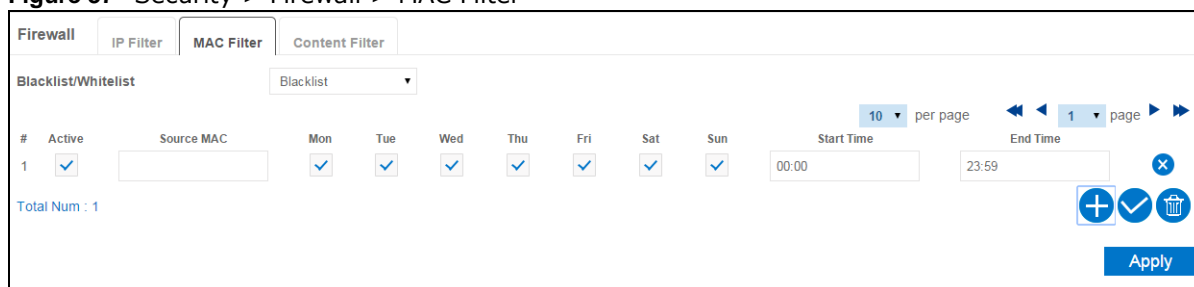
LABEL	DESCRIPTION
#	This field displays the rule index number. Click an entry to be able to modify the rule's settings.
Active	This field displays whether the rule is active or not. Click to enable or disable the rule.
Source IP	This field displays the source IP addresses to which this rule applies.

Table 32 Security > Firewall > IP Filter (continued)

LABEL	DESCRIPTION
Source from Port	This field displays a single port number of the source or the starting port number of a range. Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Source to Port	This field displays a single port number of the source or the ending port number of a range.
Destination IP	This field displays the destination IP addresses to which this rule applies.
Destination from Port	This field displays a single port number of the destination or the starting port number of a range. Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Destination to Port	This field displays a single port number of the destination or the ending port number of a range.
Protocol	This field displays the protocol (TCP , UDP , TCP/UDP or ICMP) used to transport the packets for which you want to apply the rule.
	Click an entry's delete icon to remove the rule.
  	Click the add icon to create a new rule. Click the OK icon to save the rule settings. Click the delete icon to remove all rules.
Total Num	This field displays the total number of IP filtering rules configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

8.3 MAC Filter Screen

MAC filtering means sifting traffic going through the WAH7003 based on the source MAC addresses. Use this screen to configure rules to restrict traffic by MAC addresses. To access this screen, click **Security > Firewall > MAC Filter**.





Figure 37 Security > Firewall > MAC Filter


The following table describes the labels in this screen.

Table 33 Security > Firewall > MAC Filter

LABEL	DESCRIPTION
Blacklist/Whitelist	Select Whitelist to specify traffic to allow and Blacklist to specify traffic to disallow.
#	This field displays the rule index number. Click an entry to be able to modify the rule's settings.

Table 33 Security > Firewall > MAC Filter (continued)

LABEL	DESCRIPTION
Active	This field displays whether the rule is active or not. Click to enable or disable the rule.
Source MAC	This field displays the source MAC address of the packets you wish to filter.
Mon ~ Sun	This field displays Y for the days that you want the WAH7003 to perform MAC filtering. Otherwise, it shows N .
Start Time End Time	This field displays the starting and ending time that the packets with the specified source MAC address are allowed or not allowed to go through the WAH7003.
	Click an entry's delete icon to remove the rule.
  	Click the add icon to create a new rule. Click the OK icon to save the rule settings. Click the delete icon to remove all rules.
Total Num	This field displays the total number of MAC filtering rules configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

8.4 Content Filter Screen

Use this screen to block the users on your network from accessing certain web sites. To access this screen, click **Security > Firewall > Content Filter**.





Figure 38 Security > Firewall > Content Filter


The following table describes the labels in this screen.

Table 34 Security > Firewall > Content Filter

LABEL	DESCRIPTION
Enable URL Filter	Select Off to disable content filtering. Select On to enable content filtering.
Blacklist/Whitelist	If you select Blacklist , the WAH7003 prohibits the users from accessing the web sites listed below. If you select Whitelist , the WAH7003 blocks all web sites except ones listed below.
#	This field displays the rule index number. Click an entry to be able to modify the rule's settings.

Table 34 Security > Firewall > Content Filter (continued)

LABEL	DESCRIPTION
Active	This field displays whether the rule is active or not. Click to enable or disable the rule.
URL	This field displays the website URL to which the WAH7003 blocks or allows access.
	Click an entry's delete icon to remove the rule.
  	Click the add icon to create a new rule. Click the OK icon to save the rule settings. Click the delete icon to remove all rules.
Total Num	This field displays the total number of content filtering rules configured on the WAH7003.
Apply	Click this button to save your changes to the WAH7003.

9.1 Overview

Use the system screens to configure general WAH7003 settings.

9.1.1 What You Can Do in this Chapter

- Use the **About** screen to view basic information about the WAH7003 ([Section 9.2 on page 63](#)).
- Use the **Configuration** screen to backup and restore device configurations. You can also reset your device settings back to the factory default ([Section 9.3 on page 64](#)).
- Use the **Firmware Upgrade** screen to upload new firmware to your WAH7003 ([Section 9.4 on page 65](#)).
- Use the **Power Saving** screen to enable and configure the power saving settings in the WAH7003. ([Section 9.5 on page 66](#)).
- Use the **Password** screen to change the WAH7003's system password ([Section 9.6 on page 66](#)).
- Use the **Date and Time** screens to change the WAH7003's time and date and configure daylight saving time ([Section 9.7 on page 67](#)).
- Use the **Language** screen to change the WAH7003's web configurator language ([Section 9.8 on page 69](#)).
- Use the **System Log** screens to view logged messages and specify to where the WAH7003 is to send logs ([Section 9.9 on page 70](#)).
- Use the **Reboot** screen to restart the WAH7003 ([Section 9.10 on page 71](#)).

9.2 About Screen

Use this screen to view basic information about the WAH7003. To access this screen, click **System > About**.

Figure 39 System > About

About	
Device Name	MiFi Configuration Manager
FW Version	1.00 (AAXB.0)C0
IMEI	352071000491300

The following table describes the labels in this screen.

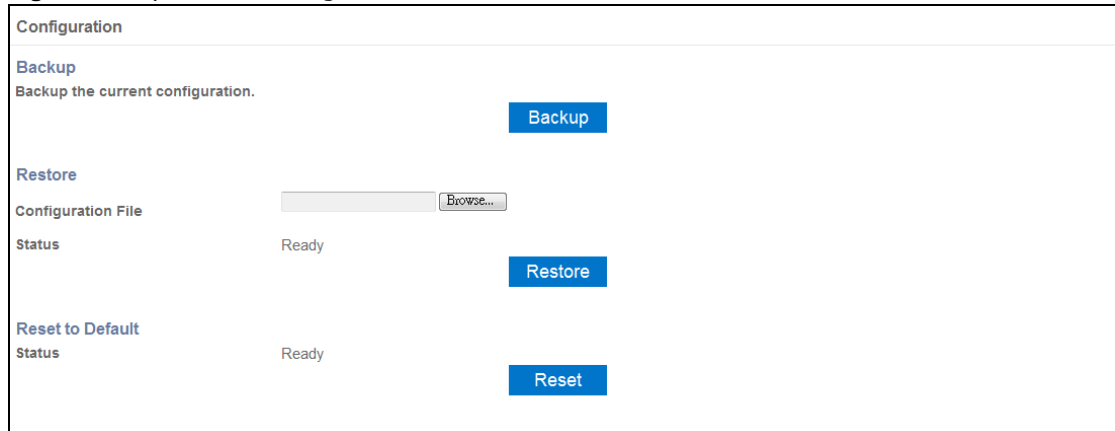
Table 35 System > About

LABEL	DESCRIPTION
Device Name	This displays the WAH7003 system name. It is used for identification.
FW Version	This displays the current firmware version of the WAH7003.
IMEI	This displays the International Mobile Equipment Number (IMEI) which is the serial number of the built-in 3G module. IMEI is a unique 15-digit number used to identify a mobile device.

9.3 Configuration Screen

The **Configuration** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

Figure 40 System > Configuration



9.3.1 Backup

Backup Configuration allows you to back up (save) the WAH7003's current configuration to a file on your computer. The configuration file should be saved and edited in UTF-8 (without BOM) format, if you're using Windows Notepad, make sure you choose **File > Save as UTF-8** in the text editor. Once your WAH7003 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the WAH7003's current configuration to your computer.

9.3.2 Restore

This screen allows you to upload a new or previously saved configuration file from your computer to your WAH7003.

Type in the location of the file you want to upload in the **Configuration File** field or click **Browse ...** or **Choose File** to find it. Remember that you must decompress compressed (.ZIP) files before you can upload them. Click **Restore** to begin the upload process. The WAH7003 automatically restarts.

Do not turn off the WAH7003 while configuration file upload is in progress.

After the WAH7003 configuration has been restored successfully, the login screen appears. If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.0.254).

9.3.3 Reset to Default

Click the **Reset** button to clear all user-entered configuration information and return the WAH7003 to its factory defaults. The WAH7003 automatically restarts.

You can also press the **Reset** button on the rear panel to reset the factory defaults of your WAH7003. Refer to [Section 1.7 on page 11](#) for more information on the **Reset** button.

9.4 Firmware Upgrade Screen

This screen allows you to upload new firmware to your WAH7003. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

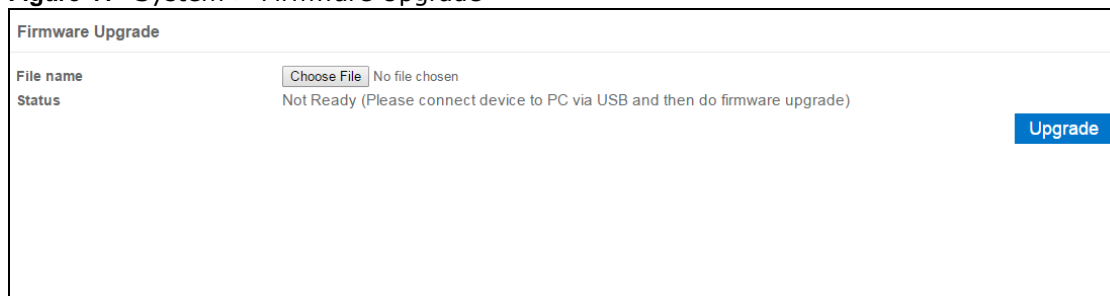
Only use firmware for your device's specific model.

To access this screen, click **System > Firmware Upgrade**. Type in the location of the file you want to upload in the **File name** field or click **Browse ...** or **Choose File** to find it. Remember that you must decompress compressed (.ZIP) files before you can upload them. Click **Upgrade** to begin the upload process.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the WAH7003 while firmware upload is in progress!

Figure 41 System > Firmware Upgrade



The screenshot shows the 'Firmware Upgrade' web interface. At the top, the title 'Firmware Upgrade' is displayed. Below the title, there are two rows of information. The first row is labeled 'File name' and contains a text input field with the placeholder text 'Choose File' and 'No file chosen'. The second row is labeled 'Status' and contains the text 'Not Ready (Please connect device to PC via USB and then do firmware upgrade)'. On the right side of the form, there is a blue button labeled 'Upgrade'.

9.5 Power Saving Screen

This screen allows you to enable and configure the power saving settings in the WAH7003. To access this screen, click **System > Power Saving**.

Figure 42 System > Power Saving

The following table describes the labels in this screen.

Table 36 System > Power Saving

LABEL	DESCRIPTION
Enable Auto Power Saving	Select On to activate power saving mode in the WAH7003. Otherwise, select Off .
Enter Standby Mode (seconds)	Specify the number of seconds the WAH7003 waits before going into standby mode to save battery power when the USB port is not connected and there is no wireless clients associating with the WAH7003. The WAH7003 wakes up from standby mode when the USB port is connected or there is a wireless client associating with it.
Enter Hibernate Mode (seconds)	Specify the number of seconds the WAH7003 waits before going into hibernate mode to save battery power when the USB port is not connected and there is no wireless clients associating with the WAH7003. When the WAH7003 is in hibernate mode, you need to press the power button to wake it up.
Auto Power Off (seconds)	Specify the number of seconds the WAH7003 waits before it automatically turns off when the USB port is not connected and there is no wireless clients associating with the WAH7003.
Apply	Click Apply to save your changes back to the WAH7003.

9.6 Password Screen

It is strongly recommended that you change your WAH7003's system password.

This screen allows you to change an account's password. See [Section 2.2 on page 13](#) for more information about login accounts.

Figure 43 System > Password

The following table describes the labels in this screen.

Table 37 System > Password

LABEL	DESCRIPTION
Select the user to change password	Select the account you want to configure.
Old password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password of between 4 and 8 characters. Note that as you type a password, the screen displays as dot (.) for each character you type.
Retype new password	Type the new password again in this field.
Apply	Click Apply to save your changes back to the WAH7003.

9.7 Date and Time Screens

For effective scheduling and logging, the WAH7003 system time must be accurate. The WAH7003 has a software mechanism to set the time manually or get the current time and date from an external server.

9.7.1 Date Screen

To change your WAH7003's time and date, click **System > Date and Time > Date**. The screen displays as shown. You can manually set the WAH7003's time and date or have the WAH7003 get the date and time from a time server.

Figure 44 System > Date and Time > Date

The following table describes the labels in this screen.

Table 38 System > Date and Time > Date

LABEL	DESCRIPTION
Current System Time	This field displays the present time and date of your WAH7003.
Mode	<p>Select Get from Time Server to have the WAH7003 get the time and date from the time server you specify. The WAH7003 requests time and date settings from the time server under the following circumstances.</p> <ul style="list-style-type: none"> • When the WAH7003 starts up. • When you click Apply in this screen. • 24-hour intervals after starting up. <p>Select Manual to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the WAH7003 uses the new setting once you click Apply.</p>
Time Protocol	Select a networking protocol which will be used for clock synchronization with the time server.
	The following fields are available if you set Mode to Manual .
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Mode to Manual , enter the new time in this field and then click Apply .
New Date (mm-dd-yyyy)	This field displays the last updated date from the time server or the last date configured manually. When you set Mode to Manual , enter the new date in this field and then click Apply .
	The following fields are available if you set Mode to Get from Time Server .
Time Server Address 1~4	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Apply	Click Apply to save your changes back to the WAH7003.

9.7.2 Time Zone Screen

To change your local time zone and configure daylight saving time, click **System > Date and Time > Time Zone**. The screen displays as shown.

Figure 45 System > Date and Time > Time Zone

The screenshot shows the 'Time Zone' configuration screen. At the top, there are two tabs: 'Date' and 'Time Zone', with 'Time Zone' selected. Below the tabs, the 'Time Zone' dropdown menu is set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. The 'Enable Daylight Saving' toggle is turned 'on'. The 'Start Date' is configured as 'First Sunday April 2 o'clock', and the 'End Date' is configured as 'Last Sunday October 2 o'clock'. An 'Apply' button is located at the bottom right.

The following table describes the labels in this screen.

Table 39 System > Date and Time > Time Zone

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select On if you use Daylight Saving Time. Otherwise, select Off .
Start Date	Configure the day and time when Daylight Saving Time starts if you set Enable Daylight Saving to On . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and type 2 in the o'clock field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you set Enable Daylight Saving to On . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes back to the WAH7003.

9.8 Language Screen

Use this screen to change the language for the Web Configurator. Click **System > Language**. The screen displays as shown.

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the WAH7003.

Figure 46 System > Language

Language

Language

9.9 System Log Screens

The Web Configurator allows you to look at all of the WAH7003's logs in one location.

9.9.1 Log Setting Screen

Use this screen to specify which logs to display in the **Log Display** screen and to where the WAH7003 is to send logs. Click **System > Log Setting**. The screen displays as shown.

Figure 47 System > Log Setting

System Log **Log Setting** Log Display

Enable Log On

Log Level

Enable Remote Log On

Remote Log Host

Remote Log Port

The following table describes the labels in this screen.

Table 40 System > Log Setting

LABEL	DESCRIPTION
Enable Log	Select On to enable system logging. Otherwise, select Off and the WAH7003 will not record the logs.
Log Level	Select the level of the logs that the WAH7003 is to record and send to the syslog server. The WAH7003 displays and records the logs with the level equal to or higher than what you selected.
Enable Remote Log	Select On to enable syslog logging. Otherwise, select Off . Syslog logging sends a log to an external log server.
Remote Log Host	Enter the server name or IP address of the syslog server that will log the selected log level of logs.
Remote Log Port	Enter the port number of the syslog server.
Apply	Click Apply to save your changes back to the WAH7003.

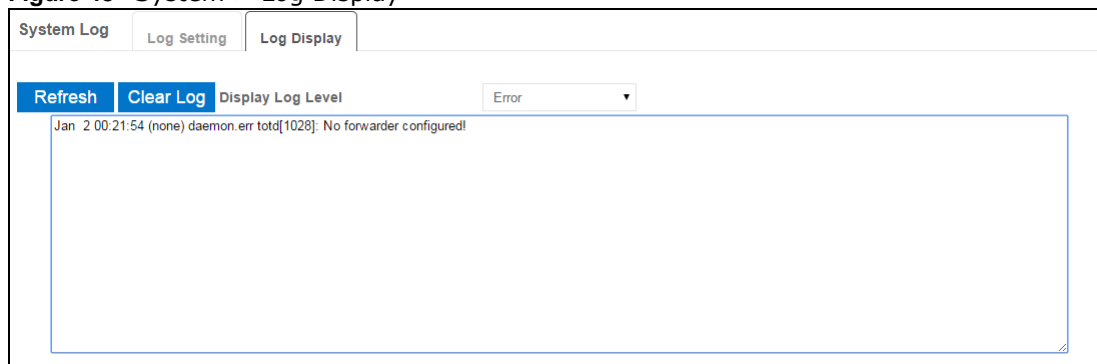
9.9.2 Log Display Screen

Use this screen to see the logged messages for the WAH7003. Click **System > Log Display**. The screen displays as shown.

The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display Log Level** drop list. When you select a log level, the WAH7003 searches through all logs of that level or higher. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

This screen displays the time the log message was recorded. It also displays the reason the log message was generated.

Figure 48 System > Log Display



9.10 Reboot Screen

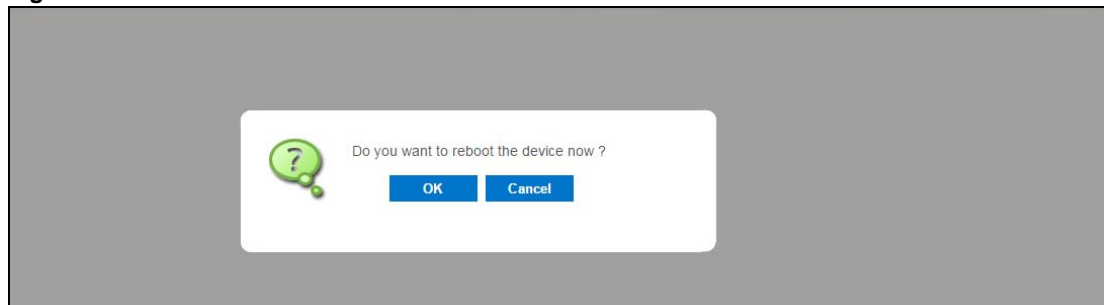
Use this screen to restart the device.

If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot.

Reboot is different to reset; reset returns the device to its default configuration.

This screen allows remote users can restart the device. To access this screen, click **System > Reboot**.

Figure 49 Maintenance > Reboot



Click the **OK** button to restart the WAH7003. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

Troubleshooting

10.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, and Hardware Installation](#)
- [WAH7003 Access and Login](#)
- [Internet Access](#)
- [Wireless Connections](#)

10.2 Power, and Hardware Installation

The WAH7003 does not turn on. The OLED display is not on.

- 1 Make sure the WAH7003 is correctly installed (refer to your Quick Start Guide).
- 2 Make sure the battery is installed and charged. Press the power button to turn the WAH7003 on. See [Section 1.5 on page 10](#) and [Section 1.6 on page 10](#).
- 3 If the problem continues, contact the vendor.

10.3 WAH7003 Access and Login

I forgot the IP address for the WAH7003.

- 1 The default IP address is 192.168.0.254.
- 2 If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.0.254.
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the WAH7003](#).
- 2 Make sure the WAH7003 is correctly installed and turned on. See the Quick Start Guide and [Section 1.5 on page 10](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 Make sure your computer is connected to the WAH7003 and is in the same subnet as the WAH7003.
- 5 Reset the device to its factory defaults, and try to access the WAH7003 with the default IP address. See [Section 1.7 on page 11](#).
- 6 Disconnect your computer from the Internet (Wireless and/or Ethernet) and then connect to the WAH7003 again.
- 7 If the problem continues, contact the vendor.

I forgot the password.

- 1 The default password is **admin** or **guest**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

I can see the **Login** screen, but I cannot log in to the WAH7003.

- 1 Make sure you have entered the user name and password correctly. The default password is **admin** or **guest**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after five minutes.
- 3 Disconnect and connect to the WAH7003 again.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

10.4 Internet Access

I cannot access the Internet.

- 5 Make sure your mobile access information (such as APN) is entered correctly in the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 6 Make sure your SIM card's account is valid and has an active data plan. Check your service contract or contact your service provider directly.
- 7 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAH7003), but my Internet connection is not available anymore.

- 8 Reboot the WAH7003.
- 9 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. If the WAH7003 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the WAH7003 closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the WAH7003.
- 4 If the problem continues, contact the network administrator or vendor.

10.5 Wireless Connections

I cannot access the WAH7003 or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the WAH7003.
- 2 Make sure the wireless adapter (installed on your computer) is working properly.

- 3 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the WAH7003's active radio.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAH7003.
- 5 Check that both the WAH7003 and your computer are using the same wireless and wireless security settings.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

10.6 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional websites are listed below.

See also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Asia

China

- ZyXEL Communications (Shanghai) Corp.
- ZyXEL Communications (Beijing) Corp.
- ZyXEL Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- ZyXEL Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- ZyXEL Kazakhstan
- <http://www.zyxel.kz>

Korea

- ZyXEL Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- ZyXEL Philippines
- <http://www.zyxel.com.ph>

Singapore

- ZyXEL Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Thailand

- ZyXEL Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- ZyXEL BY
- <http://www.zyxel.by>

Belgium

- ZyXEL Communications B.V.
- <http://www.zyxel.com/be/nl/>

Bulgaria

- ZyXEL България
- <http://www.zyxel.com/bg/bg/>

Czech

- ZyXEL Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- ZyXEL Communications A/S
- <http://www.zyxel.dk>

Estonia

- ZyXEL Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- ZyXEL Communications
- <http://www.zyxel.fi>

France

- ZyXEL France
- <http://www.zyxel.fr>

Germany

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- ZyXEL Hungary & SEE
- <http://www.zyxel.hu>

Latvia

- ZyXEL Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- ZyXEL Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- ZyXEL Benelux
- <http://www.zyxel.nl>

Norway

- ZyXEL Communications
- <http://www.zyxel.no>

Poland

- ZyXEL Communications Poland
- <http://www.zyxel.pl>

Romania

- ZyXEL Romania
- <http://www.zyxel.com/ro/ro>

Russia

- ZyXEL Russia
- <http://www.zyxel.ru>

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- ZyXEL Spain
- <http://www.zyxel.es>

Sweden

- ZyXEL Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG
- <http://www.zyxel.ch/>

Turkey

- ZyXEL Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- ZyXEL Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- ZyXEL Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Ecuador

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Egypt

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

Middle East

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- <http://www.us.zyxel.com/>

Oceania

Australia

- ZyXEL Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

Legal Information

Copyright

Copyright © 2015 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the WAH7003 is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Regulatory Notice and Statement

EUROPEAN UNION



The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE).

Български (Bulgarian)	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
Español (Spanish)	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	ZyXEL tímto prohlašuje, že tento zařízen je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.

Italiano (Italian)	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo ZyXEL deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, ZyXEL, jiddikjara li dan taghmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.

National Restrictions

This product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 2014/53/UE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 2014/53/UE) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 2014/53/EU folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":.

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This product is for indoor use only (utilisation intérieure exclusivement).
- FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)
 Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must fixed to US operation channels only.

The following warnings apply if product is disconnect device:

- A readily accessible disconnect device shall be incorporated external to the equipment; and/or
- The socket-outlet shall be installed near the equipment and shall be easily accessible.

Environment statement

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

WEEE Directive



Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

"INFORMAZIONI AGLI UTENTI"

Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

La raccolta differenziata della presente apparecchiatura giunta a fine vita e organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

Environmental Product Declaration

Bългарски (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
<p>Екологична продуктова декларация</p> <p>RoHS Директива 2011/65/ЕО WEEE Директива 2012/19/ЕО PPW Директива 94/62/ЕО REACH Регламент (ЕО) № 1907/2006 ErP Директива 2009/125/ЕО</p> <p>Име/ титла : Richard Hsu / Quality Management Division Senior Manager Подпис : Дата (dd/mm/yyyy) : 01/10/2014</p>  	<p>Environmentální prohlášení o produktu</p> <p>RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/62/EC REACH Nařízení (ES) č. 1907/2006 ErP Směrnice 2009/125/ES</p> <p>Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014</p>  	<p>Miljøerklæring</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ titel : Richard Hsu / Quality Management Division Senior Manager Underskrift : Dato (dd/mm/åååå) : 01/10/2014</p>  	<p>Produkt-Umweltdeklaration</p> <p>RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/62/EG REACH VERORDNUNG (EG) Nr. 1907/2006 ErP Richtlinie 2009/125/EG</p> <p>Name/ Titel : Richard Hsu / Quality Management Division Senior Manager Unterschrift : Datum (dd/mm/yyyy) : 2014/10/01</p>  
Eesti keel (Estonian)	English	Español (Spanish)	Français (French)
<p>Toote keskkonnadeklaratsioon</p> <p>RoHS Direktiiv 2011/65/EL WEEE Direktiiv 2012/19/EL PPW Direktiiv 94/62/EÜ REACH MAARLUS (EÜ) nr 1907/2006 ErP Direktiiv 2009/125/EÜ</p> <p>Nimi/ pealkiri : Richard Hsu / Quality Management Division Senior Manager Allkiri : Kuupäev (pp/kk/aaaa) : 01/10/2014</p>  	<p>Environmental product declaration</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/62/EC REACH Regulation (EC) No 1907/2006 ErP Directive 2009/125/EC</p> <p>Name/ title : Richard Hsu / Quality Management Division Senior Manager Signature : Date (dd/mm/yyyy) : 01/10/2014</p>  	<p>Declaraciones Ambientales de Producto</p> <p>RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGLAMENTO (CE) nº 1907/2006 ErP Directiva 2009/125/CE</p> <p>Nombre/ título : Richard Hsu / Quality Management Division Senior Manager Firma : Fecha (aaaa/mm/dd) : 2014/10/01</p>  	<p>Profil environnemental de produit</p> <p>RoHS Directive 2011/65/UE WEEE Directive 2012/19/UE PPW Directive 94/62/CE REACH RÈGLEMENT (CE) N° 1907/2006 ErP Directive 2009/125/CE</p> <p>Nom/ titre : Richard Hsu / Quality Management Division Senior Manager Signature : Date (dd/mm/yyyy) : 2014/10/01</p>  
Hrvatski (Croatian)	Italiano (Italian)	Latviešu valoda (Latvian)	Lietuvių kalba (Lithuanian)
<p>Deklaraciju o zbirjanju proizvoda</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/EZ REACH Uredbe (EZ) br. 1907/2006 ErP Direktiva 2009/125/EZ</p> <p>Ime/ nadim : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014</p>  	<p>Dichiarazione ambientale di prodotto</p> <p>RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) n. 1907/2006 ErP Direttiva 2009/125/CE</p> <p>Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager Firma : Data (aaaa/mm/yy) : 2014/10/01</p>  	<p>Produkta vides ietekmējuma deklarācija</p> <p>RoHS Direktīva 2011/65/ES WEEE Direktīva 2012/19/ES PPW Direktīva 94/62/EK REACH Regula (EK) Nr. 1907/2006 ErP Direktīva 2009/125/EK</p> <p>Nosaukums/ tālrunis : Richard Hsu / Quality Management Division Senior Manager Paraksts : Datums (dd/mm/yyyy) : 01/10/2014</p>  	<p>Aplinkosauging gaminių deklaraciją</p> <p>RoHS Direktyva 2011/65/ES WEEE Direktyva 2012/19/ES PPW Direktyva 94/62/WE REACH REGLAMENTAS (EB) Nr. 1907/2006 ErP Direktyva 2009/125/EB</p> <p>Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager Parašas : Data (ddmmmmmm) : 01/10/2014</p>  
Magyar (Hungarian)	Malti (Maltese)	Nederlands (Dutch)	Polski (Polish)
<p>Környezetvédelmi terméknyilatkozat</p> <p>RoHS 2011/65/EU irányelve WEEE 2012/19/EU irányelve PPW 94/62/EK irányelve REACH 1907/2006/EK rendelet ErP 2009/125/EK irányelve</p> <p>Név/ cím : Richard Hsu / Quality Management Division Senior Manager Aláírás : Dátum (dd/mm/yyyy) : 2014/10/01</p>  	<p>Dikjarazzjoni Ambjentali dwar il-Prodott</p> <p>RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) NR 1907/2006 ErP Direttiva 2009/125/CE</p> <p>Isem/ it-titlu : Richard Hsu / Quality Management Division Senior Manager Firma : Data (dd/mm/yyyy) : 2014/10/01</p>  	<p>Milieuproductverklaring</p> <p>RoHS Richtlijn 2011/65/EU WEEE Richtlijn 2012/19/EU PPW Richtlijn 94/62/EG REACH Verordening (EG) nr. 1907/2006 ErP Richtlijn 2009/125/EG</p> <p>Naam/ titel : Richard Hsu / Quality Management Division Senior Manager Handtekening : Datum (dd/mm/jaar) : 01/10/2014</p>  	<p>Deklarację środowiskową produktu</p> <p>RoHS Dyrektywa 2011/65/UE WEEE Dyrektywa 2012/19/UE PPW Dyrektywa 94/62/WE REACH Rozporządzenie (WE) nr. 1907/2006 ErP Dyrektywa 2009/125/WE</p> <p>Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager Podpis : Data (ddmmmmmm) : 2014/10/01</p>  
Português (Portuguese)	Română (Romanian)	Slovenčina (Slovak)	Slovenščina (Slovene)
<p>Declaração ambiental do produto</p> <p>RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH Regulamento (CE) nº 1907/2006 ErP Diretiva 2009/125/CE</p> <p>Nome/ título : Richard Hsu / Quality Management Division Senior Manager Assinatura : Data (dd/mm/aaaa) : 01/10/2014</p>  	<p>Declarație de mediu privind produsele</p> <p>RoHS Directivă 2011/65/UE WEEE Directivă 2012/19/UE PPW Directivă 94/62/CE REACH REGULAMENTUL (CE) NR. 1907/2006 ErP Directivă 2009/125/CE</p> <p>Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager Semnatura : Data (dd/mm/aaaa) : 01/10/2014</p>  	<p>Vyhľadzenie o environmentálnom výrobku</p> <p>RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EU PPW Smernica 94/62/ES REACH Nariadenie (ES) č. 1907/2006 ErP Smernica 2009/125/ES</p> <p>Meno/ titul : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014</p>  	<p>Okolijsko deklaracija izdelka</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/ES REACH Uredba (ES) št. 1907/2006 ErP Direktiva 2009/125/ES</p> <p>Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014</p>  
Suomi (Finnish)	Svenska (Swedish)	Ελληνικό (Greek)	Norsk (Norwegian)
<p>Standardin perustava ympäristötietustieto</p> <p>RoHS Direktiiv 2011/65/EU WEEE Direktiiv 2012/19/EU PPW Direktiiv 94/62/EY REACH ASETUS (EY) N:o 1907/2006 ErP Direktiiv 2009/125/EY</p> <p>Nimi/ osasto : Richard Hsu / Quality Management Division Senior Manager Ala kirjuri : Päivämäärä (pp/kk/vvvv) : 01/10/2014</p>  	<p>Miljöproduktdeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EG REACH Förordning (EG) nr 1907/2006 ErP Direktiv 2009/125/EG</p> <p>Namn/ titel : Richard Hsu / Quality Management Division Senior Manager Namnteckning : Datum (dd/mm/åååå) : 01/10/2014</p>  	<p>Περιβαλλοντική δήλωση προϊόντος</p> <p>RoHS Οδηγία 2011/65/ΕΕ WEEE Οδηγία 2012/19/ΕΕ PPW Οδηγία 94/62/ΕΚ REACH Κ.ε.π.σ.ν.α.ρ.ο.υ. (ΕΚ) αριθ. 1907/2006 ErP Οδηγία 2009/125/ΕΚ</p> <p>Όνομα/ τίτλος : Richard Hsu / Quality Management Division Senior Manager Υπογραφή : Ημερομηνία (ηη/μμ/εεεε) : 01/10/2014</p>  	<p>Miljødeklarasjon</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager Signatur : Dato (dd/mm/åååå) : 01/10/2014</p>  

台灣

802.11b/802.11g 警語：

第十二條→經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條→低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

802.11a 警語：

無線傳輸設備 (UNII)

在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。(4.7.5)

無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。(4.7.6)

無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。(4.7.7)

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw.

Index

A

access [13](#)
authentication [49](#), [50](#)
 RADIUS server [50](#)

B

Broadband [24](#)

C

certifications
 viewing [87](#)
channel, wireless LAN [48](#)
configuration [9](#)
contact information [76](#)
cookies [13](#)
copyright [82](#)
CTS threshold [49](#)
current date/time [67](#)
 daylight savings [69](#)
customer support [76](#)

D

data fragment threshold [49](#)
date [67](#)
daylight savings [69](#)
disclaimer [82](#)
documentation
 related [2](#)

E

encryption [51](#)
ESSID [74](#)
Extended Service Set IDentification [43](#)

F

filters
 MAC address [45](#), [50](#)
Firefox [13](#)
fragmentation threshold [49](#)

G

General wireless LAN screen [41](#)
Guide
 Quick Start [2](#)

H

hardware connections [10](#)

I

installation [9](#)
Internet Explorer [13](#)
IP Address [32](#)

J

Java
 permissions [13](#)

JavaScripts [13](#)

L

LEDs [10](#)

limitations

 wireless LAN [51](#)

 WPS [57](#)

logout

 Web Configurator [16](#)

M

MAC address

 filter [45, 50](#)

MAC authentication [45](#)

maintenance [9](#)

management [9](#)

managing the device

 good habits [10](#)

N

Netscape Navigator [13](#)

O

other documentation [2](#)

overview [9](#)

P

PBC [52](#)

PIN, WPS [52](#)

 example [54](#)

pop-up windows [13](#)

preamble [49](#)

product registration [87](#)

Push Button Configuration, see PBC

push button, WPS [52](#)

Q

Quick Start Guide [2](#)

R

RADIUS server [50](#)

reboot [71](#)

 vs reset [71](#)

registration

 product [87](#)

related documentation [2](#)

reset

 vs reboot [71](#)

restart [71](#)

RTS threshold [49](#)

S

screen resolution [13](#)

security

 wireless LAN [49](#)

Service Set [43](#)

SIM card [10](#)

SSID [50](#)

status [20](#)

supported browsers [13](#)

system name [20](#)

T

thresholds

 data fragment [49](#)

 RTS/CTS [49](#)

time [67](#)

trademarks [82](#)

U

example [54](#)
push button [52](#)

use [9](#)

W

WAN

Wide Area Network, see WAN [24](#)

warranty [87](#)

note [87](#)

Web Configurator [9, 13](#)

access [13](#)

requirements [13](#)

supported browsers [13](#)

web configurator [9](#)

WEP [51](#)

Wi-Fi [40](#)

wireless channel [74](#)

wireless LAN [40, 47, 74](#)

authentication [49, 50](#)

channel [48](#)

encryption [51](#)

example [47](#)

fragmentation threshold [49](#)

limitations [51](#)

MAC address filter [45, 50](#)

preamble [49](#)

RADIUS server [50](#)

RTS/CTS threshold [49](#)

security [49](#)

SSID [50](#)

WEP [51](#)

WPA [51](#)

WPA-PSK [51](#)

WPS [52, 54](#)

example [55](#)

limitations [57](#)

PIN [52](#)

push button [52](#)

wireless security [74](#)

WPA [51](#)

WPA-PSK [51](#)

WPS [52, 54](#)

example [55](#)

limitations [57](#)

PIN [52](#)