

# User's Guide

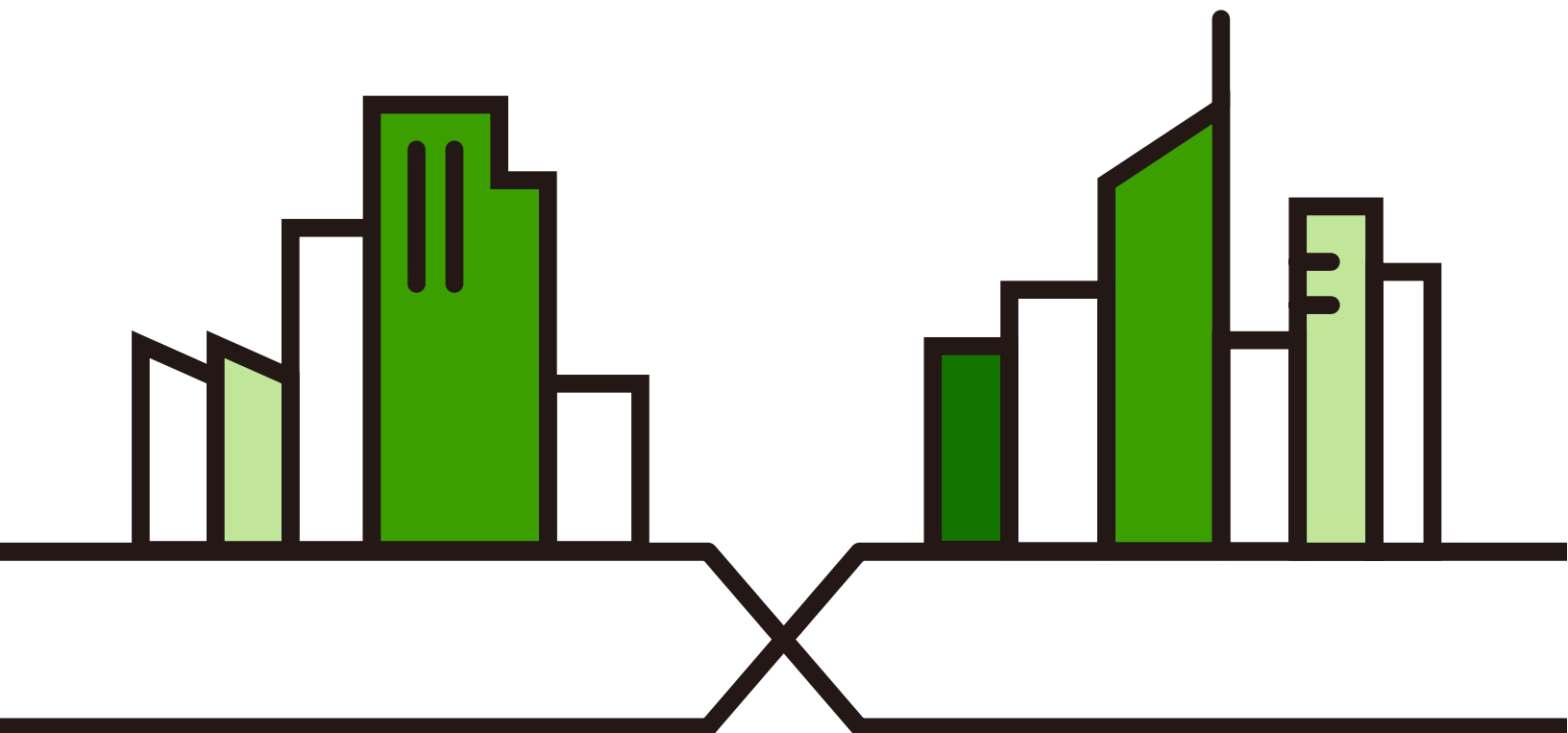
## NWA50AX PRO/NWA90AX PRO/ NWA55AXE

802.11ax (WiFi6) Dual-Radio PoE Access Point/802.11ax (WiFi6)  
Dual-Radio Outdoor PoE Access Point

### Default Login Details

Management IP Address	http://DHCP-assigned IP OR http://192.168.1.2
User Name	admin
Password	1234

Version 6.29/6.55 Edition 1, 01/2023



---

## **IMPORTANT**

### **READ CAREFULLY BEFORE USE**

### **KEEP THIS GUIDE FOR FUTURE REFERENCE**

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product hardware, firmware, or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Some screens or options in this book may not be available for your product (see the product feature tables in [Section 1.2 on page 12](#)).

### **Related Documentation**

- Quick Start Guide

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

- CLI Reference Guide

The CLI Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the Zyxel Device.

Note: It is recommended you use the Web Configurator to configure the Zyxel Device.

- Web Configurator Online Help

Click the help icon in any screen for help in configuring that screen and supplementary information.

- Nebula Control Center User's Guide

This User's Guide shows how to manage the Zyxel Device remotely. The features of these devices can be managed through Nebula Control Center. It also offers features that are not available when the Zyxel Device is in standalone mode (see [Section 2.1.2 on page 22](#)).

- More Information

Go to **support.zyxe1.com** to find other information on the Zyxel Device.



# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this guide.

**Warnings tell you about things that could harm you or your device.**











Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- All models in this series may be referred to as the “Zyxel Device” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Configuration > Network > IP Setting** means you first click **Configuration** in the navigation panel, then the **Network** sub menu and finally the **IP Setting** tab to get to that screen.

## Icons Used in Figures

Figures in this guide may use the following generic icons. The Zyxel Device icon is not an exact representation of your device.

Zyxel Device 	Router 	Switch 	Internet 
Server 	Desktop 	Laptop 	IP Phone 
Printer 	Smart T.V. 		

# Contents Overview

Introduction .....	12
AP Management .....	22
Hardware .....	30
Web Configurator .....	33
<b>Standalone Configuration .....</b>	<b>44</b>
Standalone Configuration .....	45
Dashboard .....	47
Setup Wizard .....	53
Monitor .....	59
Network .....	71
Wireless .....	78
User .....	91
AP Profile .....	98
WDS Profile .....	129
Certificates .....	131
System .....	147
Log and Report .....	166
File Manager .....	172
Diagnostics .....	183
LEDs .....	185
Reboot .....	188
Shutdown .....	189
<b>Local Configuration in Cloud Mode .....</b>	<b>190</b>
Cloud Mode .....	191
Network .....	194
Maintenance .....	197
<b>Appendices and Troubleshooting .....</b>	<b>202</b>
Troubleshooting .....	203

# Table of Contents

<b>Document Conventions .....</b>	<b>3</b>
<b>Contents Overview .....</b>	<b>4</b>
<b>Table of Contents .....</b>	<b>5</b>
<b>Chapter 1</b>	
<b>Introduction .....</b>	<b>12</b>
1.1 Overview .....	12
1.2 Zyxel Device Product Feature Comparison .....	12
1.3 Zyxel Device Roles .....	14
1.3.1 Root AP .....	17
1.3.2 Wireless Repeater .....	17
1.3.3 Radio Frequency (RF) Monitor .....	19
1.4 Sample Feature Applications .....	19
1.4.1 MBSSID .....	19
1.4.2 Dual-Radio .....	20
<b>Chapter 2</b>	
<b>AP Management.....</b>	<b>22</b>
2.1 Management Mode .....	22
2.1.1 Standalone .....	22
2.1.2 Nebula Control Center .....	22
2.2 Switching Management Modes .....	24
2.3 Zyxel One Network (ZON) Utility .....	24
2.3.1 Requirements .....	24
2.3.2 Run the ZON Utility .....	25
2.4 Ways to Access the Zyxel Device .....	28
2.5 Good Habits for Managing the Zyxel Device .....	29
<b>Chapter 3</b>	
<b>Hardware .....</b>	<b>30</b>
3.1 Zyxel Device Single LED .....	30
3.1.1 Zyxel Device LED .....	30
<b>Chapter 4</b>	
<b>Web Configurator.....</b>	<b>33</b>
4.1 Overview .....	33
4.2 Accessing the Web Configurator .....	33
4.3 Navigating the Web Configurator .....	36

4.3.1 Title Bar .....	37
4.3.2 Navigation Panel .....	38
4.3.3 Standalone Mode Navigation Panel Menus .....	38
4.3.4 Cloud Mode Navigation Panel Menus .....	40
4.3.5 Tables and Lists .....	41

## **Part I: Standalone Configuration..... 44**

### **Chapter 5 Standalone Configuration.....45**

5.1 Overview .....	45
5.2 Starting and Stopping the Zyxel Device .....	45

### **Chapter 6 Dashboard.....47**

6.1 Overview .....	47
6.1.1 CPU Usage .....	50
6.1.2 Memory Usage .....	51

### **Chapter 7 Setup Wizard.....53**

7.1 Accessing the Wizard .....	53
7.2 Using the Wizard .....	53
7.2.1 Step 1 Time Settings .....	53
7.2.2 Step 2 Password and Uplink Connection .....	54
7.2.3 Step 3 Radio .....	55
7.2.4 Step 4 SSID .....	56
7.2.5 Summary .....	58

### **Chapter 8 Monitor.....59**

8.1 Overview .....	59
8.1.1 What You Can Do in this Chapter .....	59
8.2 What You Need to Know .....	59
8.3 Network Status .....	60
8.3.1 Port Statistics Graph .....	61
8.4 Radio List .....	62
8.4.1 AP Mode Radio Information .....	64
8.5 Station List .....	65
8.6 WDS Link Info .....	66
8.7 Detected Device .....	67

8.8 View Log .....	69
<b>Chapter 9</b>	
<b>Network.....</b>	<b>71</b>
9.1 Overview .....	71
9.1.1 What You Can Do in this Chapter .....	71
9.2 IP Setting .....	71
9.3 VLAN .....	73
9.4 NCC Discovery .....	76
<b>Chapter 10</b>	
<b>Wireless .....</b>	<b>78</b>
10.1 Overview .....	78
10.1.1 What You Can Do in this Chapter .....	78
10.1.2 What You Need to Know .....	79
10.2 AP Management .....	79
10.3 Rogue AP .....	85
10.3.1 Add/Edit Rogue/Friendly List .....	88
10.4 DCS .....	89
10.5 Technical Reference .....	89
<b>Chapter 11</b>	
<b>User.....</b>	<b>91</b>
11.1 Overview .....	91
11.1.1 What You Can Do in this Chapter .....	91
11.1.2 What You Need To Know .....	91
11.2 User Summary .....	92
11.2.1 Add/Edit User .....	92
11.3 Setting .....	94
11.3.1 Edit User Authentication Timeout Settings .....	96
<b>Chapter 12</b>	
<b>AP Profile .....</b>	<b>98</b>
12.1 Overview .....	98
12.1.1 What You Can Do in this Chapter .....	98
12.1.2 What You Need To Know .....	98
12.2 Radio .....	100
12.2.1 Add/Edit Radio Profile .....	100
12.3 SSID .....	106
12.3.1 SSID List .....	106
12.3.2 Add/Edit SSID Profile .....	108
12.4 Security List .....	110
12.4.1 Add/Edit Security Profile .....	111

12.5 MAC Filter List .....	124
12.5.1 Add/Edit MAC Filter Profile .....	125
12.6 Layer-2 Isolation List .....	126
12.6.1 Add/Edit Layer-2 Isolation Profile .....	127
<b>Chapter 13</b>	
<b>WDS Profile .....</b>	<b>129</b>
13.1 Overview .....	129
13.1.1 What You Can Do in this Chapter .....	129
13.2 WDS Profile .....	129
13.2.1 Add/Edit WDS Profile .....	130
<b>Chapter 14</b>	
<b>Certificates .....</b>	<b>131</b>
14.1 Overview .....	131
14.1.1 What You Can Do in this Chapter .....	131
14.1.2 What You Need to Know .....	131
14.1.3 Verifying a Certificate .....	133
14.2 My Certificates .....	134
14.2.1 Add My Certificates .....	135
14.2.2 Edit My Certificates .....	137
14.2.3 Import Certificates .....	140
14.3 Trusted Certificates .....	141
14.3.1 Edit Trusted Certificates .....	142
14.3.2 Import Trusted Certificates .....	145
14.4 Technical Reference .....	146
<b>Chapter 15</b>	
<b>System .....</b>	<b>147</b>
15.1 Overview .....	147
15.1.1 What You Can Do in this Chapter .....	147
15.2 Host Name .....	147
15.3 Date and Time .....	148
15.3.1 Pre-defined NTP Time Servers List .....	150
15.3.2 Time Server Synchronization .....	151
15.4 WWW Overview .....	152
15.4.1 Service Access Limitations .....	152
15.4.2 System Timeout .....	152
15.4.3 HTTPS .....	152
15.4.4 Configuring WWW Service Control .....	153
15.4.5 HTTPS Example .....	155
15.5 SSH .....	160
15.5.1 How SSH Works .....	161



15.5.2 SSH Implementation on the Zyxel Device .....	162
15.5.3 Requirements for Using SSH .....	162
15.5.4 Configuring SSH .....	162
15.5.5 Examples of Secure Telnet Using SSH .....	163
15.6 FTP .....	164
<b>Chapter 16</b>	
<b>Log and Report.....</b>	<b>166</b>
16.1 Overview .....	166
16.1.1 What You Can Do In this Chapter .....	166
16.2 Log Setting .....	166
16.2.1 Log Setting Screen .....	166
16.2.2 Edit Remote Server .....	167
16.2.3 Active Log Summary .....	169
<b>Chapter 17</b>	
<b>File Manager.....</b>	<b>172</b>
17.1 Overview .....	172
17.1.1 What You Can Do in this Chapter .....	172
17.1.2 What you Need to Know .....	172
17.2 Configuration File .....	173
17.2.1 Example of Configuration File Download Using FTP .....	177
17.3 Firmware Package .....	178
17.3.1 Example of Firmware Upload Using FTP .....	179
17.4 Shell Script .....	180
<b>Chapter 18</b>	
<b>Diagnostics .....</b>	<b>183</b>
18.1 Overview .....	183
18.1.1 What You Can Do in this Chapter .....	183
18.2 Diagnostics .....	183
18.3 Remote Capture .....	184
<b>Chapter 19</b>	
<b>LEDs .....</b>	<b>185</b>
19.1 Overview .....	185
19.1.1 What You Can Do in this Chapter .....	185
19.2 Suppression Screen .....	185
19.3 Locator Screen .....	186
<b>Chapter 20</b>	
<b>Reboot.....</b>	<b>188</b>
20.1 Overview .....	188

20.1.1 What You Need To Know .....	188
20.2 Reboot .....	188
<b>Chapter 21</b>	
<b>Shutdown .....</b>	<b>189</b>
21.1 Overview .....	189
21.1.1 What You Need To Know .....	189
21.2 Shutdown .....	189
 <b>Part II: Local Configuration in Cloud Mode .....</b>	 <b>190</b>
<b>Chapter 22</b>	
<b>Cloud Mode .....</b>	<b>191</b>
22.1 Overview .....	191
22.2 Cloud Mode Web Configurator Screens .....	191
22.3 Dashboard .....	192
<b>Chapter 23</b>	
<b>Network .....</b>	<b>194</b>
23.1 Overview .....	194
23.1.1 What You Can Do in this Chapter .....	194
23.2 IP Setting .....	194
23.3 VLAN .....	196
<b>Chapter 24</b>	
<b>Maintenance .....</b>	<b>197</b>
24.1 Overview .....	197
24.1.1 What You Can Do in this Chapter .....	197
24.2 Shell Script .....	197
24.3 Diagnostics .....	198
24.4 View Log .....	199
 <b>Part III: Appendices and Troubleshooting .....</b>	 <b>202</b>
<b>Chapter 25</b>	
<b>Troubleshooting .....</b>	<b>203</b>
25.1 Overview .....	203
25.2 Power, Hardware Connections, and LED .....	203
25.3 Zyxel Device Management, Access, and Login .....	204
25.4 Internet Access .....	207

25.5 WiFi Network .....	208
25.6 Resetting the Zyxel Device .....	210
25.7 Getting More Troubleshooting Help .....	210
Appendix A Importing Certificates .....	211
Appendix B IPv6.....	235
Appendix C Customer Support .....	243
Appendix D Legal Information .....	248
<b>Index .....</b>	<b>256</b>

# CHAPTER 1

## Introduction

### 1.1 Overview

This User's Guide covers the models listed below:

- NWA50AX
- NWA90AX
- NWA55AXE
- NWA50AX PRO
- NWA90AX PRO

The Zyxel Device can be managed in one of the following methods: remote management through Nebula Control Center (NCC) or local management in Standalone Mode. The Zyxel Device runs in standalone mode by default, but it is recommended to use NCC management if it is available for your device. For more information about Access Point (AP) management, see [Section 2.1 on page 22](#).

Use the Zyxel Device to set up a WiFi network with other IEEE 802.11a/b/g/n/ac/ax compatible devices in either 2.4 GHz and 5 GHz networks or both at the same time.

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See [Section 1.3.2 on page 17](#) for more information on root and repeater APs and how to set them up.

The screens you see in the web configurator may be different depending on the Zyxel Device model you're using.

### 1.2 Zyxel Device Product Feature Comparison

The following table lists the features of the Zyxel Device.

Table 1 Zyxel Device Product Feature Table

FEATURES	NWA50AX	NWA90AX	NWA55AXE
Supported WiFi Standards	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80 MHz

Table 1 Zyxel Device Product Feature Table (continued)

FEATURES	NWA50AX	NWA90AX	NWA55AXE
Available Security Modes	None Enhanced-open WEP WPA2-MIX-Personal WPA3-Personal	None Enhanced-open WEP WPA2-MIX / WPA3 - Personal & Enterprise	None Enhanced-open WEP WPA2-MIX-Personal WPA3-Personal
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	2	2
Security Profile Radius Settings	No	Yes	No
Security Profile Enterprise Authentication Settings	No	Yes	No
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge VLAN	No	No	Yes
Layer-2 Isolation	No	Yes	No
Supported PoE Standards	IEEE 802.3at	IEEE 802.3at	IEEE 802.3at
Power Detection	No	No	No
External Antennas	No	No	Yes
Internal Antennas	Yes	Yes	No
Console Port	4-Pin Serial	4-Pin Serial	No
Reset button	Yes	Yes	No
LED Locator	Yes	Yes	No
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	No	No	No
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Ethernet Storm Control	No	No	No
Grounding	No	No	No
Power Jack	Yes	Yes	No
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	6.29	6.29	6.29

The following table lists the features of the Zyxel Device.

Table 2 Zyxel Device Product Feature Table

FEATURES	NWA50AX PRO	NWA90AX PRO
Supported WiFi Standards	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz

Table 2 Zyxel Device Product Feature Table (continued)

FEATURES	NWA50AX PRO	NWA90AX PRO
Available Security Modes	None Enhanced-open WEP WPA2-MIX-Personal WPA3-Personal	None Enhanced-open WEP WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64
Number of WiFi Radios	2	2
Security Profile Radius Settings	No	Yes
Security Profile Enterprise Authentication Settings	No	Yes
Rogue AP Detection	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes
Wireless Bridge VLAN	No	No
Layer-2 Isolation	No	Yes
Supported PoE Standards	IEEE 802.3at	IEEE 802.3at
Power Detection	No	No
External Antennas	No	No
Internal Antennas	Yes	Yes
Console Port	4-Pin Serial	4-Pin Serial
Reset button	Yes	Yes
LED Locator	Yes	Yes
LED Suppression	Yes	Yes
AC (AP Controller) Discovery	No	No
NCC Discovery	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes
Ethernet Storm Control	No	No
Grounding	No	No
Power Jack	Yes	Yes
Maximum number of log messages	512 event logs	
Latest Firmware Version Supported	6.55	6.55

## 1.3 Zyxel Device Roles

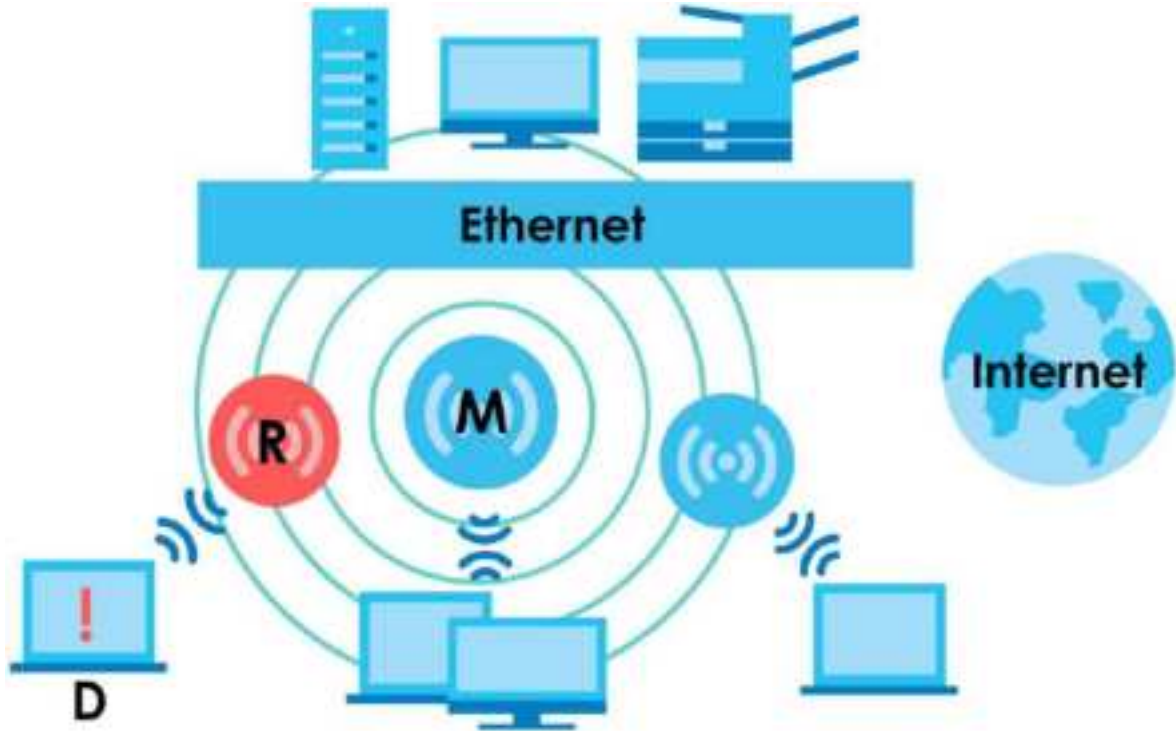
This section describes some of the different roles that your Zyxel Device can take up within a network. Not all roles are supported by all models (see [Section 1.2 on page 12](#)). The Zyxel Device can serve as a:

- Access Point (AP) - This is used to allow WiFi clients to connect to the Internet.
- Radio Frequency (RF) monitor - If your Zyxel Device supports rogue APs detection, it can serve as an RF monitor and searches for rogue APs to help eliminate network threats. An RF monitor can simultaneously act as an AP.

- Root AP - A root AP connects to the gateway or switch through a wired Ethernet connection and has wireless repeaters connected to it to extend its range.
- Wireless repeater - A wireless repeater wirelessly connects to a root AP and extends the network's wireless range. A wireless repeater can also be a wireless bridge that connects to a root AP and extends the network to wired client devices.

If a client (**D**) tries to set up his own AP (**R**) with weak security settings, the network becomes exposed to threats. The RF monitor (**M**) scans the area to detect all APs, which can help the network administrator discover these rogue APs.

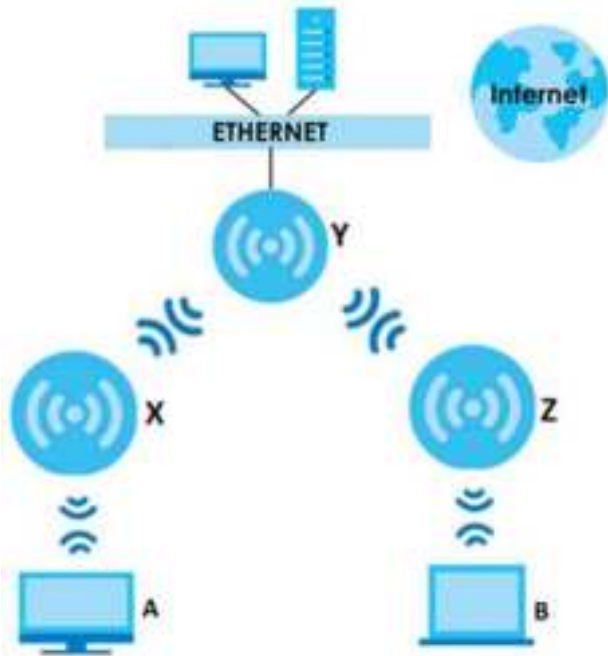
**Figure 1** Zyxel Device Application in a Network



### Wireless Distribution System (WDS) and Wireless Bridge

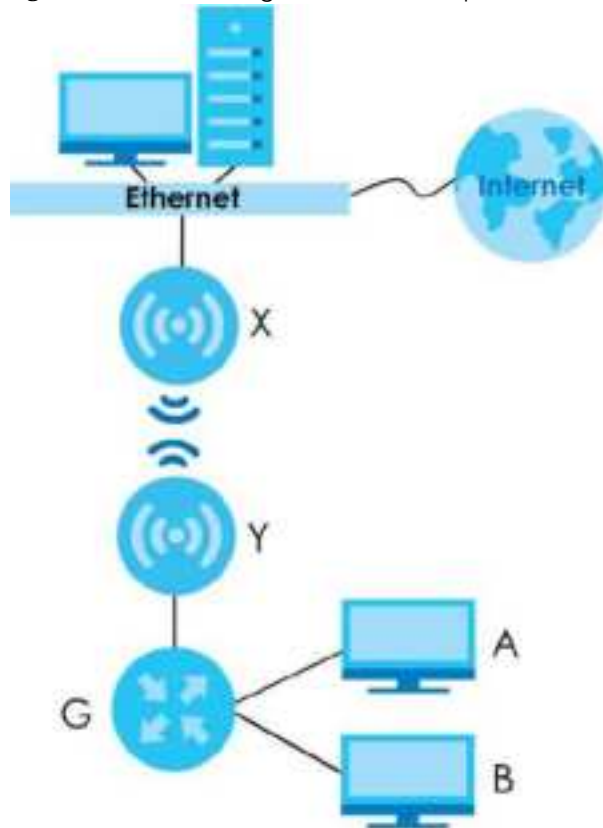
Wireless Distribution System (WDS) is a network system that allows you to distribute the network to areas that require Internet connections. You can extend your network to unreachable areas with wireless repeaters, or with wireless repeaters acting as wireless bridges.

The following figure shows you how to create a secure WDS with two wireless repeaters. The root AP (**Y**) is connected to a network with Internet access and has wireless repeaters (**X** and **Z**) connected to it to expand the WiFi network's range. Clients (**A** and **B**) can access the wired network through the wireless repeaters (**X** and **Z**) and/or root AP.

**Figure 2** Wireless Distribution System Network Example

The following figure shows an example of a WDS with a repeater acting as a wireless bridge. A wireless bridge can connect two wired networks through a wireless connection. The root AP (**X**) is connected to a network with Internet access. The wireless repeater (**Y**) is connected to the root AP (**X**) to expand the network. Clients (**A** and **B**) are connected to the wireless repeater through the switch/gateway/router (**G**). They can access the network with the extended wired network the wireless bridge (wireless repeater) provides.



**Figure 3** Wireless Bridge Network Example

### 1.3.1 Root AP

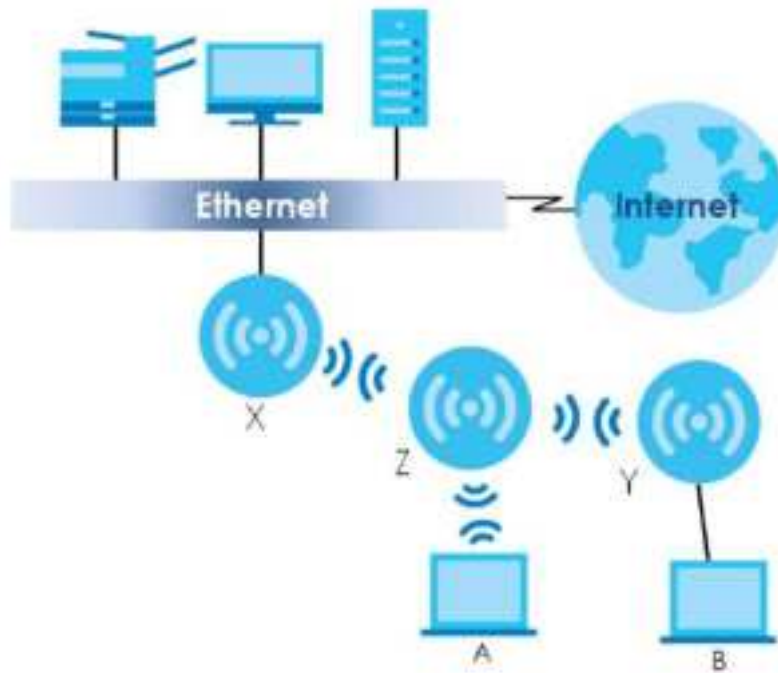
In Root AP mode, you can have multiple SSIDs active for regular WiFi connections and one SSID for the connection with a repeater (repeater SSID). WiFi clients can use either SSID to associate with the Zyxel Device in Root AP mode. A repeater must use the repeater SSID to connect to the Zyxel Device in Root AP mode.

When the Zyxel Device is in Root AP mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See [Section 10.2 on page 79](#) and [Section 13.2 on page 129](#) for more details.

Unless specified, the term “security settings” refers to the traffic between the WiFi clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

### 1.3.2 Wireless Repeater

Using Repeater mode, your Zyxel Device can extend the range of the WLAN. In the figure below, the Zyxel Device in Repeater mode (**Z**) has a wireless connection to the Zyxel Device in Root AP mode (**X**) which is connected to a wired network and also has a wireless connection to another Zyxel Device in Repeater mode (**Y**) at the same time. **Z** acts as a repeater that forwards traffic between associated WiFi clients and the wired LAN. **Y** acts as a wireless bridge (repeater with WDS wireless bridging enabled) that forwards traffic between wired clients and the wired LAN. Clients **A** and **B** access the AP and the wired network behind the AP through repeaters **Z** and **Y**.

**Figure 4** Repeater Application

When the Zyxel Device is in Repeater mode, repeater security between the Zyxel Device and other repeater is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See [Section 10.2 on page 79](#) and [Section 13.2 on page 129](#) for more details.

For NCC managed devices, you only need to enable **AP Smart Mesh** to automatically create wireless links between APs. See the NCC User's Guide for more details.

To set up a WDS in standalone mode APs, do the following steps. You should already have the root AP set up (see the Quick Start Guide for hardware connections).

- 1 Go to **Configuration > Object > WDS Profile** in your root AP Web Configurator and click **Add**.
- 2 Enter a profile name, a WDS SSID, and a pre-shared key.
- 3 Go to **Configuration > Wireless > AP Management**, select the **Radio WDS Profile** of the radio on which you are setting the WDS connection to use the WDS profile you set, and click **Apply**.
- 4 Do steps 1 and 3 for the wireless repeater using the same WDS SSID and pre-shared key.
- 5 Once the security settings of peer sides match one another, the connection between the root and repeater Zyxel Devices is made.

(Optional) If your Zyxel Device supports wireless bridging, you can extend a wired network from the port on the wireless repeater, do the following step:

- 6 Go to **Configuration > Wireless > AP Management**, select **Setup WDS Wireless Bridging** to enable wireless bridge on the wireless repeater.
- 7 Connect the client device to the Zyxel Device's port with an Ethernet cable.

Note: Make sure the VLAN settings on both the root AP and the wireless repeater are exactly the same so they can communicate.

Note: When wireless bridge is enabled, wireless interfaces for client devices will be disabled. You can only transmit data through the wireless repeater's ports.

Note: Frequency bands 5250-5350 MHz and 5470-5725 MHz are not supported in Repeater mode.

### 1.3.3 Radio Frequency (RF) Monitor

The Zyxel Device supports **Rogue AP Detection** (see [Section 10.3 on page 85](#)). **Rogue AP Detection** allows the Zyxel Device to be set to work as an RF monitor to discover nearby Access Points. The information it obtains from other APs is used to tag possible rogue APs and friendly APs. The Zyxel Device can still work as an AP while it scans the environment for wireless signals.

## 1.4 Sample Feature Applications

This section describes some possible scenarios and topologies that you can set up using your Zyxel Device.

### 1.4.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single WiFi network (usually an access point and one or more WiFi clients). The Service Set Identifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the Zyxel Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

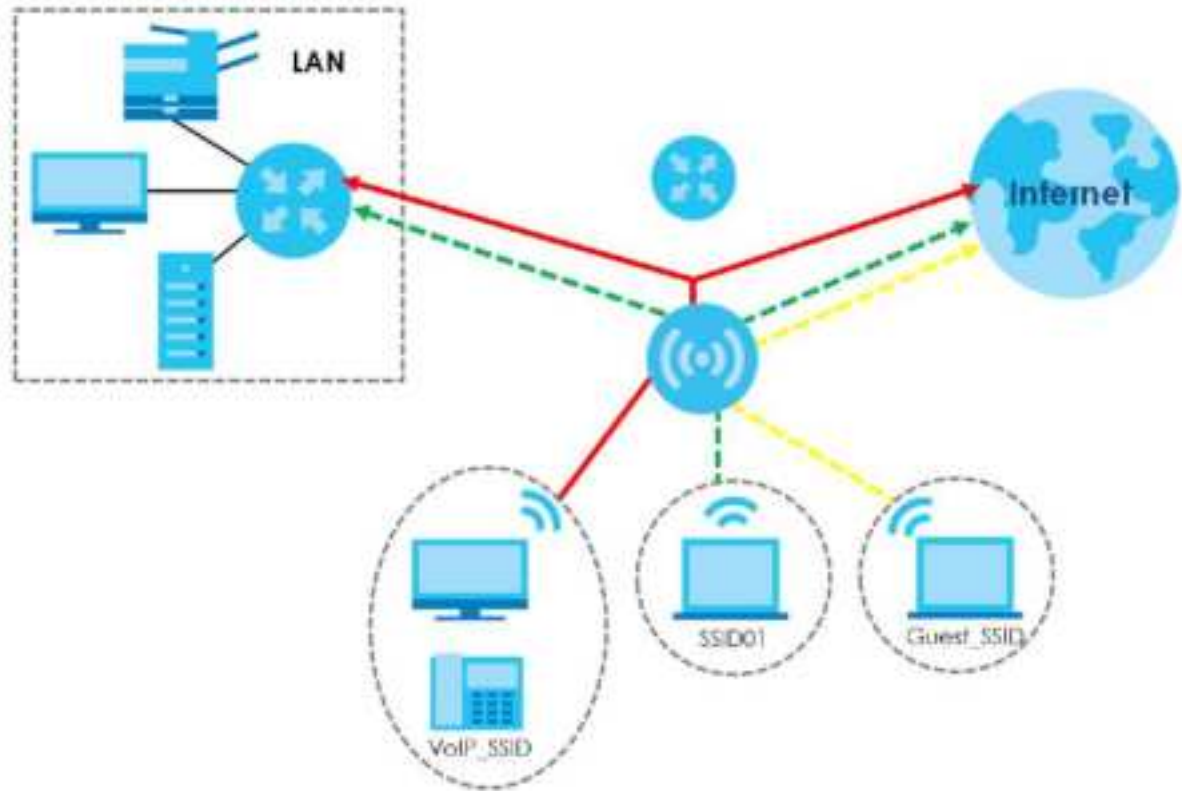
You can configure multiple SSID profiles, and have all of them active at any one time.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the WiFi clients in the network, each SSID appears to be a different access point. As in any WiFi network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a WiFi network in your office where Internet telephony (VoIP) users have priority. You also want a regular WiFi network for standard users, as well as a 'guest' WiFi network for visitors. In the following figure, **VoIP\_SSID** users have QoS priority, **SSID01** is the WiFi network for standard users, and **Guest\_SSID** is the WiFi network for guest users. In this example, the guest user is forbidden access to the wired Local Area Network (LAN) behind the AP and can access only the Internet.

**Figure 5** Multiple BSSs



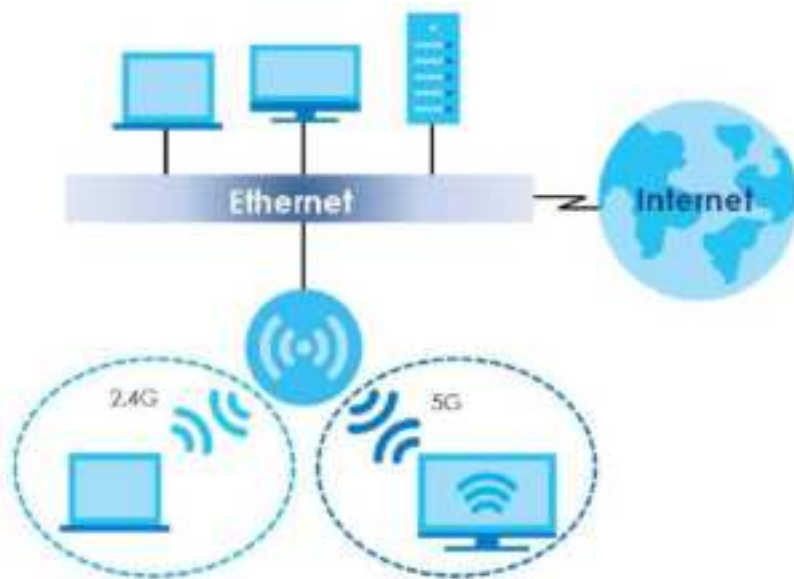
### 1.4.2 Dual-Radio

Some of the Zyxel Device models are equipped with dual WiFi radios. This means you can configure two different WiFi networks to operate simultaneously.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

**Figure 6** Dual-Radio Application



# CHAPTER 2

## AP Management

### 2.1 Management Mode

The Zyxel Device is a unified AP and can be managed by the NCC or work as a standalone device. We recommend you use NCC to manage multiple APs (see the NCC User's Guide).

Note: Not all models can be managed by NCC or an AC. See [Section 1.2 on page 12](#) to check whether your product supports these.

The following table shows the default IP addresses and firmware upload methods for different management modes.

Table 3 Zyxel Device Management Mode Comparison

MANAGEMENTMODE	DEFAULTIP ADDRESS	UPLOAD FIRMWARE VIA
Nebula Control Center	Dynamic	NCC Portal
Standalone	Dynamic or Static (192.168.1.2)	Built-in Web Configurator

When the Zyxel Device is in standalone mode and connects to a DHCP server, it uses the IP address assigned by the DHCP server. Otherwise, the Zyxel Device uses the default static management IP address (192.168.1.2). You can use the **NCC Discovery** screen to allow the Zyxel Device to be managed by the NCC.

When the Zyxel Device is managed by the NCC, it acts as a DHCP client and obtains an IP address from the NCC. It can be configured ONLY by the NCC. To change the Zyxel Device back to standalone mode, use the **Reset** button to restore the default configuration. Alternatively, you need to check the NCC for the Zyxel Device's IP address and use FTP to upload the default configuration file at conf/system-default.conf to the Zyxel Device and reboot the device.

#### 2.1.1 Standalone

When working in standalone mode, the Zyxel Device is configured mainly with its built-in Web Configurator. You can only connect to and set up one Zyxel Device at a time in this mode.

See [Chapter 5 on page 45](#) for detailed information about the standalone Web Configurator screens.

#### 2.1.2 Nebula Control Center

In this mode, which is also called cloud mode, you can manage and monitor the Zyxel Device through the Zyxel Nebula cloud-based network management system. This means you can manage devices remotely without the need of connecting to each device directly. It offers many features to better manage and monitor not just the Zyxel Device, but your network as a whole, including supported

switches and gateways. Your network can also be managed through your smartphone using the Nebula Mobile app. See [Section on page 191](#) for an example NCC managed network topology.

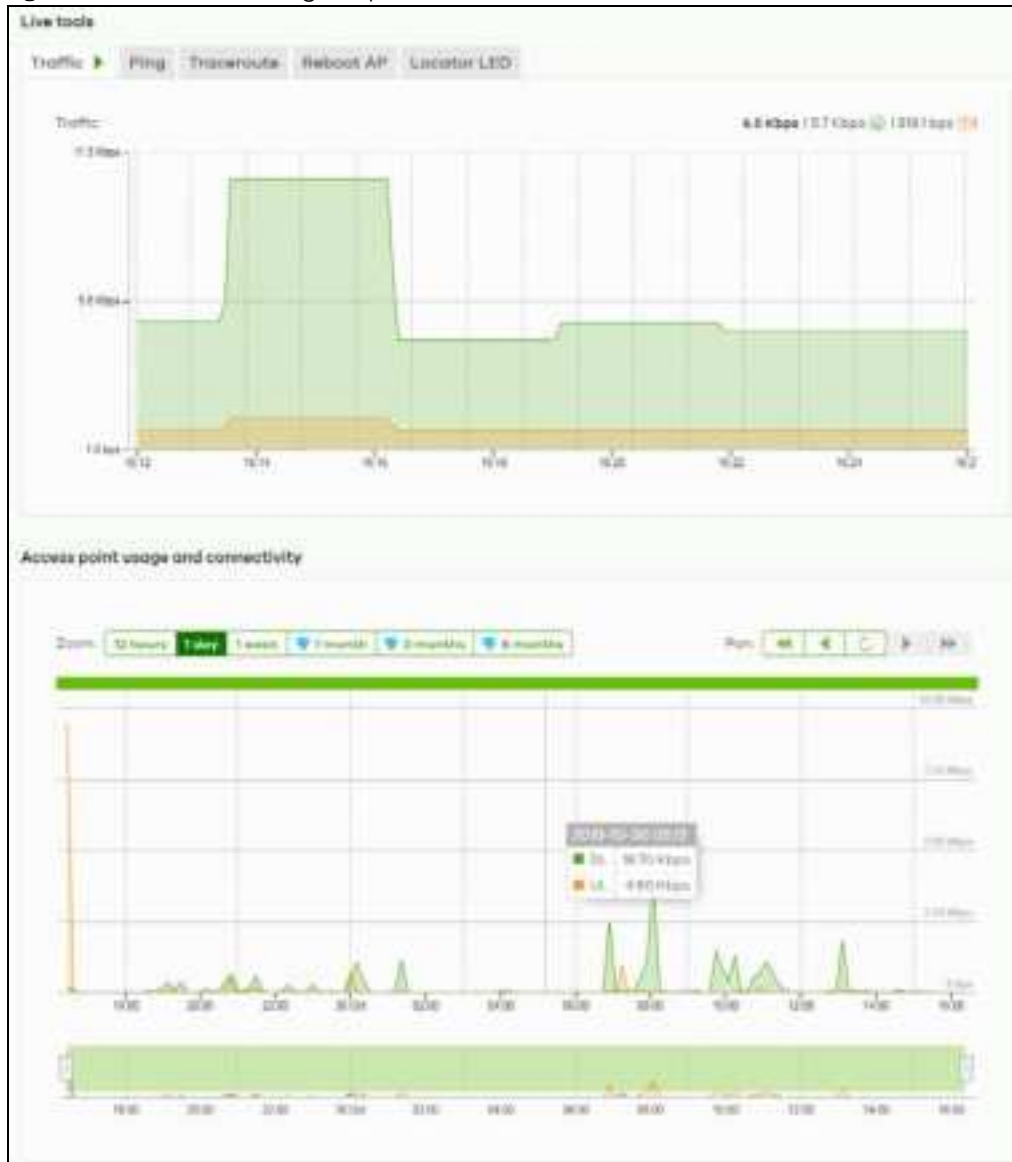
NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 4 NCC Management Levels

Organization			
Site A		Site B	
Device A-1	Device A-2	Device B-1	Device B-2

It graphically presents your device/network statistics and shows an overview of your network topology, as shown in the following figure. It also sends reports, alerts, and notifications for events, such as when a site goes offline.

**Figure 7** Traffic Monitoring Graph From NCC



See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See [Chapter 23 on page 194](#) if you want to change the Zyxel Device's VLAN setting or manually set its IP address.

Note: Make sure your network firewall allows TCP ports 443, 4335, and 6667 as well as UDP port 123 so the device can connect to and sync with the NCC.

## 2.2 Switching Management Modes

The Zyxel Device is in standalone mode by default, with NCC discovery enabled.

### Standalone-to-NCC

Register the Zyxel Device at the NCC website and then turn on the Zyxel Device. Make sure that **NCC Discovery** is enabled (see [Section 9.4 on page 76](#)). The NCC manages the Zyxel Device automatically when it is discovered. Settings on the Zyxel Device will be overwritten with what you have configured on the NCC website.

### NCC-to-Standalone

Unregister the Zyxel Device from the NCC organization/site. The Zyxel Device will automatically reset to its factory defaults and return to standalone mode.

## 2.3 Zyxel One Network (ZON) Utility

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be near it.

The ZON Utility issues requests via Zyxel Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at [www.zyxel.com](http://www.zyxel.com) and install it on your computer (Windows operating system).

### 2.3.1 Requirements

Before installing the ZON Utility on your PC, please make sure it meets the requirements listed below.

#### Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)



- Window 10 (both 32-bit / 64-bit versions)

Note: To check for your Windows operating system version, right-click on **My Computer > Properties** on your computer. You should see this information in the **General** tab.

Note: It is suggested that you install Npcap, the packet capture library for Windows operating systems, and remove WinPcap or any other installed packet capture tools before you install the ZON utility.

## Hardware

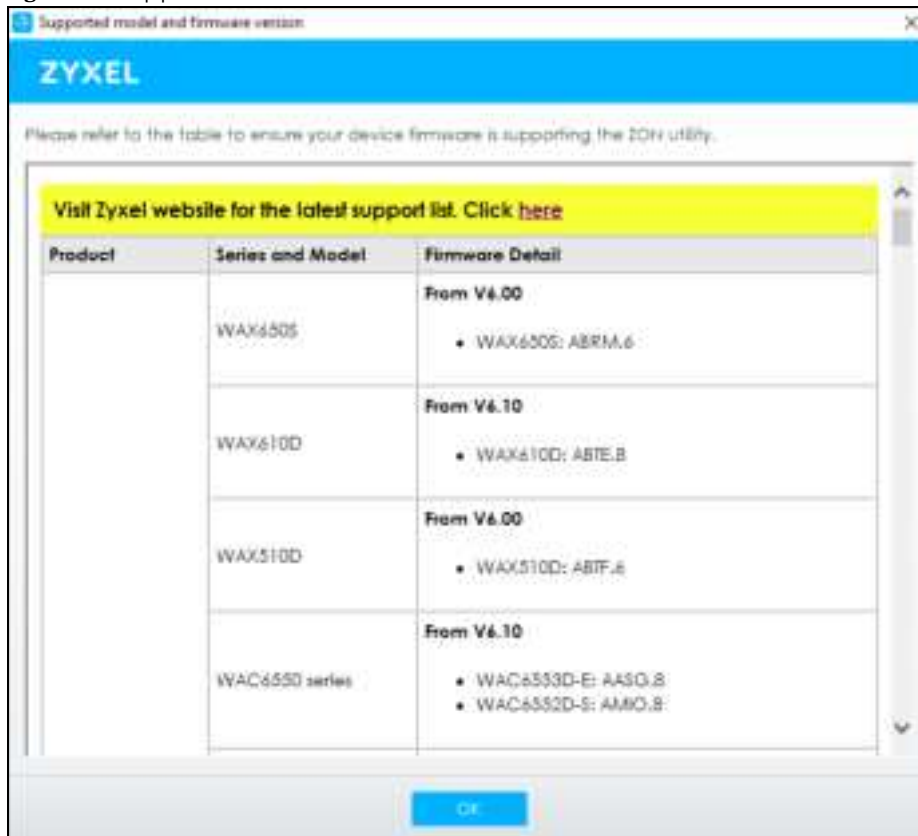
Here are the minimum hardware requirements to use the ZON Utility on your PC.

- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

### 2.3.2 Run the ZON Utility

- 1 Double-click the ZON Utility to run it.
- 2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

**Figure 8** Supported Devices and Versions



If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON Utility support. The release notes are in the firmware zip file on the Zyxel web site.

**Figure 9** ZON Utility Screen



- 3 Select a network adapter to which your supported devices are connected.

**Figure 10** Network Adapter



- 4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

**Figure 11** Discovery



- 5 The ZON Utility screen shows the devices discovered.

**Figure 12** ZON Utility Screen

- 6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

Note: You must know the selected device admin password before taking actions on the device using the ZON Utility icons.

**Figure 13** Password Prompt

The following table describes the icons numbered from left to right in the ZON Utility screen.

**Table 5** ZON Utility Icons

ICON	DESCRIPTION
1 IP Configuration	Change the selected device's IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations.
5 Locator LED	Use this icon to locate the selected device by causing its <b>Locator</b> LED to blink.
6 Web GUI	Use this to access the selected device Web Configurator from your browser. You will need a username and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance.
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.

Table 5 ZON Utility Icons (continued)

ICON	DESCRIPTION
9 Configure NCC Discovery	The option is available if the selected device supports Nebula Control Center (NCC) discovery. You must have Internet access to use this feature. Use this icon on the selected device to enable or disable the Nebula Control Center (NCC) discovery feature.  If the feature is enabled, the selected device will try to connect to the NCC. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the Nebula cloud mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 6 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support <b>IP Configuration</b> , <b>Renew IP address</b> and <b>Flash Locator LED</b> , this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.
NCC Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature.  If the feature is enabled, the selected device will try to connect to the NCC. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the Nebula cloud mode.
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.
IPv6 Address	This field displays the IPv6 address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.

## 2.4 Ways to Access the Zyxel Device

You can use the following ways to configure the Zyxel Device.

### **Web Configurator**

The Web Configurator allows easy Zyxel Device setup and management using an Internet browser. If your Zyxel Device is managed by the NCC or an AC, use this only for troubleshooting if you cannot connect to the Internet. This User's Guide provides information about the Web Configurator.

### **NCC**

This is the primary means by which you manage the Zyxel Device in cloud (NCC) mode. With the NCC, you can remotely manage and monitor the Zyxel Device through a cloud-based network management system. See the NCC User's Guide for more information.

### **ZON Utility**

Zyxel One Network (ZON) Utility is a utility tool that assists you to set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at [www.zyxel.com](http://www.zyxel.com) and install it on your computer (Windows operating system). For more information on ZON Utility see [Section 2.3 on page 24](#).

### **Command-Line Interface (CLI)**

The CLI allows you to use text-based commands to configure the Zyxel Device. You can access it using remote management (SSH) or via the console port. See the Command Reference Guide for more information.

### **File Transfer Protocol (FTP)**

This protocol can be used for firmware upgrades and configuration backup and restore.

## **2.5 Good Habits for Managing the Zyxel Device**

Do the following things regularly to make the Zyxel Device 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 Zyxel Device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you will not have to totally re-configure the Zyxel Device; you can simply restore your last configuration.

# CHAPTER 3

## Hardware

See the Quick Start Guide for hardware installation and connections.

### 3.1 Zyxel Device Single LED

The LED of the Zyxel Device can be controlled by using the suppression feature such that the LEDs stay lit (ON) or OFF after the Zyxel Device is ready. Refer to [Chapter 19 on page 185](#) for the LED **Suppression** and **Locator** menus in standalone mode.











#### 3.1.1 Zyxel Device LED

**Figure 14** NWA50AX/NWA90AX/NWA50AX PRO/NWA90AX PRO LED



The following are the LED descriptions for the Zyxel Device.

Table 7 Zyxel Device LED

COLOR		STATUS	DESCRIPTION
	Amber	Blinks between amber and green alternately (300ms interval).	The Zyxel Device is booting up or is connecting with NCC.
	Green		
	Amber	Blinks between amber and green alternately 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC or an AC.
	Green		
	Amber	Blinks between amber and green alternately 2 times and then turns solid green for 3 seconds.	The Zyxel Device is managed by an AC but the uplink is disconnected.
	Green		
	Green	Slow Blinking (On for 1 second, Off for 1 second)	The wireless module of the Zyxel Device is disabled or fails, the Zyxel Device is using default WiFi settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC.
	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or WiFi clients are connected to the Zyxel Device.
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no WiFi clients connected.
	Blue	Slow Blinking (Blink for 1 time, Off for 1 second)	The Zyxel Device is performing a Channel Availability Check (CAC) with Dynamic Frequency Selection (DFS) to monitor a channel for radar signals.
	Red	On	The Zyxel Device failed to boot up or is experiencing system failure.
		Fast Blinking (On for 50 milliseconds, Off for 50 milliseconds)	The Zyxel Device is undergoing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3 seconds)	The Uplink port of the Zyxel Device in standalone mode is disconnected.

**Figure 15** NWA55AXE



Note: The NWA55AXE does not have LEDs.



# CHAPTER 4

## Web Configurator

### 4.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management via internet browser. Use a browser that supports HTML5, such Mozilla Firefox, or Google Chrome, Microsoft Edge. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

### 4.2 Accessing the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected, and your computer is connected to the Zyxel Device through wired or WiFi connection. See the Quick Start Guide.
- 2 If the Zyxel Device and your computer are not connected to a DHCP server, make sure your computer's IP address is in the range between "192.168.1.3" and "192.168.1.254".
- 3 Browse to the Zyxel Device's DHCP-assigned IP address or <http://192.168.1.2>. The **Login** screen appears. If you are in cloud mode, check the NCC's **Access Point > Monitor > Access Points** screen for the Zyxel Device's LAN IP address.

**Figure 16** Login Page

If a Zyxel Device is in standalone mode and supports NCC, the following page displays.

Here, you can watch a tutorial for using the Zyxel Nebula Control Center (NCC) or access the link to the NCC, as shown in the following figure. Otherwise, continue with the next step. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Zyxel Device (see [Section 2.1.2 on page 22](#))

**Figure 17** Nebula Intro Page

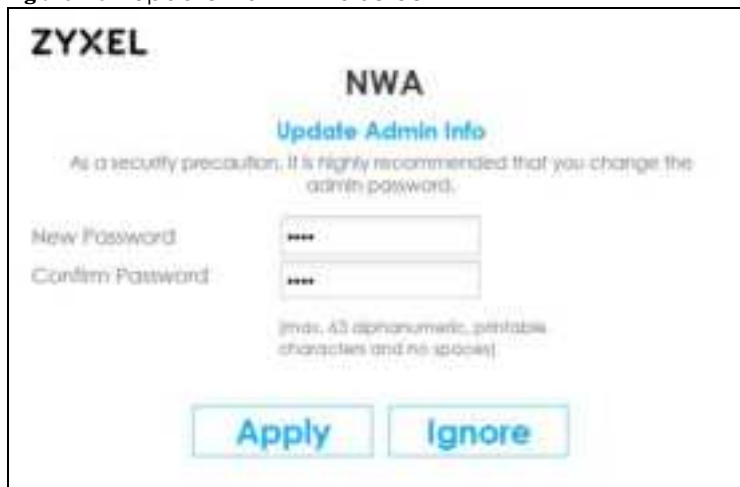
To go to the login page, click **Standalone Mode**. Login page displays as shown in the following figure.

**Figure 18** Login Page in Standalone Mode

- 4 Enter the user name (default: "admin") and password (default: "1234").

Note: If the Zyxel Device is being managed or has been managed by the NCC, check **Local credentials** in the NCC's **Site-Wide > Configure > General settings** screen for the Zyxel Device's current password.

- 5 Select the language you prefer for the Web Configurator. Click **Login**.
- 6 The wizard screen opens when the Zyxel Device is accessed for the first time or when you reset the Zyxel Device to its default factory settings.
- 7 If you logged in using the default user name and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.

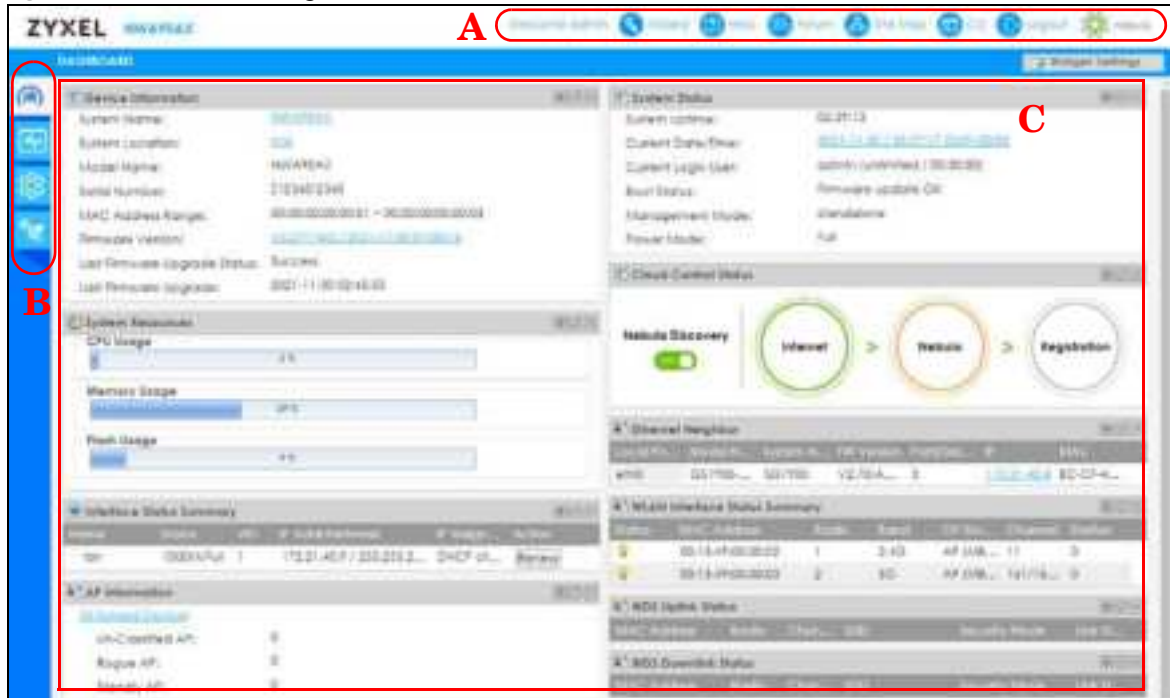
**Figure 19** Update Admin Info Screen

The **Update Admin Info** screen appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

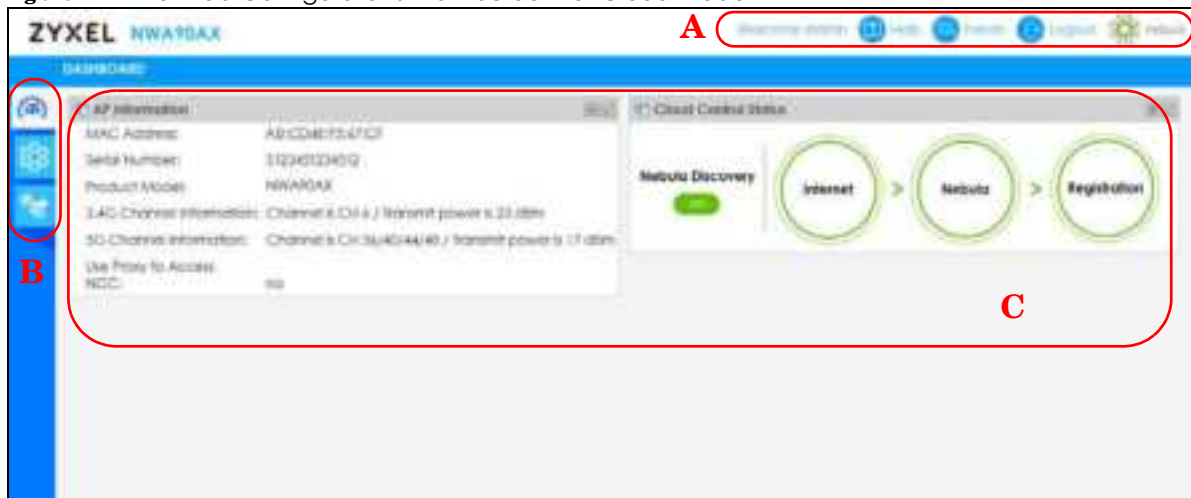
## 4.3 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Dashboard** screen. The following figures show the **Dashboard** screen for standalone mode and for cloud (NCC) mode. The screen is different for standalone mode and cloud (NCC) mode and may vary slightly for different models.

**Figure 20** The Web Configurator's Main Screen for Standalone Mode



**Figure 21** The Web Configurator's Main Screen for Cloud Mode



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

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

### 4.3.1 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. If your Zyxel Device is in NCC mode, not all icons will be available in the Title Bar.

**Figure 22** Title Bar



The icons provide the following functions.

**Table 8** Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See <a href="#">Chapter 7 on page 63</a> for more information.
Help	Click this to open the help page for the current screen.
Community	Click this to log into the Zyxel forum to post questions, contribute to a discussion and get feedback on Zyxel Device.
Site Map	Click this to see an overview of links to the Web Configurator screens.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator.
Logout	Click this to log out of the Web Configurator.
nebula	Click this to open the NCC web site login page in a new tab or window.

### Site Map

Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

**Figure 23** Site Map



## CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

**Figure 24** CLI Messages



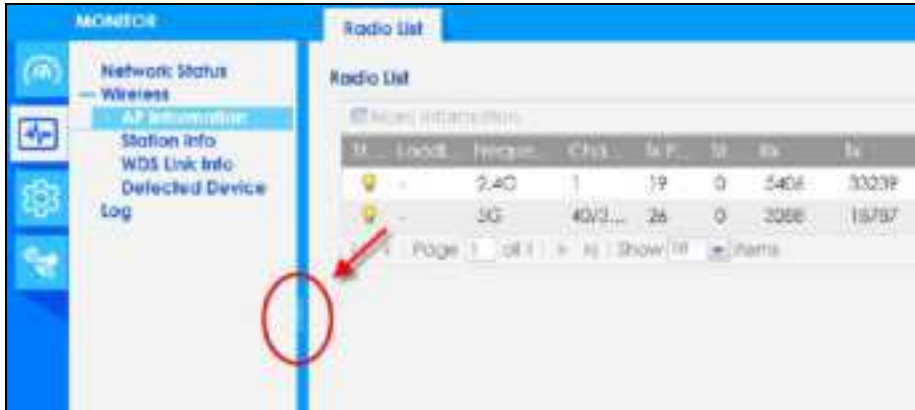
Click **Clear** to remove the currently displayed information.

Note: See the Command Reference Guide for information about the commands.

## 4.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features. Click the arrow in the middle of the right edge of the navigation panel to hide the navigation panel menus or drag it to resize them. The following sections introduce the Zyxel Device's navigation panel menus and their screens.

**Figure 25** Navigation Panel



## 4.3.3 Standalone Mode Navigation Panel Menus

The following are the screens available in standalone mode. Note that some screens may not be available for your Zyxel Device model. See [Section 1.2 on page 12](#) to see which features your Zyxel Device model supports.

## Dashboard

The dashboard displays information such as general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see [Chapter 6 on page 47](#).

## Monitor Menu

The monitor menu screens display status and statistics information.

Table 9 Monitor Menu Screens Summary

FO I D E R O R L I N K	T A B	F U N C T I O N
Network Status	Network Status	Display general LAN interface information and packet statistics.
Wireless		
AP Information	Radio List	Display information about the radios of the connected APs.
Station Info	Station List	Display information about the connected stations.
WDS Link Info	WDS Link Info	Display statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
Detected Device	Detected Device	Display information about suspected rogue APs.
Log	View Log	Display log entries for the Zyxel Device.

## Configuration Menu

Use the configuration menu screens to configure the Zyxel Device's features.

Table 10 Configuration Menu Screens Summary

FO I D E R O R L I N K	T A B	F U N C T I O N
Network	IP Setting	Configure the IP address for the Zyxel Device Ethernet interface.
	VLAN	Manage the Ethernet interface VLAN settings.
	NCC Discovery	Configure proxy server settings to access the NCC.
Wireless		
AP Management	WLAN Setting	Manage the Zyxel Device's general WiFi settings.
Rogue AP	Rogue/Friendly AP List	Configure how the Zyxel Device monitors for rogue APs.
DCS	DCS	Configure dynamic WiFi channel selection.
Object		
User	User	Create and manage users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
AP Profile	Radio	Create and manage WiFi radio settings files that can be associated with different APs.
	SSID	Create and manage WiFi SSID, security, MAC filtering, and layer-2 isolation files that can be associated with different APs.
WDS Profile	WDS	Create and manage WDS profiles that can be used to connect to different APs in WDS.

Table 10 Configuration Menu Screens Summary (continued)

FOIDER OR LINK	TAB	FUNCTION
Certificate	My Certificates	Create and manage the Zyxel Device's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
System		
Host Name	Host Name	Configure the system and domain name for the Zyxel Device.
Date/Time	Date/Time	Configure the current date, time, and time zone in the Zyxel Device.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
SSH	SSH	Configure SSH server and SSH service settings.
FTP	FTP	Configure FTP server settings.
Log & Report		
Log Setting	Log Setting	Configure the system log and remote syslog servers.

## Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the Zyxel Device.

Table 11 Maintenance Menu Screens Summary

FOIDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the Zyxel Device.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information.
	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
LEDs	Suppression	Enable this feature to keep the LEDs off after the Zyxel Device starts.
	Locator	Enable this feature to see the actual location of the Zyxel Device between several devices in the network.
Reboot	Reboot	Restart the Zyxel Device.
Shutdown	Shutdown	Turn off the Zyxel Device.

### 4.3.4 Cloud Mode Navigation Panel Menus

If your Zyxel Device is in cloud (NCC) mode, you only need to use the Web Configurator for troubleshooting if your Zyxel Device cannot connect to the Internet.

## Dashboard

The dashboard displays general Zyxel Device information, and AP information in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see [Chapter 22 on page 192](#).



## Configuration Menu

Use the configuration menu screens to configure the Zyxel Device's features.

Table 12 Configuration Menu Screens Summary

FOlder oR LINK	TAB	FUNCTION
Network	IP Setting	Configure the IP address for the Zyxel Device Ethernet interface.
	VLAN	Manage the Ethernet interface VLAN settings.

## Maintenance Menu

Use the maintenance menu screens to configure the Zyxel Device's features.

Table 13 Maintenance Menu Screens Summary

FOlder oR LINK	TAB	FUNCTION
Shell Script	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information.
	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
Log	View Log	Displays the log when the Zyxel Device is not connected to the Nebula.

## 4.3.5 Tables and Lists

The Web Configurator tables and lists are quite flexible and provide several options for how to display their entries.

### 4.3.5.1 Manipulating Table Display

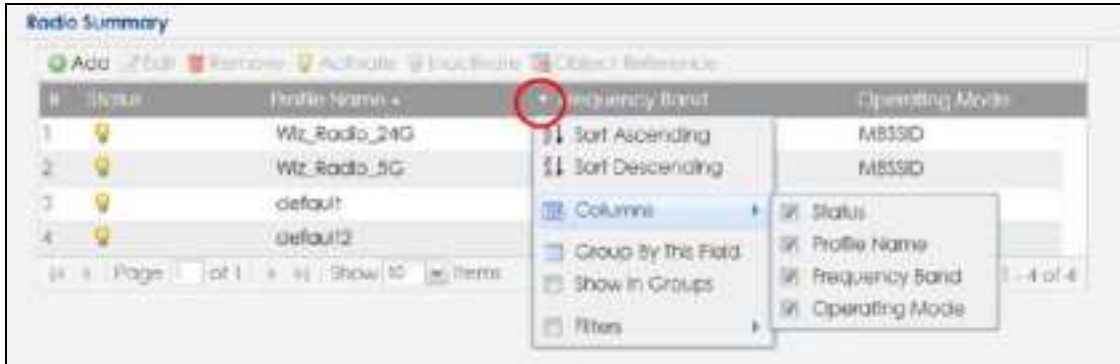
Here are some of the ways you can manipulate the Web Configurator tables.

- 1 Click a column heading to sort the table's entries according to that column's criteria.

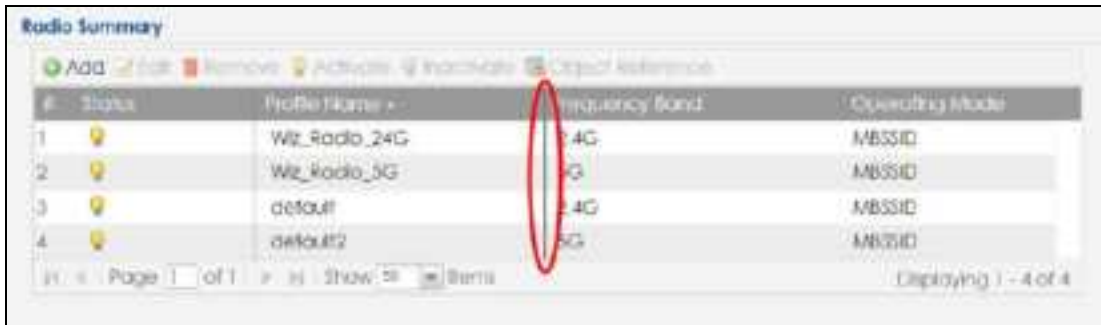


- 2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:
  - Sort in ascending alphabetical order
  - Sort in descending (reverse) alphabetical order
  - Select which columns to display
  - Group entries by field

- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text.



- 3 Select a column heading cell's right border and drag to re-size the column.



- 4 Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.



- 5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.



### 4.3.5.2 Working with Table Entries

The tables have icons for working with table entries. A sample is shown next. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

**Figure 26** Common Table Icons



Here are descriptions for the most common table icons.

**Table 14** Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click <b>Add</b> to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click <b>Remove</b> . The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click <b>Activate</b> .
Inactivate	To turn off an entry, select it and click <b>Inactivate</b> .
Object Reference	Select an entry and click <b>Object Reference</b> to open a screen that shows which settings use the entry.

---

# **PART I**

## **Standalone Configuration**

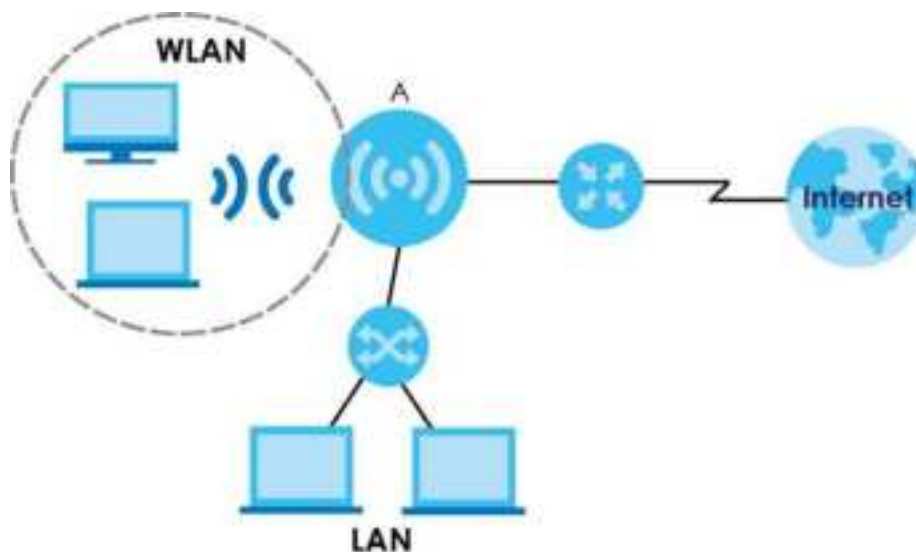
---

# CHAPTER 5

## Standalone Configuration

### 5.1 Overview

The Zyxel Device is in standalone mode by default. Use the web configurator to manage and configure the Zyxel Device directly. As shown in the following figure, WiFi clients can connect to the Zyxel Device (A) to access network resources.



### 5.2 Starting and Stopping the Zyxel Device

Here are some of the ways to start and stop the Zyxel Device.

**Always use Maintenance > Shutdown or the shutdown command before you turn off the Zyxel Device or remove the power. Not doing so can cause the firmware to become corrupt.**

Table 15 Starting and Stopping the Zyxel Device

METHOD	DESCRIPTION
Turning on the power	A cold start occurs when you turn on the power to the Zyxel Device. The Zyxel Device powers up, checks the hardware, and starts the system processes.
Rebooting the Zyxel Device	A warm start (without powering down and powering up again) occurs when you use the <b>Reboot</b> button in the <b>Reboot</b> screen or when you use the <code>reboot</code> command. The Zyxel Device writes all cached data to the local storage, stops the system processes, and then does a warm start.

Table 15 Starting and Stopping the Zyxel Device (continued)

METHOD	DESCRIPTION
Using the <b>RESET</b> button	<p>If you press the <b>RESET</b> button on the back of the Zyxel Device, the Zyxel Device sets the configuration to its default values and then reboots. See <a href="#">Section 25.6 on page 210</a> for more information.</p> <p>Note: Some models do not have a <b>RESET</b> button due to feature differences.</p>
Clicking <b>Maintenance &gt; Shutdown &gt; Shutdown</b> or using the <code>shutdown</code> command	Clicking <b>Maintenance &gt; Shutdown &gt; Shutdown</b> or using the <code>shutdown</code> command writes all cached data to the local storage and stops the system processes. Wait for the Zyxel Device to shut down and then manually turn off or remove the power. It does not turn off the power.
Disconnecting the power	Power off occurs when you turn off the power to the Zyxel Device. The Zyxel Device simply turns off. It does not stop the system processes or write cached data to local storage.

The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

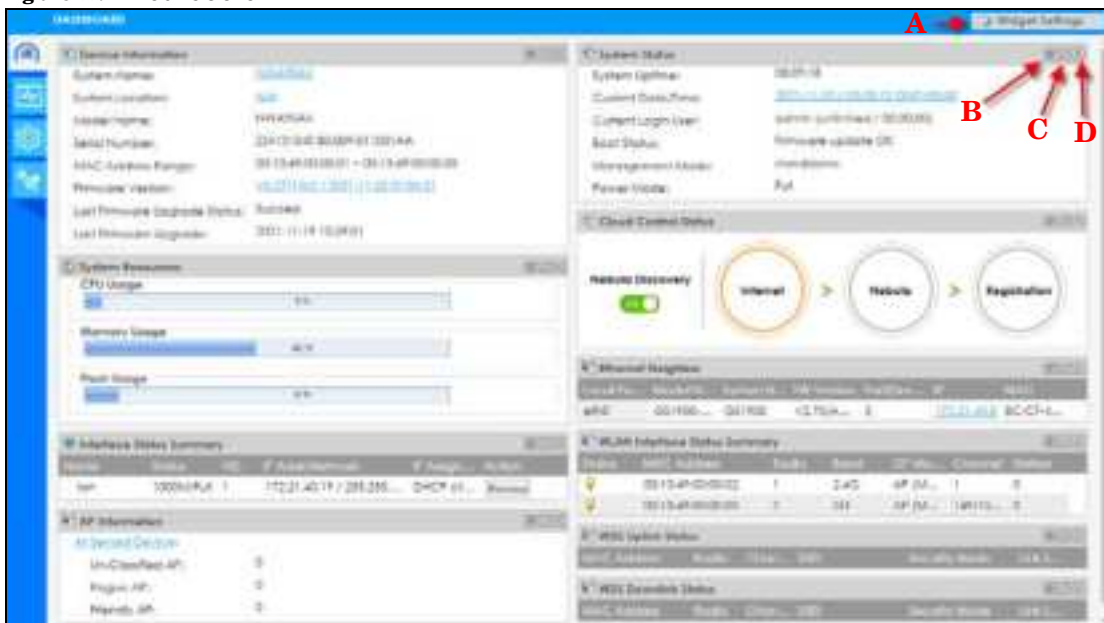
# CHAPTER 6

## Dashboard

### 6.1 Overview

This screen displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets. Fields in this screen may slightly differ by models.

**Figure 27** Dashboard



The following table describes the labels in this screen.

**Table 16** Dashboard

IA BEL	DESC RITION
Widget Settings (A)	Use this link to re-open closed widgets. Widgets that are already open appear grayed out.
Refresh Time Setting (B)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (C)	Click this to update the widget's information immediately.
Close Widget (D)	Click this to close the widget. Use <b>Widget Settings</b> to re-open it.
Device Information	
System Name	This field displays the name used to identify the Zyxel Device on any network. Click the icon to open the screen where you can change it.
System Location	This field displays the location of the Zyxel Device. Click the icon to open the screen where you can change it.
Model Name	This field displays the model name of this Zyxel Device.
Serial Number	This field displays the serial number of this Zyxel Device.

Table 16 Dashboard (continued)

Label	Description
MAC Address Range	This field displays the MAC addresses used by the Zyxel Device. Each physical port or WiFi radio has one MAC address. The first MAC address is assigned to the Ethernet LAN port, the second MAC address is assigned to the first radio, and so on.
Firmware Version	This field displays the version number and date of the firmware the Zyxel Device is currently running. Click the icon to open the screen where you can upload firmware.
Last Firmware Upgrade Status	This field displays whether the latest firmware update was successfully completed.
Last Firmware Upgrade	This field displays the date and time when the last firmware update was made.
System Resources	
CPU Usage	This field displays what percentage of the Zyxel Device's processing capability is currently being used. Hover your cursor over this field to display the <b>Show CPU Usage</b> icon that takes you to a chart of the Zyxel Device's recent CPU usage.
Memory Usage	This field displays what percentage of the Zyxel Device's RAM is currently being used. Hover your cursor over this field to display the <b>Show Memory Usage</b> icon that takes you to a chart of the Zyxel Device's recent memory usage.
Flash Usage	This field displays what percentage of the Zyxel Device's onboard flash memory is currently being used.
Ethernet Neighbor	
Local Port (Description)	This field displays the port of the Zyxel Device, on which the neighboring device is discovered.
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
FW Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the discovered device's port which is connected to the Zyxel Device.
IP	This field displays the IP address of the discovered device. Click the IP address to access and manage the discovered device using its Web Configurator.
MAC	This field displays the MAC address of the discovered device.
WDS (Wireless Distribution System) Uplink/Downlink Status	
MAC Address	This field displays the MAC address of the root AP or repeater to which the Zyxel Device is connected using WDS.
Radio	This field displays the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS.
Channel	This field displays the channel number on the root AP or repeater to which the Zyxel Device is connected using WDS.
SSID	This field displays the name of the WiFi network to which the Zyxel Device is connected using WDS.
Security Mode	This field displays which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS.
Link Status	This field displays the RSSI (Received Signal Strength Indicator) and transmission/reception rate of the wireless connection in WDS.
System Status	
System Uptime	This field displays how long the Zyxel Device has been running since it last restarted or was turned on.
Current Date/Time	This field displays the current date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.



Table 16 Dashboard (continued)

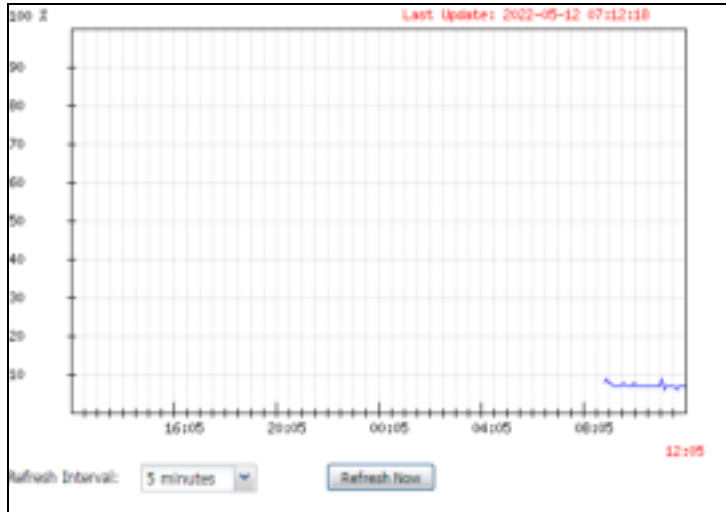
LABEL	DESCRIPTION
Boot Status	<p>This field displays details about the Zyxel Device's startup state.</p> <p><b>OK</b> - The Zyxel Device started up successfully.</p> <p><b>Firmware update OK</b> - A firmware update was successful.</p> <p><b>Problematic configuration after firmware update</b> - The application of the configuration failed after a firmware upgrade.</p> <p><b>System default configuration</b> - The Zyxel Device successfully applied the system default configuration. This occurs when the Zyxel Device starts for the first time or you intentionally reset the Zyxel Device to the system default settings.</p> <p><b>Fallback to lastgood configuration</b> - The Zyxel Device was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file.</p> <p><b>Fallback to system default configuration</b> - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf).</p> <p><b>Booting in progress</b> - The Zyxel Device is still applying the system configuration.</p>
Management Mode	<p>This shows whether the Zyxel Device is set to work as a stand alone AP.</p>
Cloud Control Status	<p>This field displays:</p> <ul style="list-style-type: none"> <li>• The Zyxel Device Internet connection status.</li> <li>• The connection status between the Zyxel Device and NCC.</li> <li>• The Zyxel Device registration status on NCC.</li> </ul> <p>Mouse over the circles to display detailed information.</p> <p>To pass your Zyxel Device management to NCC, first make sure your Zyxel Device is connected to the Internet. Then go to NCC and register your Zyxel Device. You can also view this information in <b>Configuration &gt; Network &gt; NCC Discovery</b>.</p> <p><b>1. Internet</b></p> <p>Green - The Zyxel Device is connected to the Internet.</p> <p>Orange - The Zyxel Device is not connected to the Internet.</p> <p><b>2. Nebula</b></p> <p>Green - The Zyxel Device is connected to NCC.</p> <p>Orange - The Zyxel Device is not connected to NCC.</p> <p><b>3. Registration</b></p> <p>Green - The Zyxel Device is registered on NCC.</p> <p>Gray - The Zyxel Device is not registered on NCC.</p> <p>Note: All circles will gray out if you disable <b>Nebula Discovery</b>.</p>
Nebula Discovery	<p>Slide the switch to the right to enable NCC discovery on the Zyxel Device. The Zyxel Device will connect to NCC and change to the NCC management mode if it:</p> <ul style="list-style-type: none"> <li>• is connected to the Internet.</li> <li>• has been registered on NCC.</li> </ul>
Interface Status Summary	<p>If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the <b>Detail</b> icon to go to a (more detailed) summary screen of interface statistics.</p>
Name	<p>This field displays the name of each interface.</p>

Table 16 Dashboard (continued)

LABEL	DESCRIPTION
Status	<p>This field displays the current status of each interface. The possible values depend on what type of interface it is.</p> <p><b>Inactive</b> - The Ethernet interface is disabled.</p> <p><b>Down</b> - The Ethernet interface is enabled but not connected.</p> <p><b>Speed / Duplex</b> - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (<b>Full</b> or <b>Half</b>).</p>
VID	This field displays the VLAN ID to which the interface belongs.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.
IP Assignment	<p>This field displays how the interface gets its IP address.</p> <p><b>Static</b> - This interface has a static IP address.</p> <p><b>DHCP Client</b> - This interface gets its IP address from a DHCP server.</p>
Action	<p>If the interface has a static IP address, this shows <b>n/a</b>.</p> <p>If the interface has a dynamic IP address, use this field to get or to update the IP address for the interface. Click <b>Renew</b> to send a new DHCP request to a DHCP server.</p>
WLAN Interface Status Summary	This displays status information for the WLAN interface.
Status	This displays whether or not the WLAN interface is activated.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the Zyxel Device.
Band	This indicates the WiFi frequency band currently being used by the radio.
OP Mode	This indicates the radio's operating mode. Operating modes are <b>AP (MBSSID)</b> , <b>Root AP</b> or <b>Repeater</b> .
Channel	This indicates the channel number the radio is using.
Station	This displays the number of WiFi clients connected to the Zyxel Device.
AP Information	This shows a summary of connected wireless Access Points (APs).
All Sensed Device	This sections displays a summary of all wireless devices detected by the network. Click the link to go to the <b>Monitor &gt; Wireless &gt; Detected Device</b> screen.
Un-Classified AP	This displays the number of detected unclassified APs.
Rogue AP	This displays the number of detected rogue APs.
Friendly AP	This displays the number of detected friendly APs.

### 6.1.1 CPU Usage

Use this screen to look at a chart of the Zyxel Device's recent CPU usage. To access this screen, click **CPU Usage** in the dashboard.

**Figure 28** Dashboard > CPU Usage

The following table describes the labels in this screen.

**Table 17** Dashboard > CPU Usage

LABEL	DESCRIPTION
%	The y-axis represents the percentage of CPU usage.
time	The x-axis shows the time period over which the CPU usage occurred.
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

## 6.1.2 Memory Usage

Use this screen to look at a chart of the Zyxel Device's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the dashboard.

**Figure 29** Dashboard > Memory Usage

The following table describes the labels in this screen.

Table 18 Dashboard > Memory Usage

<b>LABEL</b>	<b>DESCRIPTION</b>
%	The y-axis represents the percentage of RAM usage.
time	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

# CHAPTER 7

## Setup Wizard

### 7.1 Accessing the Wizard

When you log into the Web Configurator for the first time or when you reset the Zyxel Device to its default configuration, the wizard screen displays.

Note: If you have already configured the wizard screens and want to open it again, click the **Wizard** icon on the upper right corner of any Web Configurator screen.

### 7.2 Using the Wizard

This wizard helps you configure the Zyxel Device IP address, change time zone, daylight saving and radio settings, and edit an SSID profile to change general WiFi and WiFi security settings.

#### 7.2.1 Step 1 Time Settings

Use this screen to configure the Zyxel Device's country code, time zone and daylight saving time.

- **Country:** Select the country where the Zyxel Device is located.

Note: The **Country** field is not available and you cannot change the country code if the Zyxel Device products comply with the U.S. laws, policies and regulations and are to be sold to the U.S. market.

- **Time Zone:** Select the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
- **Enable Daylight Saving:** Select the option if you use Daylight Saving Time. Configure the day and time when Daylight Saving Time starts and ends.
- **Offset** allows you to specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments).

Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

**Figure 30** Wizard: Time Settings

### 7.2.2 Step 2 Password and Uplink Connection

Use this screen to configure the Zyxel Device's system password and IP address.

**Change Password:** Enter a new password and retype it to confirm.

**Uplink Connection:** Select **Auto (DHCP)** if the Zyxel Device is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Zyxel Device in order to access the Zyxel Device's Web Configurator again.

Otherwise, select **Static IP** when the Zyxel Device is NOT connected to a router or you want to assign it a fixed IP address. You will need to manually enter:

- the Zyxel Device's IP address and subnet mask.
- the IP address of the router that helps forward traffic.
- a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

Note: The number of characters shown is not an actual representation of your current password. If you click **Next** without changing password in the **New Password** and **Confirm Password** fields, your current password will not be changed.

**Figure 31** Wizard: Change Password and Uplink Connection

The screenshot shows the 'Wizard Setting' window with 'Step 2' selected. The 'Change Password' section has two password fields, both containing six asterisks. The 'Uplink Connection' section has two radio buttons: 'Auto(DHCP)' and 'Static IP'. The 'Static IP' option is selected. Below it are four input fields for 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS Server', each containing four zeros. At the bottom right are 'Prev', 'Next', and 'Cancel' buttons.

### 7.2.3 Step 3 Radio

Use this screen to configure the Zyxel Device's radio transmitter(s).

- **Channel Selection:** Select **Auto** to have the Zyxel Device automatically choose a radio channel that has least interference. Otherwise, select **Manual** and specify a channel the Zyxel Device will use in the 2.4 GHz or 5 GHz wireless LAN. The options vary depending on the frequency band and the country you are in.
- **Maximum Output Power:** Enter the maximum output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs.

Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

**Figure 32** Wizard: Radio

The screenshot shows the 'Wizard setting' window with 'Step 3' selected. It displays two radio configuration sections. The top section is for 2.4GHz, with 'Channel Width' set to 20MHz and 'Channel Selection' set to 'Auto'. The 'Maximum Output Power' is set to 30 dBm(0-30). The bottom section is for 5GHz, with 'Channel Width' set to 20/40/80MHz and 'Channel Selection' set to 'Auto'. The 'Maximum Output Power' is also set to 30 dBm(0-30). At the bottom right are 'Prev', 'Next', and 'Cancel' buttons.

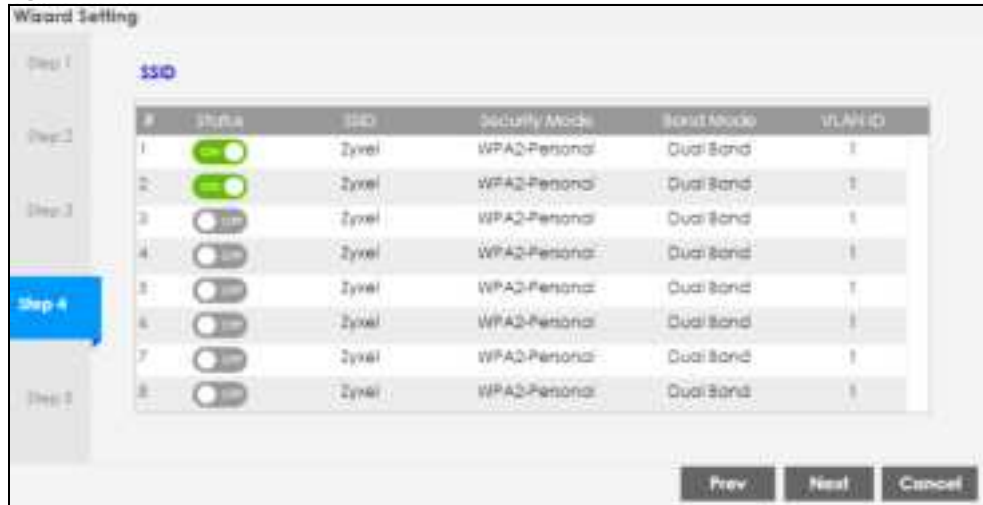
## 7.2.4 Step 4 SSID

Use this screen to enable, disable or edit an SSID profile.

Select an SSID profile and click the **Status** switch to turn it on or off. To change an SSID profile's settings, such as the SSID (WiFi network name) and WiFi password, double-click the SSID profile entry from the list. See [Section 7.2.4.1 on page 56](#) for more information.

Note: You cannot add or remove an SSID profile after running the setup wizard.

**Figure 33** Wizard: SSID



### 7.2.4.1 Edit SSID Profile

Use this screen to configure an SSID profile.

The screen varies depending on the security type you selected.

- **SSID**: Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- **VLAN ID**: Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.  
**Band Mode**: Select the WiFi band which this profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n WiFi clients. 5 GHz is the frequency used by IEEE 802.11ac/a/n WiFi clients.
- **Security Type**: Select **WPA2** to add security on this WiFi network. Otherwise, select **OPEN** to allow any WiFi client to associate this network without authentication.
- **Personal**: If you set **Security Type** to **WPA2** and select **Personal**, enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
- **Enterprise**: Select this option and the **Primary / Secondary RADIUS Server** check box to have the Zyxel Device use the specified RADIUS server. You have to enter the IP address, port number and shared secret password of the RADIUS server to be used for authentication.

Note: Not all Zyxel Devices support the enterprise authentication settings; see [Table 1 on page 12](#) for more information.

Click **OK** to proceed. Click **Cancel** to close the screen without saving.



**Figure 34** Wizard: SSID: Edit (WPA2-Personal)

The 'Edit SSID Profile' dialog box shows the following configuration:

- SSID: Zyxel
- Status: Active
- VLAN ID: 1 (range 1-4094)
- Band Mode: 2.4G
- Security Type: WPA2
- Personal: ☒ (selected)
- Secret: 12345678
- Enterprise: ☐

Buttons: OK, Cancel

**Figure 35** Wizard: SSID: Edit (WPA2-Enterprise)

The 'Edit SSID Profile' dialog box shows the following configuration:

- SSID: Zyxel
- Status: Active
- VLAN ID: 1 (range 1-4094)
- Band Mode: 2.4G
- Security Type: WPA2
- Personal: ☐
- Enterprise: ☒ (selected)
- Primary Radius Server: ☒
- RADIUS Server IP Address: [Redacted]
- RADIUS Server Port: [Redacted] (range 1-65535)
- RADIUS Server Secret: [Redacted]
- Secondary Radius Server: ☐
- RADIUS Server IP Address: [Redacted]
- RADIUS Server Port: [Redacted] (range 1-65535)
- RADIUS Server Secret: [Redacted]

Buttons: OK, Cancel

## 7.2.5 Summary

Use this screen to check whether what you have configured is correct. Click **Save** to apply your settings and complete the wizard setup. Otherwise, click **Prev** to return to the previous screen or click **Cancel** to close the wizard without saving.

**Figure 36** Wizard: Summary

The screenshot shows the 'Wizard Setting' window with a sidebar on the left containing steps Step 1 through Step 5. Step 5 is highlighted in blue and labeled 'Step 5'. The main area is titled 'Summary' and lists the following settings:

- Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
- Daylight Saving: Disable
- Management IP: Static IP
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Gateway: 0.0.0.0
- Dns Server: 0.0.0.0
- 2.4G Radio: Auto
- 5G Radio: Auto
- SSID

Below the settings list is a table with the following headers and values:

	Status	SSID	Security Mode	Band Mode	WLAN ID
1	ON				

At the bottom right of the window are three buttons: 'Prev', 'Save', and 'Cancel'.

# CHAPTER 8

## Monitor

### 8.1 Overview

Use the **Monitor** screens to check status and statistics information.

#### 8.1.1 What You Can Do in this Chapter

- The **Network Status** screen ([Section 8.3 on page 60](#)) displays general LAN interface information and packet statistics.
- The **AP Information > Radio List** screen ([Section 8.4 on page 62](#)) displays statistics about the WiFi radio transmitters in the Zyxel Device.
- The **Station Info** screen ([Section 8.5 on page 65](#)) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen ([Section 8.6 on page 66](#)) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen ([Section 8.7 on page 67](#)) displays information about suspected rogue APs.
- The **View Log** screen ([Section 8.8 on page 69](#)) displays the Zyxel Device's current log messages. You can change the way the log is displayed, you can email the log, and you can also clear the log in this screen.

### 8.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

#### Rogue AP

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security.

#### Friendly AP

Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from neighboring networks, for example).

## 8.3 Network Status

Use this screen to look at general Ethernet interface information and packet statistics. To access this screen, click **Monitor > Network Status**.

**Figure 37** Monitor > Network Status



The following table describes the labels in this screen.

Table 19 Monitor > Network Status

LABEL	DESCRIPTION
Interface Summary	
IPv6 Interface Summary	
	Use the <b>Interface Summary</b> section for IPv4 network settings. Use the <b>IPv6 Interface Summary</b> section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
Name	This field displays the name of the physical Ethernet port on the Zyxel Device.
Status	This field displays the current status of each physical port on the Zyxel Device.  <b>Down</b> - The port is not connected.  <b>Speed / Duplex</b> - The port is connected. This field displays the port speed and duplex setting ( <b>Full</b> or <b>Half</b> ).
VID	This field displays the VLAN ID to which the port belongs.
IP Addr/ Netmask IP Address	This field displays the current IP address (and subnet mask) of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or :: (in the IPv6 network), the interface does not have an IP address yet.
IP Assignment	This field displays how the interface gets its IPv4 address.  <b>Static</b> - This interface has a static IPv4 address.  <b>DHCP Client</b> - This interface gets its IPv4 address from a DHCP server.
Action	Use this field to get or to update the IP address for the interface. Click <b>Renew</b> to send a new DHCP request to a DHCP server. If the interface cannot use one of these ways to get or to update its IP address, this field displays <b>n/a</b> .
Port Statistics Table	

Table 19 Monitor &gt; Network Status (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Poll Interval	Enter how often you want this window to be updated automatically, and click <b>Set Interval</b> .
Set Interval	Click this to set the <b>Poll Interval</b> the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the <b>Poll Interval</b> and clicking <b>Set Interval</b> .
Switch to Graphic View	Click this to display the port statistics as a line graph.
Name	This field displays the name of the interface.
Status	This field displays the current status of the physical port.  <b>Down</b> - The physical port is not connected.  <b>Speed / Duplex</b> - The physical port is connected. This field displays the port speed and duplex setting ( <b>Full</b> or <b>Half</b> ).
TxPkts	This field displays the number of packets transmitted from the Zyxel Device on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the Zyxel Device on the physical port since it was last connected.
Tx Bcast	This field displays the number of broadcast packets transmitted from the Zyxel Device on the physical port since it was last connected.
Rx Bcast	This field displays the number of broadcast packets received by the Zyxel Device on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the Zyxel Device has been running since it last restarted or was turned on.

### 8.3.1 Port Statistics Graph

Use the port statistics graph to look at a line graph of packet statistics for the Ethernet port. To view, click **Monitor > Network Status** and then the **Switch to Graphic View** button.

**Figure 38** Monitor > Network Status > Switch to Graphic View

The following table describes the labels in this screen.

Table 20 Monitor &gt; Network Status &gt; Switch to Graphic View

Label	Description
General Settings	
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Usage	
Port Selection	Select the Ethernet port for which you want to view the packet statistics.
Switch to Grid View	Click this to display the port statistics as a table.
Kbps/Mbps	The y-axis represents the speed of transmission or reception.
Time	The x-axis shows the time period over which the transmission or reception occurred.
TX	This line represents traffic transmitted from the Zyxel Device on the physical port since it was last connected.
RX	This line represents the traffic received by the Zyxel Device on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.

## 8.4 Radio List

Use this screen to view statistics for the Zyxel Device's WiFi radio transmitters. To access this screen, click **Monitor > Wireless > AP Information > Radio List**.

**Figure 39** Monitor > Wireless > AP Information > Radio List (for Zyxel Device that supports WDS)

Radio List

Radio List

More Info

Status	Frequency	Chan	Trans	Sta	Upload	Downl	MAC Addr	R	OP Mod	AP / WDS Profile
💡	2.4G	1	25	0	0	670310	60:31:97:0...	1	AP (M...	default / default
💡	5G	161/1...	28	0	0	668x10	60:31:97:0...	2	AP (M...	default2 / def...

Page 1 of 1 | Show 10 Items

Deploying 1 - 2 of 2

Refresh

**Figure 40** Monitor > Wireless > AP Information > Radio List (for Zyxel Device that does not support WDS)

Status	Frequency Band	Channel	Transmit Power	Station	Upload	Download	MAC Address	Radio	OP Mode	Channel Utilization
5G	161/167/149/153	34	0	0	800276	8040	00:13:49:00:00:03	2	AP (M888E)	28%
2.4G	1	33	0	0	142230	0	00:13:49:00:00:02	1	AP (M888E)	91%

The following table describes the labels in this screen.

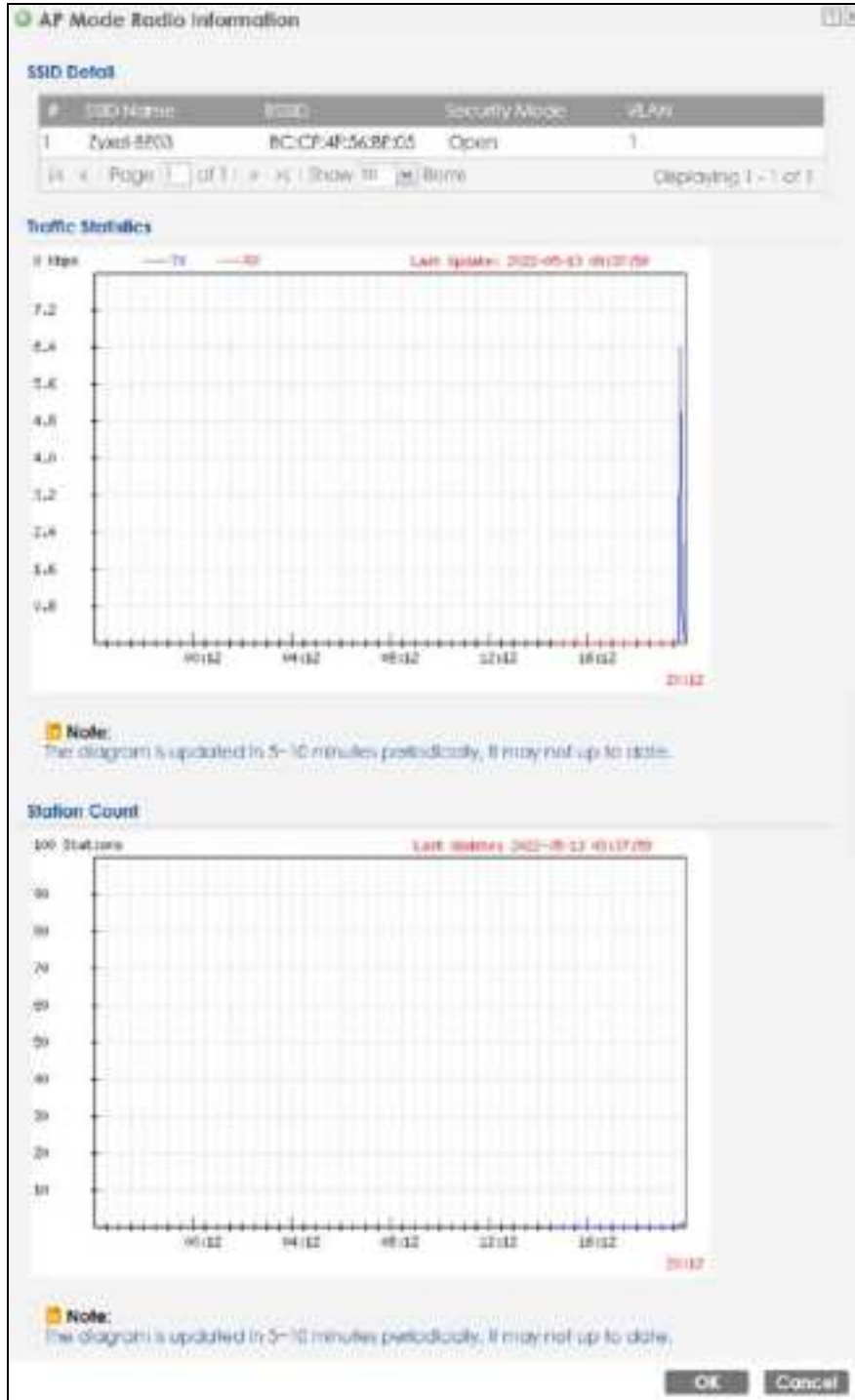
Table 21 Monitor &gt; Wireless &gt; AP Information &gt; Radio List

LABEL	DESCRIPTION
More Information	Click this to view additional information about the selected radio's wireless traffic and station count. Information spans a 24 hour period.
Status	This displays whether or not the radio is enabled.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the Zyxel Device to which it belongs.
OP Mode	This indicates the radio's operating mode. Operating modes are <b>AP (MBSSID)</b> , <b>Root AP</b> or <b>Repeater</b> .
AP/WDS Profile	This indicates the AP profile name and WDS profile name to which the radio belongs. This field is available only on the Zyxel Device that supports WDS.
Profile	This indicates the AP profile name to which the radio belongs. This field is available only on the Zyxel Device that does not support WDS.
Frequency Band	This indicates the wireless frequency band currently being used by the radio.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of WiFi clients connected to this radio on the Zyxel Device.
Upload	This displays the total number of packets received by the radio.
Download	This displays the total number of packets transmitted by the radio.
Channel Utilization	This indicates how much IEEE 802.11 traffic the radio can receive on the channel. It displays what percentage of the radio's channel is currently being used.

### 8.4.1 AP Mode Radio Information

This screen allows you to view a selected radio's SSID details, wireless traffic statistics and station count for the preceding 24 hours. To access this window, select a radio and click the **More Information** button in the **Radio List** screen.

**Figure 41** Monitor > Wireless > AP Information > Radio List > More Information





The following table describes the labels in this screen.

Table 22 Monitor > Wireless > AP Information > Radio List > More Information

LABEL	DESCRIPTION
SSID Detail	This list shows information about all the WiFi clients that have connected to the specified radio over the preceding 24 hours.
#	This is the items sequential number in the list. It has no bearing on the actual data in this list.
SSID Name	This displays an SSID associated with this radio. There can be up to eight maximum.
BSSID	This displays a BSSID associated with this radio. The BSSID is tied to the SSID.
Security Mode	This displays the security mode in which the SSID is operating.
VLAN	This displays the VLAN ID associated with the SSID.
Traffic Statistics	This graph displays the overall traffic information of the radio over the preceding 24 hours.
Kbps/Mbps	This y-axis represents the amount of data moved across this radio in megabytes per second.
Time	This x-axis represents the amount of time over which the data moved across this radio.
Station Count	This graph displays the connected station information of the radio over the preceding 24 hours.
Stations	The y-axis represents the number of connected stations.
Time	The x-axis shows the time period over which a station was connected.
Last Update	This field displays the date and time the information in the window was last updated.
OK	Click this to close this window.
Cancel	Click this to close this window.

## 8.5 Station List

Use this screen to view statistics pertaining to the associated stations (or "WiFi clients"). Click **Monitor > Wireless > Station Info** to access this screen.

Figure 42 Monitor > Wireless > Station Info



The screenshot shows a web interface titled "Station List". It contains a table with the following columns: #, IP Addr, MAC Addr, Radio, Capability, BSSID, SSID Name, Security, Signal Str., Tx Rate, and Assoc. Time. The first row of data shows: 1, 172..., 00:19:cd..., I, 802.11b/g, N/A, Zylin-803, Open, -35dBm, 54M, 54M, 19:58:40... Below the table, there is a pagination bar showing "Page 1 of 1" and "Showing 1 of 1 items". A "Refresh" button is located at the bottom right of the table area.

The following table describes the labels in this screen.

Table 23 Monitor > Wireless > Station Info

LABEL	DESCRIPTION
#	This is the station's index number in this list.
IP Address	This is the station's IP address.
Band	This is the frequency band to which the station is connected.

Table 23 Monitor &gt; Wireless &gt; Station Info (continued)

LABEL	DESCRIPTION
MAC Address	This is the station's MAC address.
Radio	This is the radio number on the Zyxel Device to which the station is connected.
Capability	This displays the supported standard currently being used by the station or the standards supported by the station.
802.11 Features	This displays whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above ( <b>N/A</b> ).
SSID Name	This indicates the name of the WiFi network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This indicates which secure encryption methods is being used by the station to connect to the network.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the station's WiFi connection.
Tx Rate	This is the maximum transmission rate of the station.
Rx Rate	This is the maximum reception rate of the station.
Association Time	This displays the time the station first associated with the Zyxel Device's WiFi network.
Refresh	Click this to refresh the items displayed on this page.

## 8.6 WDS Link Info

Use this screen to view the WDS traffic statistics between the Zyxel Device and a root AP or repeaters. See [Section 1.3 on page 14](#) to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

**Figure 43** Monitor > Wireless > WDS Link Info

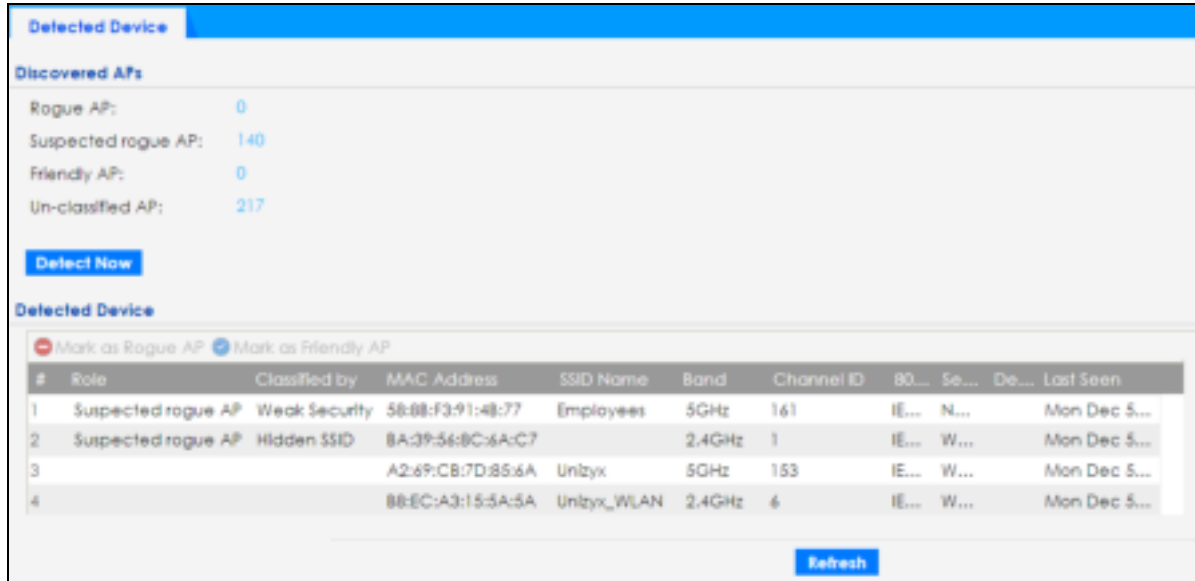
The following table describes the labels in this screen.

Table 24 Monitor > Wireless > WDS Link Info

LABEL	DESCRIPTION
WDS Uplink Info	<b>Uplink</b> refers to the WDS link from the repeaters to the root AP.
WDS Downlink Info	<p><b>Downlink</b> refers to the WDS link from the root AP to the repeaters.</p> <p>When the Zyxel Device is in root AP mode and connected to a repeater, only the downlink information is displayed.</p> <p>When the Zyxel Device is in repeater mode and connected to a root AP directly or via another repeater, the uplink information is displayed.</p> <p>When the Zyxel Device is in repeater mode and connected to a root AP and other repeater(s), both the uplink and downlink information would be displayed.</p>
#	This is the index number of the root AP or repeater in this list.
MAC Address	This is the MAC address of the root AP or repeater to which the Zyxel Device is connected using WDS.
Band	This is the frequency band of the WiFi network to which the Zyxel Device is connected using WDS.
Radio	This is the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS.
SSID Name	This indicates the name of the WiFi network to which the Zyxel Device is connected using WDS.
Security Mode	This indicates which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the wireless connection in WDS.
Tx Rate	This is the maximum transmission rate of the root AP or repeater to which the Zyxel Device is connected using WDS.
Rx Rate	This is the maximum reception rate of the root AP or repeater to which the Zyxel Device is connected using WDS.
Association Time	This displays the time the Zyxel Device first associated with the wireless network using WDS.
Refresh	Click this to refresh the items displayed on this page.

## 8.7 Detected Device

Use this screen to view information about surrounding APs which you could mark as Rogue or Friendly. Click **Monitor > Wireless > Detected Device** to access this screen. For more information about Rogue APs, see [Section 10.3 on page 85](#).

**Figure 44** Monitor > Wireless > Detected Device

The following table describes the labels in this screen.

**Table 25** Monitor > Wireless > Detected Device

LABEL	DESCRIPTION
Discovered APs	
Rogue AP	This shows how many devices are detected as rogue APs.
Suspected rogue AP	This shows how many devices are detected as possible rogue APs based on the classification rule(s) in <a href="#">Section 10.3 on page 85</a> .
Friendly AP	This shows how many devices are detected as friendly APs.
Un-classified AP	This shows how many devices are detected, but have not been classified as either Rogue or Friendly by the Zyxel Device.
Detect Now	Click this button for the Zyxel Device to scan for APs in the network.
Detected Device	
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. For more on managing rogue APs, see the <b>Configuration &gt; Wireless &gt; Rogue AP</b> screen ( <a href="#">Section 10.3 on page 85</a> ).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the <b>Configuration &gt; Wireless &gt; Rogue AP</b> screen ( <a href="#">Section 10.3 on page 85</a> ).
#	This is the detected device's index number in this list.
Status	This indicates the detected device's status.
Device	This indicates the type of device detected.
Role	This indicates the detected device's role (such as friendly or rogue).
Classified by	This indicates the detected device's classification rule.
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Band	This is the frequency band to which the station is connected.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n/ac/ax) transmitted by the detected device.
Security	This indicates the encryption method (if any) used by the detected device.

Table 25 Monitor &gt; Wireless &gt; Detected Device (continued)

LABEL	DESCRIPTION
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the <b>Configuration &gt; Wireless &gt; Rogue AP</b> screen (Section 10.3 on page 85).
Last Seen	This indicates the last time the device was detected by the Zyxel Device.
Refresh	Click this to refresh the items displayed on this page.

## 8.8 View Log

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

Note: 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.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

The Web Configurator saves the filter settings once you click **Search**. If you leave the **View Log** screen and return to it later, the last filter settings would still apply.

Figure 45 Monitor &gt; Log &gt; View Log

**View Log**  
Hide Filter

**Logs**

Display: All Logs  
Source Address:   
Source Interface: any  
Protocol: any  
Priority: any  
Destination Address:   
Destination Interface: any  
Keyword:   
**Search**

**Refresh** **Clear Log**

#	Time	Priority	Category	Message	Source	Dest.	Note
77	2022-12-05 ...	Info	User	Admin's password has been changed.			USER
6	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
75	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
78	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
76	2022-12-05 ...	notice	User	Administrator admin http/https logout	172.21.40.38		Account: admin
35	2022-12-05 ...	notice	User	Administrator admin http/https logout (lease timeout).	172.21.40.38		Account: admin
79	2022-12-05 ...	alert	User	Failed login attempt to WAX6405-6E from http/https (inc...	172.21.40.38		Account: admin
1...	2022-12-04 ...	error	System	NTP update failed with Missing default gateway setting.			System

Page 1 of 11 | Show 30 items | Displaying 1 - 30 of 512

The following table describes the labels in this screen.

Table 26 Monitor > Log > View Log

<b>LABEL</b>	<b>DESCRIPTION</b>
Show Filter / Hide Filter	Click this button to show or hide the filter settings.  The <b>Priority</b> , <b>Source Address</b> , <b>Destination Address</b> , <b>Source Interface</b> , <b>Destination Interface</b> , <b>Protocol</b> , <b>Keyword</b> , and <b>Search</b> fields are only available if the filter settings are shown.
Display	Select the category of log message(s) you want to view. You can also view <b>All Logs</b> at one time, or you can view the <b>Debug Log</b> .
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: <b>any</b> , <b>emerg</b> , <b>alert</b> , <b>crit</b> , <b>error</b> , <b>warn</b> , <b>notice</b> , and <b>info</b> , from highest priority to lowest priority. This field is read-only if the <b>Category</b> is <b>Debug Log</b> .
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the <b>Message</b> , <b>Source</b> , <b>Destination</b> and <b>Note</b> fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks (!) ' , ; : ? ! + - * / = # \$ % @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the <b>Priority</b> field above.
Category	This field displays the log that generated the log message. It is the same value used in the <b>Display</b> and (other) <b>Category</b> fields.
Message	This field displays the reason the log message was generated. The text "[count=x]", where <i>x</i> is a number, appears at the end of the <b>Message</b> field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.
Protocol	This field displays the service protocol in the event that generated the log message.
Note	This field displays any additional information about the log message.

# CHAPTER 9

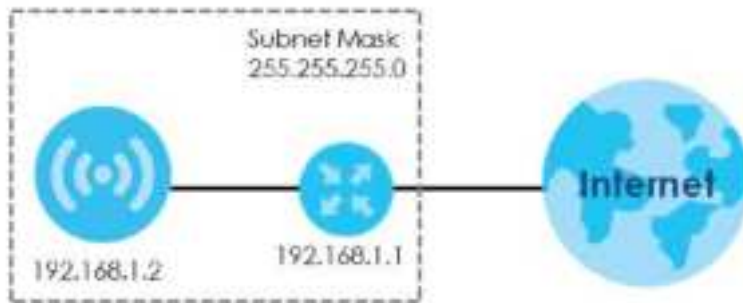
## Network

### 9.1 Overview

This chapter describes how you can configure the management IP address and VLAN settings of your Zyxel Device.

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.

**Figure 46** IP Setup



The figure above illustrates one possible setup of your Zyxel Device. The gateway IP address is 192.168.1.1 and the managed IP address of the Zyxel Device is 192.168.1.2 (default), but if the Zyxel Device is assigned an IP address by a DHCP server, the default (192.168.1.2) will not be used. The gateway and the Zyxel Device must belong in the same IP subnet to be able to communicate with each other.

#### 9.1.1 What You Can Do in this Chapter

- The **IP Setting** screen ([Section 9.2 on page 71](#)) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen ([Section 9.3 on page 73](#)) configures the Zyxel Device's VLAN settings.
- The **NCC Discovery** screen ([Section 9.4 on page 76](#)) configures the Zyxel Device's Nebula Control Center (NCC) discovery settings.

### 9.2 IP Setting

Use this screen to configure the IP address for your Zyxel Device. To access this screen, click **Configuration > Network > IP Setting**.

**Figure 47** Configuration > Network > IP Setting

Each field is described in the following table.

**Table 27** Configuration > Network > IP Setting

LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
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.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
IPv6 Address Assignment	
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on the Zyxel Device. The Zyxel Device will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network.
Link-Local Address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the LAN interface.



Table 27 Configuration &gt; Network &gt; IP Setting (continued)

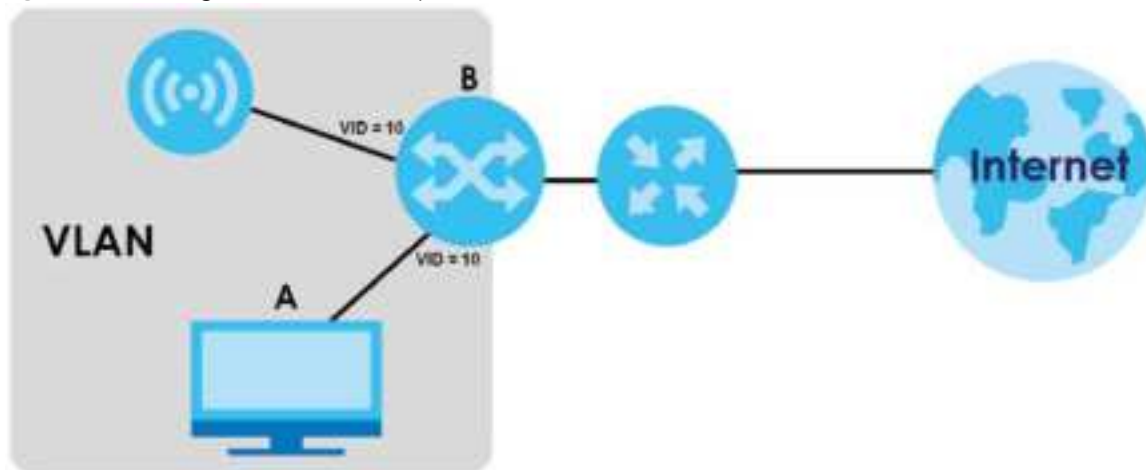
LABEL	DESCRIPTION
IPv6 Address/Prefix Length	Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional.  The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on the LAN interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first. Enter zero to set the metric to 1024 for IPv6.
DHCPv6 Client	Select this option to set the Zyxel Device to act as a DHCPv6 client.
DUID	This field displays the DHCP Unique Identifier (DUID) of the Zyxel Device, which is unique and used for identification purposes when the Zyxel Device is exchanging DHCPv6 messages with others. See <a href="#">Appendix B on page 235</a> for more information.
Request Address	Select this option to get an IPv6 address from the DHCPv6 server.
DHCPv6 Request Options	Select this option to determine what additional information to get from the DHCPv6 server.
DNS Server	Select this option to obtain the IP address of the DNS server.
NTP Server	Select this option to obtain the IP address of the NTP server.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

## 9.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings.

Note: Mis-configuring the management VLAN settings on your Zyxel Device can make it inaccessible. If this happens, you will have to reset the Zyxel Device.

**Figure 48** Management VLAN Setup



In the figure above, to access and manage the Zyxel Device from computer **A**, the Zyxel Device and switch **B**'s ports to which computer **A** and the Zyxel Device are connected should be in the same VLAN.

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

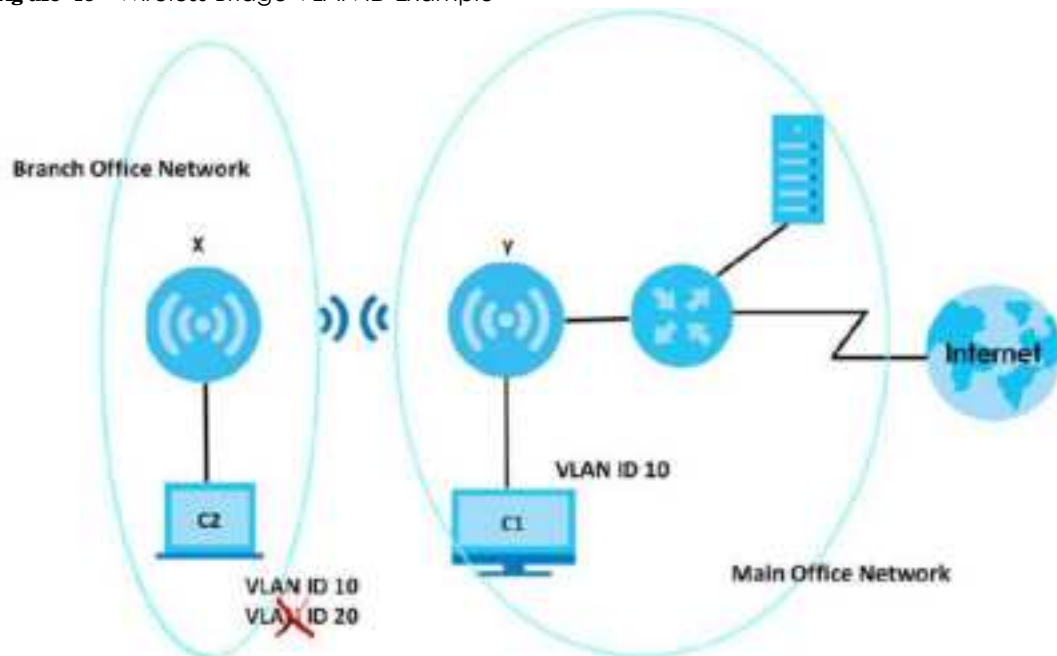
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

### Wireless Bridge VLAN ID

Wireless bridge VLAN allows you to have clients in different WiFi networks appear to be in the same virtual network using VLAN IDs. VLAN IDs are sent across the wireless bridge so that only clients with the same VLAN ID receive that network traffic. See [Section 1.3 on page 14](#) for more information on the wireless bridge.

In the figure below, a client (**C2**) in the branch office wants to connect to the main office (**Y**). The branch office client (**C2**) can connect to the main office network using the **VLAN ID 10**. However, the branch office client (**C2**) cannot connect to the main office network using the **VLAN ID 20** because that VLAN ID does not exist in the main office network. To bridge the branch office network and the main office network, the VLAN IDs you set on the Zyxel Device (**X**) should be the same as the VLAN IDs you set on the root AP (**Y**).

**Figure 49** Wireless Bridge VLAN ID Example



### IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority.

The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

Use this screen to configure the VLAN settings for your Zyxel Device. To access this screen, click **Configuration > Network > VLAN**.

Note: Not all Zyxel Devices support the wireless bridge VLAN settings; see [Table 1 on page 12](#) for more information.

**Figure 50** Configuration > Network > VLAN

**Figure 51** Configuration > Network > VLAN

Each field is described in the following table.

Table 28 Configuration > Network > VLAN

Label	Description
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device. The range is 1–4094.
As Native VLAN	Select this option to treat this VLAN ID as a VLAN created on the Zyxel Device and not one assigned to it from outside the network.
Wireless Bridge Vlan Setting	
This section appears if your Zyxel Device supports wireless bridge. See the feature comparison table in <a href="#">Section 1.2 on page 12</a> .	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.

Table 28 Configuration &gt; Network &gt; VLAN (continued)

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID (1-4094)	Enter a VLAN ID for the wireless bridge. Duplicate VLAN IDs are not allowed. The VLAN IDs you set on your root AP should be the same as the VLAN IDs you set here. See <a href="#">Section 1.3 on page 14</a> for more information on wireless bridge.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

## 9.4 NCC Discovery

You can manage the Zyxel Device through the Zyxel Nebula Control Center (NCC). Use this screen to configure the proxy server settings if the Zyxel Device is behind a proxy server.

To access this screen, click **Configuration > Network > NCC Discovery**.

Figure 52 Configuration &gt; Network &gt; NCC Discovery

Each field is described in the following table.

Table 29 Configuration &gt; Network &gt; NCC Discovery

LABEL	DESCRIPTION
Nebula Control Center Status	
Internet	This field displays whether the Zyxel Device can connect to the Internet.
Nebula Connectivity	This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC).
Nebula Control Center Discovery Setting	

Table 29 Configuration &gt; Network &gt; NCC Discovery

LABEL	DESCRIPTION
Enable	<p>Select this option to turn on NCC discovery on the Zyxel Device. The Zyxel Device will try to discover the NCC and go into NCC management mode when it is connected to the Internet and has been registered in the NCC.</p> <p>If NCC discovery is disabled, the Zyxel Device will not discover the NCC and remain in standalone operation.</p>
Use Proxy to Access NCC	If the Zyxel Device is behind a proxy server, you need to select this option and configure the proxy server settings so that the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter the service port number used by the proxy server.
Authentication	Select this option if the proxy server requires authentication before it grants access to the NCC.
User Name	Enter your proxy user name.
Password	Enter your proxy password.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

# CHAPTER 10

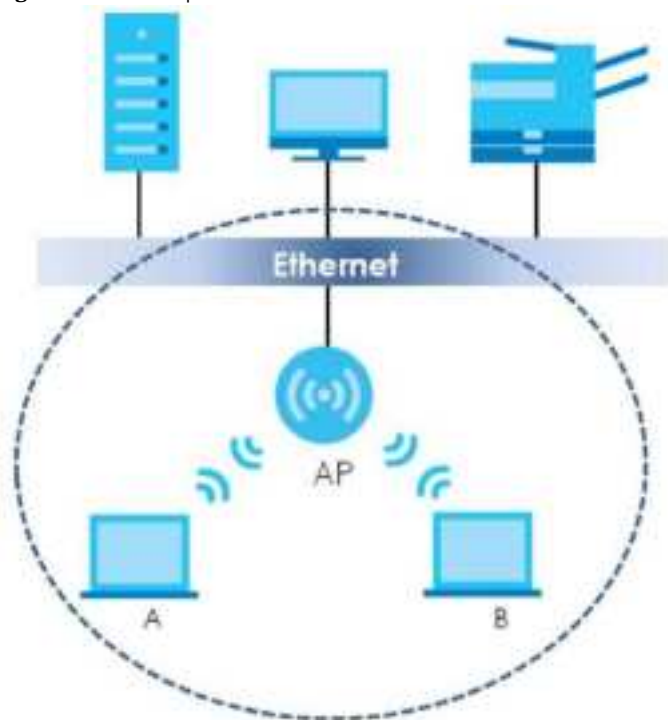
## Wireless

### 10.1 Overview

This chapter discusses how to configure the WiFi network settings in your Zyxel Device.

The following figure provides an example of a WiFi network.

**Figure 53** Example of a WiFi Network



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

#### 10.1.1 What You Can Do in this Chapter

- The **AP Management** screen ([Section 10.2 on page 79](#)) allows you to manage the Zyxel Device's general WiFi settings.
- The **Rogue AP** screen ([Section 10.3 on page 85](#)) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **DCS** screen ([Section 10.4 on page 89](#)) allows you to configure dynamic radio channel selection.

### 10.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### **Station / WiFi Client**

A station or WiFi client is any WiFi-capable device that can connect to an AP using a WiFi signal.

#### **Dynamic Channel Selection (DCS)**

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel which it broadcasts. For more information, see [Section 10.5 on page 89](#).

## 10.2 AP Management

Use this screen to manage the Zyxel Device's general WiFi settings. Click **Configuration > Wireless > AP Management** to access this screen.

Note: Not all Zyxel Devices support the wireless bridge VLAN settings; see [Table 1 on page 12](#) for more information.

**Figure 54** Configuration > Wireless > AP Management- AP Mode

**WLAN Setting**

☐ Create new Object

**Radio 1 Setting**

☒ Radio 1 Activate

Radio 1 OP Mode: ☒ AP Mode ☐ Root AP ☐ Repeater ⓘ

Radio 1 Profile: default ⓘ + ⓘ ⓘ ⓘ

Max Output Power: 30 dBm [0-30]

**MSSDP Settings**

#	MSSDP Profile	
1	default	+ ⓘ
2	disable	+ ⓘ
3	disable	+ ⓘ
4	disable	+ ⓘ
5	disable	+ ⓘ
6	disable	+ ⓘ
7	disable	+ ⓘ
8	disable	+ ⓘ

**Radio 2 Setting**

☒ Radio 2 Activate

Radio 2 OP Mode: ☒ AP Mode ☐ Root AP ☐ Repeater ⓘ

Radio 2 Profile: default ⓘ + ⓘ ⓘ ⓘ

Max Output Power: 30 dBm [0-30]

**MSSDP Settings**

#	MSSDP Profile	
1	default	+ ⓘ
2	disable	+ ⓘ
3	disable	+ ⓘ
4	disable	+ ⓘ
5	disable	+ ⓘ
6	disable	+ ⓘ
7	disable	+ ⓘ
8	disable	+ ⓘ

Apply Reset



**Figure 55** Configuration > Wireless > AP Management- Repeater Mode

**WLAN Setting**  
 (Create New Object)

**Radio 1 Setting**

☒ Radio 1 Activate

Radio 1 OP Mode: ☐ AP Mode ☐ Root AP ☒ Repeater

Radio 1 Profile: default

Radio 1 WDS Profile: default

☒ Enable WDS Wireless Bridging

Uplink Selection Mode: ☒ AUTO ☐ Manual

[Select Uplink Profile](#)

Max Output Power: 30 dBm (0~30)

**MBSSID Settings**

Profile	1	2	3	4	5	6	7	8
default	default	disable	disable	disable	disable	disable	disable	disable

**Radio 2 Setting**

☒ Radio 2 Activate

Radio 2 OP Mode: ☒ AP Mode ☐ Root AP ☐ Repeater

Radio 2 Profile: default2

Max Output Power: 30 dBm (0~30)

**MBSSID Settings**

Profile	1	2	3	4	5	6	7	8
default	default	disable	disable	disable	disable	disable	disable	disable

**Apply** **Reset**

**Figure 56** Configuration > Wireless > AP Management > Setup Wireless Bridge Vlan ID: Wireless Bridge Vlan Setting

Each field is described in the following table.

Table 30 Configuration &gt; Wireless &gt; AP Management

LABEL	DESCRIPTION
Radio 1 Setting	
Radio 1 Activate	Select the check box to enable the Zyxel Device's first (default) radio.
Radio 1 OP Mode	<p>Select the operating mode for radio 1.</p> <p><b>AP Mode</b> means the radio can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing).</p> <p><b>Root AP</b> means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS (Wireless Distribution System) to extend its wireless network.</p> <p><b>Repeater</b> means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.</p>
Radio 1 Profile	<p>Select the radio profile the radio uses.</p> <p>Note: You can only apply a 2.4G AP radio profile to radio 1. Otherwise, the first radio will not be working.</p>
Radio 1 WDS Profile	<p>This field is available only when the radio is in <b>Root AP</b> or <b>Repeater</b> mode.</p> <p>Select the WDS profile the radio uses to connect to a root AP or repeater.</p>
Enable WDS Wireless Bridging	<p>If you set the Zyxel Device as a root AP, the radio that's bridging with the Zyxel Device should be in repeater mode.</p> <p>Be careful to avoid bridge loops. For example, if your root AP and the Zyxel Device are connected to a switch, and they're also connected to each other using a WiFi connection. This will create bridge loops.</p> <p>This field is available only when the radio is in <b>Repeater</b> mode. Select this to enable WDS wireless bridging on the Zyxel Device. See <a href="#">Section 1.3 on page 14</a> for more information on Wireless Distribution System (WDS).</p>

Table 30 Configuration &gt; Wireless &gt; AP Management (continued)









LABEL	DESCRIPTION
Uplink Selection Mode	<p>This field is available only when the radio is in <b>Repeater</b> mode.</p> <p>Select <b>AUTO</b> to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater.</p> <p>Select <b>Manual</b> to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the <b>Radio 1 Uplink MAC Address</b> field.</p>
Setup Wireless Bridge Vlan ID	<p>This appears if you select <b>Enable WDS Wireless Bridging</b>.</p> <p>Click this to show the <b>Wireless Bridge Vlan Setting</b> pop-up window. This link is available only when the radio is in <b>Root AP</b> or <b>Repeater</b> mode.</p>
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See <a href="#">Section 1.3 on page 14</a> for more information on wireless bridge.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Close	Click <b>Close</b> to close the pop-up window without saving your changes.
Max Output Power	<p>Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs.</p> <p>Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.</p>
MBSSID Settings	
Add 	<p>This button is not available after you configure the Zyxel Device using the wizard.</p> <p>Click the <b>Add</b> icon () to open a screen where you can create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click <b>Add</b> to create a new entry after the selected entry.</p>
Edit 	Click the <b>Edit</b> icon (  ) to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field displays the SSID profile that is associated with the radio profile.
Radio 2 Setting	
For models that support triple radios, you can find the <b>Radio 3 Setting</b> fields at the bottom of the screen.	
Radio 2 Activate	<p>This displays if the Zyxel Device has a second radio.</p> <p>Select the check box to enable the Zyxel Device's second radio.</p>

Table 30 Configuration &gt; Wireless &gt; AP Management (continued)

LABEL	DESCRIPTION
Radio 2 OP Mode	<p>This displays if the Zyxel Device has a second radio. Select the operating mode for radio 2.</p> <p><b>AP Mode</b> means the radio can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing).</p> <p><b>Root AP</b> means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS to extend its wireless network.</p> <p><b>Repeater</b> means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.</p>
Radio 2 Profile	<p>This displays if the Zyxel Device has a second radio. Select the radio profile the radio uses.</p> <p>Note: For models that do not support BandFlex, you can only apply a 5G AP radio profile to radio 2. Otherwise, the second radio will not be working. See <a href="#">Section 1.3 on page 14</a> for more information.</p>
Radio 2 WDS Profile	<p>This field is available only when the radio is in <b>Root AP</b> or <b>Repeater</b> mode.</p> <p>Select the WDS profile the radio uses to connect to a root AP or repeater.</p>
Enable WDS Wireless Bridging	<p>If you set the Zyxel Device as a root AP, the radio that's bridging with the Zyxel Device should be in repeater mode.</p> <p>Be careful to avoid bridge loops. For example, if your root AP and the Zyxel Device are connected to a switch, and they're also connected to each other using a WiFi connection. This will create bridge loops.</p> <p>This field is available only when the radio is in <b>Repeater</b> mode. Select this to enable WDS wireless bridging on the Zyxel Device. See <a href="#">Section 1.3 on page 14</a> for more information on Wireless Distribution System (WDS).</p>
Uplink Selection Mode	<p>This field is available only when the radio is in <b>Repeater</b> mode.</p> <p>Select <b>AUTO</b> to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater.</p> <p>Select <b>Manual</b> to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the <b>Radio 1 Uplink MAC Address</b> field.</p>
Setup Wireless Bridge Vlan ID	Click this to show the <b>Wireless Bridge Vlan Setting</b> pop-up window. This link is available only when the radio is in <b>Root AP</b> or <b>Repeater</b> mode.
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See <a href="#">Section 1.3 on page 14</a> for more information on wireless bridge.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Close	Click <b>Close</b> to close the pop-up window without saving your changes.
Max Output Power	<p>Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs.</p> <p>Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.</p>
MBSSID Settings	

Table 30 Configuration &gt; Wireless &gt; AP Management (continued)

LABEL	DESCRIPTION
Add 	This button is not available after you configure the Zyxel Device using the wizard.  Click the <b>Add</b> icon (  ) to open a screen where you can create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click <b>Add</b> to create a new entry after the selected entry.
Edit 	Click <b>Edit</b> (  ) to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field shows the SSID profile that is associated with the radio profile.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

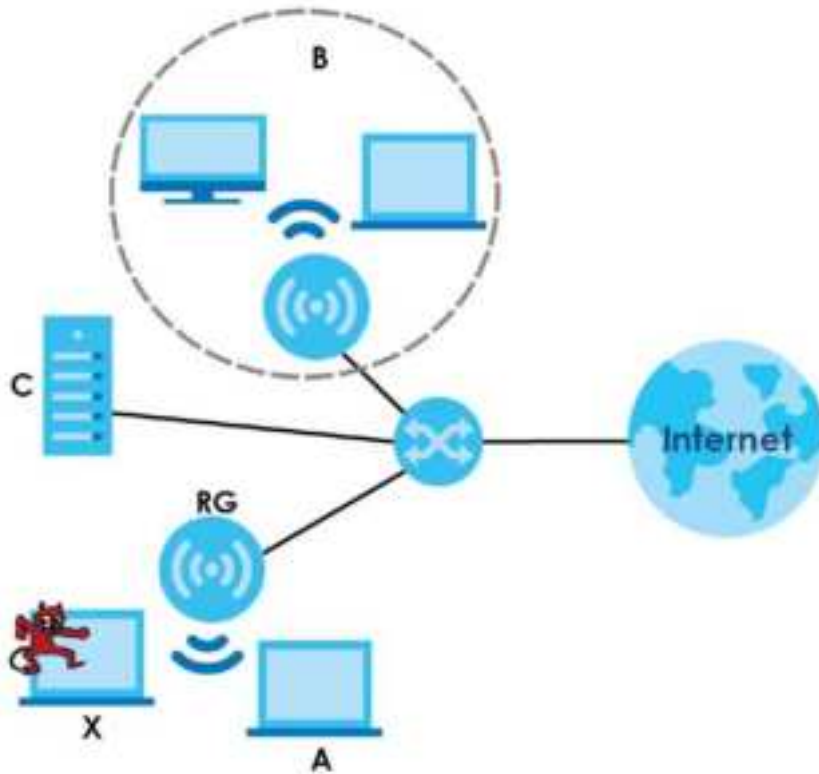
## 10.3 Rogue AP

Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

### Rogue APs

A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

In the following example, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate WiFi network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

**Figure 57** Rogue AP Example

### Friendly APs

If you have more than one AP in your WiFi network, you should also configure a list of “friendly” APs. Friendly APs are wireless access points that you know are not a threat. It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points. Exported lists show MAC addresses in txt file format separated by line breaks.

### Rogue AP Detection

This feature allows the Zyxel Device to monitor the WiFi signals for other wireless APs (see also [Section 1.3.3 on page 19](#)). Detected APs will appear in the **Monitor > Wireless > Detected Device** screen, where the Zyxel Device will label APs with the criteria you select in **Suspected Rogue AP Classification Rule** as a suspected rogue. The APs which you mark as either rogue or friendly APs in the **Monitor > Wireless > Detected Device** screen will appear in the **Wireless > Rogue AP** screen. See [Section 1.2 on page 12](#) to know which models support **Rogue AP Detection**.

Note: Enabling **Rogue AP Detection** might affect the performance of WiFi clients associated with the Zyxel Device.

**Figure 58** Configuration > Wireless > Rogue AP

**Rogue/Friendly AP List**

**Rogue AP Detection Setting**

☒ Enable Rogue AP Detection

**Suspected Rogue AP Classification Rule**

☒ Weak Security (Open, WEP, WPA-PSK)

☒ Hidden SSID

☒ SSID Keyword

#	SSID Keyword
1	test

**Rogue/Friendly AP List**

#	Role	MAC Address	Description
1	friendly-ap	60:31:97:7D:58:51	
2	rogue-ap	00:A0:C6:01:23:45	rogue-ap

Displaying 1 - 2 of 2

**Rogue AP List Importing/Exporting**

File:

**Friendly AP List Importing/Exporting**

File:

Each field is described in the following table.

**Table 31** Configuration > Wireless > Rogue AP

Label	Description
<b>Rogue AP Detection Setting</b>	
Enable Rogue AP Detection	Select this check box to detect Rogue APs in the network.
Suspected Rogue AP Classification Rule	Select the check boxes ( <b>Weak Security (Open, WEP, WPA-PSK)</b> , <b>Hidden SSID</b> , <b>SSID Keyword</b> ) of the characteristics an AP should have for the Zyxel Device to mark it as a Rogue AP.
Add	Click this to add an SSID Keyword.
Edit	Select an SSID Keyword and click this button to modify it.
Remove	Select an existing SSID keyword and click this button to delete it.
#	This is the SSID Keyword's index number in this list.
SSID Keyword	This field displays the SSID Keyword.
<b>Rogue/Friendly AP List</b>	
Add	Click this button to add an AP to the list and assign it either friendly or rogue status.
Edit	Select an AP in the list to edit and reassign its status.
Remove	Select an AP in the list to remove.

Table 31 Configuration &gt; Wireless &gt; Rogue AP (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Role	This field indicates whether the selected AP is a <b>rogue-ap</b> or a <b>friendly-ap</b> . To change the AP's role, click the <b>Edit</b> button.
MAC Address	This field indicates the AP's radio MAC address.
Description	This field displays the AP's description. You can modify this by clicking the <b>Edit</b> button.
Rogue/Friendly AP List Importing/Exporting	These controls allow you to export the current list of rogue and friendly APs or import existing lists.
File Path / Browse / Importing	Enter the file name and path of the list you want to import or click the <b>Browse</b> button to locate it. Once the <b>File Path</b> field has been populated, click <b>Importing</b> to bring the list into the Zyxel Device.  You need to wait a while for the importing process to finish.
Exporting	Click this button to export the current list of either rogue APs or friendly APS.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

### 10.3.1 Add/ Edit Rogue/ Friendly List

Click **Add** or select an AP and click the **Edit** button in the **Configuration > Wireless > Rogue AP** table to display this screen.

**Figure 59** Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

Each field is described in the following table.

Table 32 Configuration &gt; Wireless &gt; Rogue AP &gt; Add/Edit Rogue/Friendly AP List

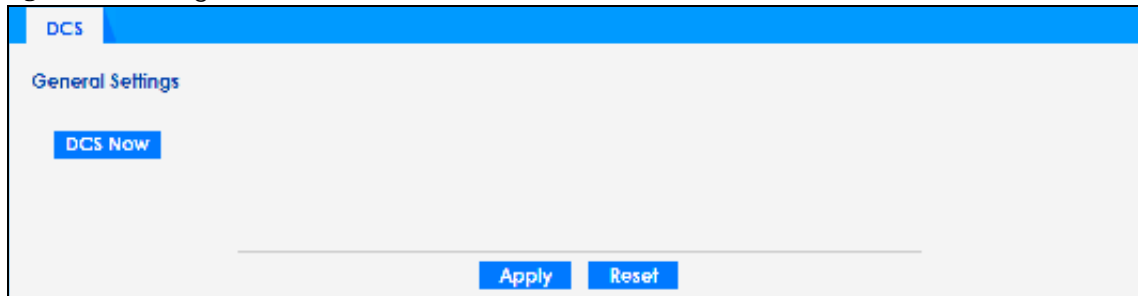
LABEL	DESCRIPTION
MAC	Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadecimal format: xx:xx:xx:xx:xx:xx where xx is a hexadecimal number separated by colons.
Description	Enter up to 60 characters for the AP's description. Spaces and underscores are allowed.
Role	Select either <b>Rogue AP</b> or <b>Friendly AP</b> for the AP's role.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to close the window with changes unsaved.



## 10.4 DCS

Use this screen to configure dynamic radio channel selection (see [Dynamic Channel Selection \(DCS\) on page 79](#)). Click **Configuration > Wireless > DCS** to access this screen.

**Figure 60** Configuration > Wireless > DCS



Each field is described in the following table.

**Table 33** Configuration > Wireless > DCS

LABEL	DESCRIPTION
DCS Now	Click this to have the Zyxel Device scan for and select an available channel immediately.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

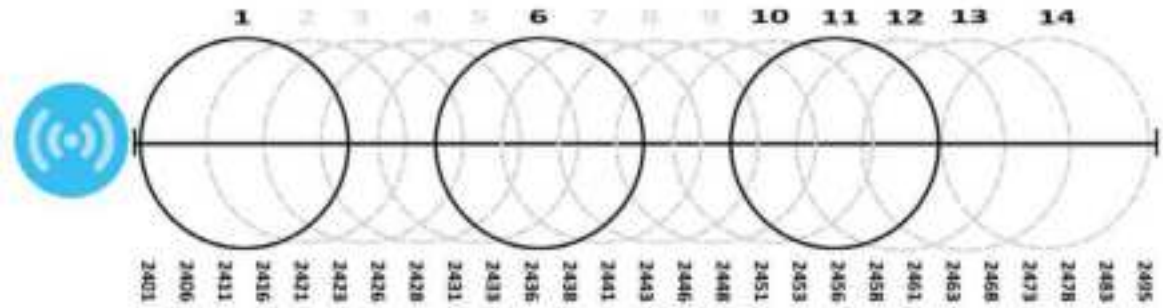
## 10.5 Technical Reference

The following section contains additional technical information about the features described in this chapter.

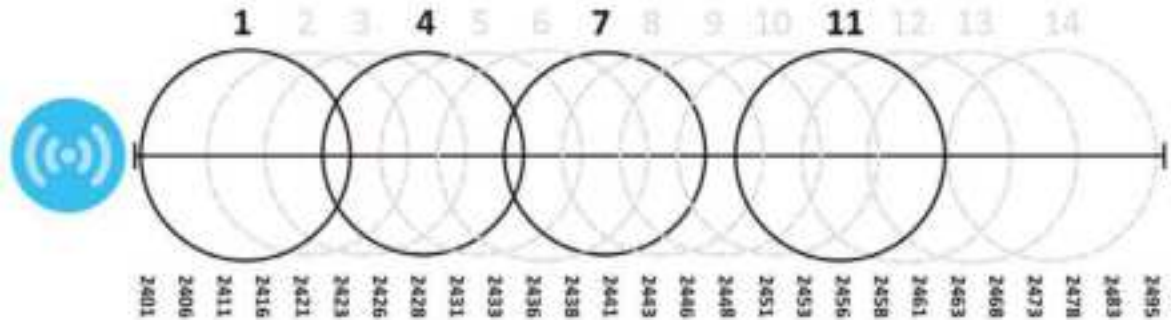
### Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

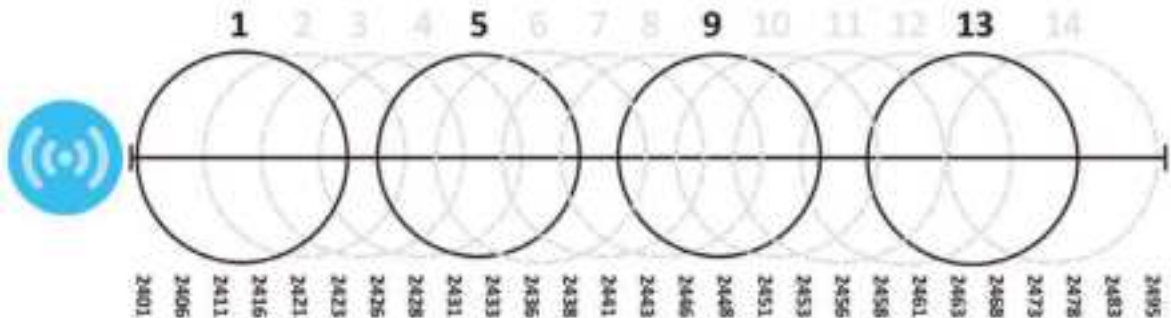
**Figure 61** An Example Three-Channel Deployment

Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these 3 channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

**Figure 62** An Example Four-Channel Deployment

However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called "safe" channels (1, 6 and 11) that interference becomes inevitable, the severity of it is dependent upon other factors: proximity to the affected AP, signal strength, activity, and so on.

Finally, there is an alternative four channel scheme for ETSI, consisting of channels 1, 5, 9, 13. This offers significantly less overlap than the other one.

**Figure 63** An Alternative Four-Channel Deployment

# CHAPTER 11

## User

### 11.1 Overview

This chapter describes how to set up user accounts and user settings for the Zyxel Device.

#### 11.1.1 What You Can Do in this Chapter

- The **User** screen (see [Section 11.2 on page 92](#)) provides a summary of all user accounts.
- The **Setting** screen (see [Section 11.3 on page 94](#)) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

#### 11.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

##### User Account

A user account defines the privileges of a user logged into the Zyxel Device. User accounts are used in controlling access to configuration and services in the Zyxel Device.

##### User Types

These are the types of user accounts the Zyxel Device uses.

Table 34 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access  Browse user-mode commands (CLI)	

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting.

## 11.2 User Summary

The **User** screen provides a summary of all user accounts. To access this screen click **Configuration > Object > User**.

**Figure 64** Configuration > Object > User



The following table describes the labels in this screen.

**Table 35** Configuration > Object > User

<b>LABEL</b>	<b>DESCRIPTION</b>
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click <b>Remove</b> . The ZyXel Device confirms you want to remove it before doing so.
Object Reference	Select an entry and click <b>Object Reference</b> to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays type of user this account was configured as. <ul style="list-style-type: none"> <li>• <b>admin</b> - this user can look at and change the configuration of the ZyXel Device</li> <li>• <b>limited-admin</b> - this user can look at the configuration of the ZyXel Device but not to change it</li> <li>• <b>user</b> - this user has access to the ZyXel Device's services but cannot look at the configuration</li> </ul>
Description	This field displays the description for each user.

### 11.2.1 Add/ Edit User

The **UserAdd/ Edit** screen allows you to create a new user account or edit an existing one.

#### 11.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- \_ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (\_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:
  - adm
  - admin
  - any
  - bin
  - daemon
  - debug
  - devicehaecived
  - ftp
  - games
  - halt
  - ldap-users
  - lp
  - mail
  - news
  - nobody
  - operator
  - radius-users
  - root
  - shutdown
  - sshd
  - sync
  - uucp
  - zyxel

To access this screen, go to the **User** screen, and click **Add** or **Edit**.

**Figure 65** Configuration > Object > User > Add/Edit A User

The following table describes the labels in this screen.

**Table 36** Configuration > User > User > Add/Edit A User

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved.
User Type	Select what type of user this is. Choices are: <ul style="list-style-type: none"> <li>• <b>admin</b> - this user can look at and change the configuration of the Zyxel Device</li> <li>• <b>limited-admin</b> - this user can look at the configuration of the Zyxel Device but not to change it</li> <li>• <b>user</b> - this is used for embedded RADIUS server and SNMPv3 user access</li> </ul>
Password	Enter the password of this user account. It can consist of 4 - 63 alphanumeric characters.
Retype	Re-enter the password to make sure you have entered it correctly.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.

Table 36 Configuration &gt; User &gt; User &gt; Add/Edit A User (continued)

LABEL	DESCRIPTION
Authentication Timeout Settings	This field is not available if the user type is <b>user</b> .  If you want to set authentication timeout to a value other than the default settings, select <b>Use Manual Settings</b> then fill your preferred values in the fields that follow. Otherwise, select <b>Use Default Settings</b> to use the default settings displayed below.
Lease Time	This field is not available if the user type is <b>user</b> .  Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator.
Reauthentication Time	This field is not available if the user type is <b>user</b> .  Type the number of minutes this user can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike <b>Lease Time</b> , the user has no opportunity to renew the session without logging out.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

## 11.3 Setting

This screen controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User > Setting**.

**Figure 66** Configuration > Object > User > Setting

**User Default Setting**

**Default Authentication Timeout Settings**

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	user	-	-

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

**User Logon Settings**

☒ Limit the number of simultaneous logons for administration account

Maximum number per administration account:  (1-64)

**User Logout Settings**

☒ Enable logon retry limit

Maximum retry count:  (1-99)

Lockout period:  (1-5535 minutes)

The following table describes the labels in this screen.

**Table 37** Configuration > Object > User > Setting

LABEL	DESCRIPTION
User Default Setting	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the Zyxel Device supports. <ul style="list-style-type: none"> <li><b>admin</b> - this user can look at and change the configuration of the Zyxel Device</li> <li><b>limited-admin</b> - this user can look at the configuration of the Zyxel Device but not to change it</li> <li><b>user</b> - this is used for embedded RADIUS server and SNMPv3 user access</li> </ul>
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out.  Admin users renew the session every time the main screen refreshes in the Web Configurator.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike <b>Lease Time</b> , the user has no opportunity to renew the session without logging out.
User Logon Settings	

Table 37 Configuration &gt; Object &gt; User &gt; Setting (continued)

LABEL	DESCRIPTION
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when <b>Limit ... for administration account</b> is checked. Type the maximum number of simultaneous logins by each admin user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when <b>Enable logon retry limit</b> is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified <b>lockout period</b> . The number must be between 1 and 99.
Lockout period	This field is effective when <b>Enable logon retry limit</b> is checked. Type the number of minutes the user must wait to try to login again, if <b>logon retry limit</b> is enabled and the <b>maximum retry count</b> is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click <b>Apply</b> to save the changes.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

### 11.3.1 Edit User Authentication Timeout Settings

This screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User > Setting** screen, select one of the **Default Authentication Timeout Settings** entry and click the **Edit** icon.

Figure 67 User &gt; Setting &gt; Edit User Authentication Timeout Settings

**Edit User Authentication Timeout Settings**

User Type: admin

Lease Time:  (0-1440 minutes, 0 is unlimited)

Reauthentication Time:  (0-1440 minutes, 0 is unlimited)

OK Cancel



The following table describes the labels in this screen.

Table 38 User > Setting > Edit User Authentication Timeout Settings

LABEL	DESCRIPTION
User Type	<p>This read-only field identifies the type of user account for which you are configuring the default settings.</p> <ul style="list-style-type: none"> <li>• <b>admin</b> - this user can look at and change the configuration of the Zyxel Device.</li> <li>• <b>limited-admin</b> - this user can look at the configuration of the Zyxel Device but not to change it.</li> </ul>
Lease Time	<p>Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited.</p> <p>Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the <b>Renew</b> button on their screen. If you allow access users to renew time automatically, the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.</p>
Reauthentication Time	<p>Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike <b>Lease Time</b>, the user has no opportunity to renew the session without logging out.</p>
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

# CHAPTER 12

## AP Profile

### 12.1 Overview

This chapter shows you how to configure preset profiles for the Zyxel Device.

#### 12.1.1 What You Can Do in this Chapter

- The **Radio** screen ([Section 12.2 on page 100](#)) creates radio configurations that can be used by the APs.
- The **SSID** screen ([Section 12.3 on page 106](#)) configures three different types of profiles for your networked APs.

#### 12.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

##### Wireless Profiles

At the heart of all wireless AP configurations on the Zyxel Device are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 64 radio profiles on the Zyxel Device.
- **SSID** - This profile type defines the properties of a single WiFi network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 64 SSID profiles on the Zyxel Device.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a WiFi client to associate itself with the SSID. You can have a maximum of 64 security profiles on the Zyxel Device.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on WiFi client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 64 MAC filtering profiles on the Zyxel Device.
- **Layer 2 Isolation** - This profile defines the MAC addresses of the devices that you want to allow the associated WiFi clients to have access to when layer-2 isolation is enabled.

##### SSID

The SSID (Service Set Identifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the WiFi network that clients use to connect to it.

## **WEP**

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

## **WPA2**

WPA2 (IEEE 802.11i) is a WiFi security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA2 and WEP are improved data encryption and user authentication.

## **WPA3**

WPA3 is a WiFi security standard based on IEEE 802.11i, with security improvements like adopting enhanced PSK (Pre-Shared Key) authentication mechanism.

## **Personal vs Enterprise**

A secure WiFi connection relies on WiFi encryption and authentication. There are two authentication modes: Personal and Enterprise.

Personal mode requires a password called Pre-Shared Key (PSK). Users enter the same PSK to connect to the WiFi network.

Enterprise mode requires an external RADIUS server for authentication. Authentication of user identity is required to connect to the WiFi network.

## **IEEE 802.1X**

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

## **IEEE 802.11k/ v Assisted Roaming**

IEEE 802.11k is a standard for radio resource management of wireless LANs, which allows clients to request neighbor lists from the connected AP and discover the best available AP when roaming. An 802.11k neighbor list can contain up to six BSSIDs with the highest RCPI (Received Channel Power Indicator) value in both bands (5 GHz and 2.4 GHz, in the ratio of 4:2).

The IEEE 802.11v BSS Transition Management feature lets an AP automatically provide load information of the neighbor APs to clients. It helps the Zyxel Device steer clients to a suitable AP for better performance or load balancing.

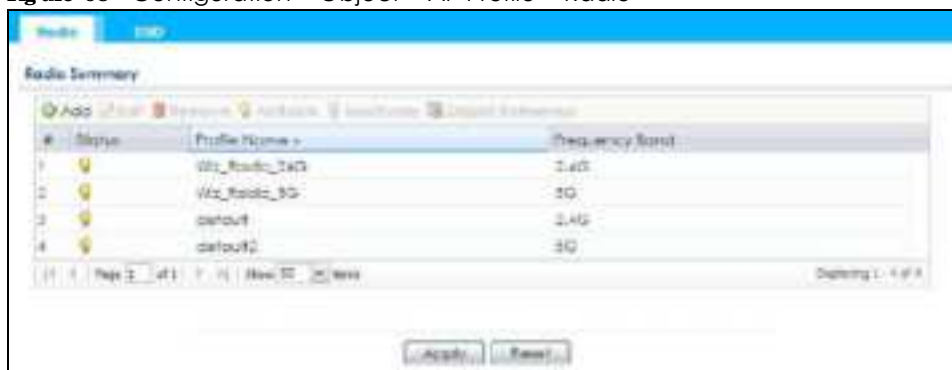
Note:

## 12.2 Radio

This screen allows you to create radio profiles for the Zyxel Device. A radio profile is a list of settings that an Zyxel Device can use to configure its radio transmitter(s). To access this screen click **Configuration > Object > AP Profile**.

Note: You can have a maximum of 32 radio profiles on the Zyxel Device.

**Figure 68** Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

Table 39 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click <b>Activate</b> .
Inactivate	To turn off an entry, select it and click <b>Inactivate</b> .
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific user.
Status	This field shows whether or not the entry is activated. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

### 12.2.1 Add/ Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

**Figure 69** Configuration > Object > AP Profile > Radio > Add/Edit

**Add Radio Profile**

☐ Hide Advanced Settings

**General Settings**

☒ Activate

Profile Name:

802.11 Band: ☐ 2.4G ☐ 5G

802.11 mode:

Channel Width:

Channel Selection: ☒ DFS ☐ Manual

☐ Enable DFS Client Aware

2.4 GHz Channel Selection Method:

2.4 GHz Channel Deployment:

**Time Interval**

☒ Schedule

Start Time:

Week Day: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

**Advanced Settings**

☒ Enable A-MPDU Aggregation

☒ Enable A-MSDU Aggregation

Set RTS Threshold:  (5-2347)

Set Fragment Threshold:  (4096-10000)

Set Signal Threshold:  (1-2357)

Disassociate Station Threshold:  (30s-10s)

Disassociate Aggressiveness:

☐ Allow 802.11p/802.11s stations only

☒ Enable 802.11s

**Multicast Settings**

Transmission Mode: ☒ Multicast to unicast ☐ Feed Multicast Rate

Multicast Rate (Mbps):

Maximum WLAN Rate Control Setting:

The following table describes the labels in this screen.

**Table 40** Configuration > Object > AP Profile > Radio > Add/Edit

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the <b>Advanced Settings</b> in this window.
<b>General Settings</b>	
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
802.11 Band	Select whether this radio would use the 2.4 GHz or 5 GHz band.

Table 40 Configuration &gt; Object &gt; AP Profile &gt; Radio &gt; Add/Edit (continued)

LABEL	DESCRIPTION
802.11 Mode	<p>Select how to let wireless clients connect to the AP.</p> <p>If <b>802.11 Band</b> is set to <b>2.4G</b>:</p> <ul style="list-style-type: none"> <li>• <b>11b/g</b>: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The Zyxel Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.</li> <li>• <b>11n</b>: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Zyxel Device.</li> <li>• <b>11ax</b>: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on.</li> </ul> <p>If <b>802.11 Band</b> is set to <b>5G</b>:</p> <ul style="list-style-type: none"> <li>• <b>11a</b>: allows only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device.</li> <li>• <b>11n</b>: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the Zyxel Device.</li> <li>• <b>11ac</b>: allows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ac, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on.</li> <li>• <b>11ax</b>: allows IEEE802.11n, IEEE802.11a, IEEE802.11ac, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11ac, and so on.</li> </ul>
Channel Width	<p>Select the channel bandwidth you want to use for your wireless network.</p> <p>Select <b>20 MHz</b> if you want to lessen radio interference with other wireless devices in your neighborhood.</p> <p>Select <b>20/ 40 MHz</b> to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference.</p> <p>Select <b>20/ 40/ 80</b> to allow the Zyxel Device to choose the channel bandwidth (20 or 40 or 80) that has least interference. This option is available only when you select <b>11ac</b> or <b>11ax</b> in the <b>802.11 Mode</b> field.</p> <p>Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth.</p>
Channel Selection	<p>This is the radio channel which the signal will use for broadcasting by this radio profile.</p> <ul style="list-style-type: none"> <li>• <b>DCS</b>: Choose Dynamic Channel Selection to have the Zyxel Device choose a radio channel that has least interference.</li> <li>• <b>Manual</b>: Choose from the available radio channels in the list. If your Zyxel Device is outdoor type, be sure to choose non-indoors channels.</li> </ul>
Enable DCS Client Aware	<p>This field is available when you set <b>Channel Selection</b> to <b>DCS</b>.</p> <p>Select this to have the Zyxel Device switch channels only when there are no clients connected to it. If there is a client connected, the Zyxel Device will not switch channels but generate a log. The Zyxel Device tries to scan and switch channels again at the end of the specified time interval or at the scheduled time.</p> <p>If you disable this then the Zyxel Device switches channels immediately regardless of any client connections. In this instance, clients that are connected to the Zyxel Device are dropped when it switches channels.</p>

Table 40 Configuration &gt; Object &gt; AP Profile &gt; Radio &gt; Add/Edit (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Selection Method	<p>This field is available when you set <b>Channel Selection</b> to <b>DCS</b>.</p> <p>Select how you want to specify the channels the Zyxel Device switches between for 2.4 GHz operation.</p> <p>Select <b>auto</b> to have the Zyxel Device display a <b>2.4 GHz Channel Deployment</b> field you can use to limit channel switching to 3 or 4 channels.</p> <p>Select <b>manual</b> to select the individual channels the Zyxel Device switches between.</p> <p>Note: The method is automatically set to <b>auto</b> when no channel is selected or any one of the previously selected channels is not supported.</p>
Channel ID	<p>This field is available only when you set <b>Channel Selection</b> to <b>DCS</b> and set <b>2.4 GHz Channel Selection Method</b> to <b>manual</b>.</p> <p>Select the channels that you want the Zyxel Device to use.</p>
2.4 GHz Channel Deployment	<p>This is available when you set <b>Channel Selection</b> to <b>DCS</b> and the <b>2.4 GHz Channel Selection Method</b> is set to <b>auto</b>.</p> <p>Select <b>Three-Channel Deployment</b> to limit channel switching to channels 1, 6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels.</p> <p>Select <b>Four-Channel Deployment</b> to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.</p>
Avoid 5G DFS Channel	<p>This field is available only when you set <b>802.11 Band</b> to <b>5G</b>, <b>Channel Selection</b> to <b>DCS</b> and <b>5 GHz Channel Selection Method</b> to <b>auto</b>.</p> <p>Dynamic Frequency Selection (DFS) is a WiFi channel allocation scheme that allows APs to use channels in the 5 GHz band normally reserved for radar. Before using a DFS channel, an AP must ensure there is no radar present by performing a Channel Availability Check (CAC). This check takes 1-10 minutes, depending on the country in which the AP is located.</p> <p>Select this if you don't want to wait for the Zyxel Device to perform a CAC before using a channel by forcing the Zyxel Device to only use the non-DFS channels.</p> <p>Clear this to allow the Zyxel Device to use the DFS channels for more channel options. The Zyxel Device only switches to a DFS channel when a nearby AP is broadcasting the same SSID the Zyxel Device uses. This allows WiFi clients to switch to connect to the same SSID on another AP when the Zyxel Device is under the CAC process before switching to a DFS channel.</p>
5 GHz Channel Selection Method	<p>Select how you want to specify the channels the Zyxel Device switches between for 5 GHz operation.</p> <p>Select <b>Auto</b> to have the Zyxel Device automatically select the best channel.</p> <p>Select <b>manual</b> to select the individual channels the Zyxel Device switches between.</p> <p>Note: The method is automatically set to <b>auto</b> when no channel is selected or any one of the previously selected channels is not supported.</p>
Channel ID	<p>This field is available only when you set <b>Channel Selection</b> to <b>DCS</b> and set <b>5 GHz Channel Selection Method</b> to <b>manual</b>.</p> <p>Select the channels that you want the Zyxel Device to use.</p>
Time Interval	<p>Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.</p>

Table 40 Configuration &gt; Object &gt; AP Profile &gt; Radio &gt; Add/Edit (continued)

LABEL	DESCRIPTION
DCS Time Interval	<p>This field is available when you set <b>Channel Selection</b> to <b>DCS</b> and select the <b>Time Interval</b> option.</p> <p>Enter a number of minutes. This regulates how often the Zyxel Device surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the Zyxel Device will then dynamically select the next available clean channel or a channel with lower interference.</p>
Schedule	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at a specific time on selected days of the week.
Start Time	Specify the time of the day (in 24-hour format) to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Week Days	Select each day of the week to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Advanced Settings	
Guard Interval	<p>This field is available only when the channel width is <b>20 MHz</b>, <b>20/40MHz</b> or <b>20/40/80MHz</b> and the <b>802.11 Mode</b> is either <b>11n</b> or <b>11ac</b>.</p> <p>Set the guard interval for this radio profile to either <b>short</b> or <b>long</b>.</p> <p>The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.</p>
Enable A-MPDU Aggregation	<p>This field is not available when you set <b>802.11 Mode</b> to <b>11a</b> or <b>11b/g</b>.</p> <p>Select this to enable A-MPDU aggregation.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p>
Enable A-MSDU Aggregation	<p>This field is not available when you set <b>802.11 Mode</b> to <b>11a</b> or <b>11b/g</b>.</p> <p>Select this to enable A-MSDU aggregation.</p> <p>Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.</p>
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the WiFi network if you have WiFi clients that are associated with the same AP but out of range of one another. When enabled, a WiFi client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops WiFi clients from transmitting packets at the same time (and causing data collisions).</p> <p>A WiFi client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the <b>Fragmentation Threshold</b> to turn RTS/CTS off.</p>
Fragmentation Threshold	<p>This field is only available when you set <b>802.11 Mode</b> to <b>11a</b> or <b>11b/g</b>.</p> <p>A fragmentation threshold is the maximum data fragment size (between 256 and 2436 bytes) that can be sent in the WiFi network before the AP will fragment the packet into smaller data frames.</p> <p>A large fragmentation threshold is recommended for networks not prone to interference. A smaller threshold is recommended for busy networks or networks that are prone to interference.</p>



Table 40 Configuration &gt; Object &gt; AP Profile &gt; Radio &gt; Add/Edit (continued)

LABEL	DESCRIPTION
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the Zyxel Device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Enable Signal Threshold	<p>Select the check box to use the signal threshold to ensure WiFi clients receive good throughput. This allows only WiFi clients with strong signals to connect to the Zyxel Device. The Zyxel Device will disconnect WiFi clients with signal strengths lower than the <b>Disassociate Station Threshold</b> you specify.</p> <p>Clear the check box to not require WiFi clients to have a minimum signal strength to keep their connections with the Zyxel Device.</p>
Disassociate Station Threshold	<p>Set a minimum kick-off signal strength. You can set from -20dBm (the strongest signal) to -105dBm (the weakest signal).</p> <p>When a WiFi client's signal strength is lower than the specified threshold, the Zyxel Device checks the traffic between the Zyxel Device and the WiFi client. The Zyxel Device will only disconnect the WiFi client when</p> <ul style="list-style-type: none"> <li>the WiFi client signal strength falls below the kick-off strength and</li> <li>the WiFi client's traffic throughput is below a minimum threshold.</li> </ul> <p>You can set the WiFi client's minimum traffic throughput threshold in <b>Disassociate Aggressiveness</b>.</p>
Disassociate Aggressiveness	<p>Set the minimum traffic throughput threshold here.</p> <p><b>High:</b> Select this if you want the Zyxel Device to not disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is heavy. The Zyxel Device will disconnect the WiFi client if the traffic between the Zyxel Device and the WiFi client is medium or low.</p> <p><b>Standard:</b> Select this if you want the Zyxel Device to not disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is medium. The Zyxel Device will disconnect the WiFi client if the traffic between the Zyxel Device and the WiFi client is low.</p> <p><b>Low:</b> Select this if you want the Zyxel Device to not disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is low. At the time of writing, the Zyxel Device will disconnect the WiFi client if there's no packet sent between the Zyxel Device and the WiFi client in one second.</p>
Allow 802.11n/ac/ax stations only	Select this option to allow only 802.11 n/ac/ax clients to connect, and reject 802.11a/b/g clients.
Blacklist DFS channels in presence of radar	<p>This field is available if <b>802.11 Band</b> is set to <b>5G</b> and <b>Channel Selection</b> is set to <b>DCS</b>.</p> <p>Enable this to temporarily blacklist the wireless channels in the Dynamic Frequency Selection (DFS) range whenever a radar signal is detected by the Zyxel Device.</p>
Enable 802.11d	<p>Clear the checkbox to prevent the AP from broadcasting a country code, also called a country Information Element (IE), in beacon frames. This makes the AP incompatible with 802.11d networks and devices.</p> <p>802.11d is a WiFi network specification that allows the AP to broadcast a country code to WiFi client. The country code indicates where the AP is located. If WiFi clients are unable to connect to the AP due to an incompatible country code, you should disable 802.11d.</p>
Multicast Settings	

Table 40 Configuration &gt; Object &gt; AP Profile &gt; Radio &gt; Add/Edit (continued)

LABEL	DESCRIPTION
Transmission Mode	<p>Specify how the Zyxel Device handles wireless multicast traffic.</p> <p>Select <b>Multicast to Unicast</b> to broadcast wireless multicast traffic to all of the WiFi clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets.</p> <p>Select <b>Fixed Multicast Rate</b> to send multicast traffic to all WiFi clients at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.</p>
Multicast Rate(Mbps)	<p>If you set <b>Transmission Mode</b> to <b>Fixed Multicast Rate</b>, select a data rate at which the Zyxel Device transmits multicast packets to WiFi clients. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.</p>
Minimum WLAN Rate Control Setting	<p>Sets the minimum data rate that 2.4Ghz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54.</p> <p>Sets the minimum data rate that 5Ghz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 6, 9, 12, 18, 24, 36, 48, 54.</p> <p>Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.</p>
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

## 12.3 SSID

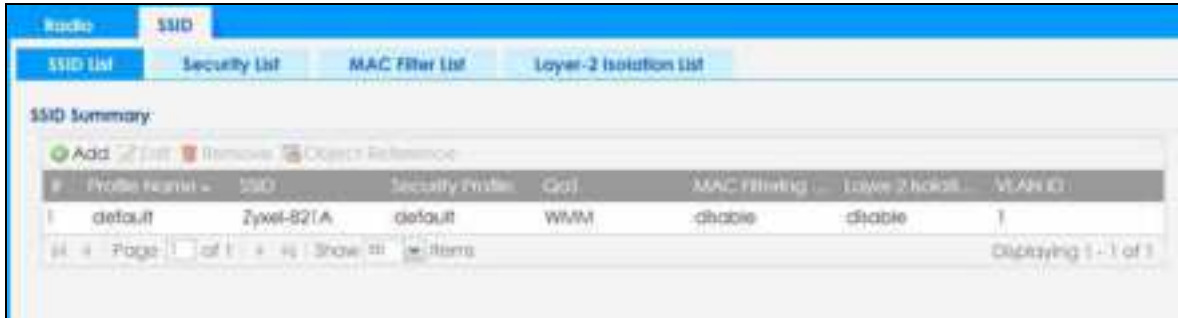
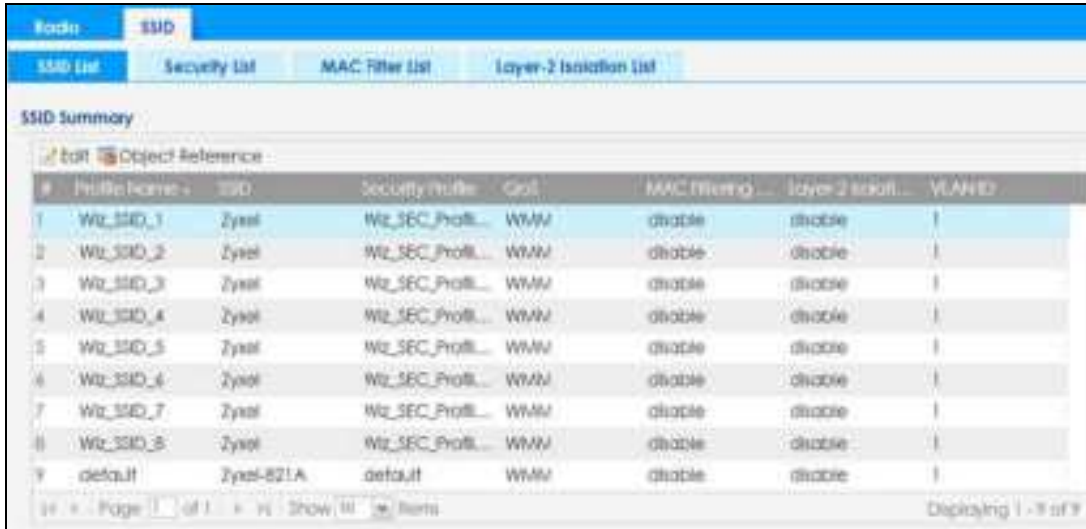
The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing WiFi clients to connect to them; and a MAC filter list, which can limit connections to an AP based on WiFi clients MAC addresses.

### 12.3.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set Identifier, is basically the name of the WiFi network to which a WiFi client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the WiFi network name when a person makes a connection to it.

To access this screen, click **Configuration > Object > AP Profile > SSID > SSID List**.

Note: You cannot add or remove an SSID profile after running the setup wizard.

**Figure 70** Configuration > Object > AP Profile > SSID > SSID List (Default)**Figure 71** Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)

The following table describes the labels in this screen.

**Table 41** Configuration > Object > AP Profile > SSID > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile. This button is not available after you configure the Zyxel Device using the wizard.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile. This button is not available after you configure the Zyxel Device using the wizard.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to WiFi clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.
MAC Filtering Profile	This field indicates which (if any) MAC filter Profile is associated with the SSID profile.
Layer-2 Isolation Profile	This field indicates which (if any) layer-2 isolation Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

### 12.3.2 Add/ Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the **Add** button or select a SSID profile from the list and click the **Edit** button.

**Figure 72** Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile

The following table describes the labels in this screen.

Table 42 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to WiFi clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	<p>Select a security profile from this list to associate with this SSID. If none exist, you can use the <b>Create new Object</b> menu to create one.</p> <p>It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.</p>

Table 42 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; SSID List &gt; Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	<p>Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the <b>Create new Object</b> menu to create one.</p> <p>MAC filtering allows you to limit the WiFi clients connecting to your network through a particular SSID by WiFi client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections.</p> <p>The <b>disable</b> setting means no MAC filtering is used.</p>
Layer-2 Isolation Profile	<p>Select a layer-2 isolation profile from the list to associate with this SSID. If none exist, you can use the <b>Create new Object</b> menu to create one.</p> <p>Layer-2 isolation allows you to prevent WiFi clients associated with your Zyxel Device from communicating with other WiFi clients, APs, computers or routers in a network.</p> <p>The <b>disable</b> setting means no layer-2 isolation is used.</p>
QoS	<p>Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a WiFi network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets.</p> <p>QoS access categories are as follows:</p> <p><b>WMM:</b> Enables automatic tagging of data packets. The Zyxel Device assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such.</p> <p><b>WMM_VOICE:</b> All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls.</p> <p><b>WMM_VIDEO:</b> All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing.</p> <p><b>WMM_BEST EFFORT:</b> All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet.</p> <p><b>WMM_BACKGROUND:</b> All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.</p>
Rate Limiting (Per Station Traffic Rate)	
Downlink	Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis. The range is from 0–160. Enter 0 to set the maximum rate to unlimited.
Uplink	Define the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis. The range is from 0–160. Enter 0 to set the maximum rate to unlimited.
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID. The range is from 1–4094.
Hidden SSID	<p>Select this if you want to "hide" your SSID from WiFi clients. This tells any WiFi clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all WiFi clients respect this flag and display it anyway.</p> <p>When a SSID is "hidden" and a WiFi client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your WiFi connection setup screen(s) (these vary by client, client connectivity software, and operating system).</p>
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same BSSID on the Zyxel Device.
Enable U-APSD	Select this option to enable Unscheduled Automatic Power Save Delivery (U-APSD), which is also known as WMM-Power Save. This helps increase battery life for battery-powered WiFi clients connected to the Zyxel Device using this SSID profile.

Table 42 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; SSID List &gt; Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
802.11k/v Assisted Roaming	Select this option to enable IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming.
Schedule SSID	Select this option and set whether the SSID is enabled or disabled on each day of the week. You also need to select the hour and minute (in 24-hour format) to specify the time period of each day during which the SSID is enabled/enabled.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

## 12.4 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

Note: You can have a maximum of 32 security profiles on the Zyxel Device.

Figure 73 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List



The following table describes the labels in this screen.

Table 43 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List

LABEL	DESCRIPTION
Add	Click this to add a new security profile. This button is not available after you configure the Zyxel Device using the wizard.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile. This button is not available after you configure the Zyxel Device using the wizard.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

### 12.4.1 Add/ Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

These screens' options change based on the **Security Mode** selected.

Note: Not all Zyxel Devices support the enterprise authentication settings and radius settings; see [Table 1 on page 12](#) for more information.

**Figure 74** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: none

The following table describes the labels in this screen.

Table 44 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: none

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Enterprise	Select this to enable 802.1X secure authentication with a RADIUS server.

Table 44 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: none (continued)

LABEL	DESCRIPTION
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Advance  Note: Click on the <b>Show Advanced Settings</b> button to show the fields describe below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Radius Settings	
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external authentication server.  Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.



**Figure 75** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced-open

The following table describes the labels in this screen.

Table 45 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced- open

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Transition Mode	This option only displays if you set the <b>Security Mode</b> to <b>wpa3</b> or <b>enhanced-open</b> . This option is always enabled for backwards compatibility. This creates two virtual APs (VAPs) with a primary ( <b>wpa3</b> or <b>enhanced-open</b> ) and fallback ( <b>wpa2</b> or <b>none</b> ) security method.
Advance	
Note: Click on the <b>Show Advanced Settings</b> button to show the fields described below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.

Table 45 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: enhanced- open (continued)

LABEL	DESCRIPTION
Management Frame Protection	<p>This field is configurable only when you select <b>wpa2</b> in the <b>Security Mode</b> field and set <b>CipherType</b> to <b>aes</b>.</p> <p>Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks.</p> <p>Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. This option is always enabled if you select <b>enhanced-open</b> or <b>WPA3</b> as the <b>Security Mode</b>.</p> <p>If <b>Optional</b> is selected, WiFi clients will not be required to support MFP. Management frames will be encrypted if the clients support MFP.</p> <p>If <b>Required</b> is selected, WiFi clients must support MFP in order to join the Zyxel Device's WiFi network.</p>
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

**Figure 76** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep

**Edit Security Profile default**

☐ Hide Advanced Settings

**General Settings**

Profile Name: default

Security Mode: wep

**Authentication Settings**

☒ Enterprise

ReAuthentication Timer: 0 (30-30000 seconds, 0 is unlimited)

Authentication Type: open

Key Length: WEP-64

44-bit: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F) for each Key (1-4).  
 128-bit: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F) for each Key (1-4).

Key 1:

Key 2:

Key 3:

Key 4:

☒ Advance

Idle Timeout: 300 (30-30000 seconds)

**Radius Settings**

☒ Primary Radius Server Activate

Radius Server IP Address:

Radius Server Port:  (1~65535)

Radius Server Secret:

☐ Secondary Radius Server Activate

☐ Primary Accounting Server Activate

☐ Secondary Accounting Server Activate

General Server Settings

NAS IP Address:  (Optional)

NAS Identifier:  (Optional)

OK Cancel

The following table describes the labels in this screen.

**Table 46** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.

Table 46 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: wep (continued)

LABEL	DESCRIPTION
Authentication Settings	
Enterprise	Select this to enable 802.1X secure authentication with a RADIUS server.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Authentication Type	Select a WEP authentication method. Choices are <b>Open</b> or <b>Share</b> key.
Key Length	<p>Select the bit-length of the encryption key to be used in WEP connections.</p> <p>If you select <b>WEP-64</b>:</p> <ul style="list-style-type: none"> <li>Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each <b>Key</b> used.</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each <b>Key</b> used.</li> </ul> <p>If you select <b>WEP-128</b>:</p> <ul style="list-style-type: none"> <li>Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each <b>Key</b> used.</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each <b>Key</b> used.</li> </ul>
Key 1~4	Based on your <b>Key Length</b> selection, enter the appropriate length hexadecimal or ASCII key.
Advance	
Note: Click on the <b>Show Advanced Settings</b> button to show the fields describe below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Radius Settings	
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	<p>This field is available only when you enable user accounting through an external authentication server.</p> <p>Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.</p>

Table 46 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep (continued)

Label	Description
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

Figure 77 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2

The following table describes the labels in this screen.

Table 47 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Enterprise	Select this to enable 802.1X secure authentication with a RADIUS server.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Personal	This field is available when you select the <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> security mode.  Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Advance	
Note: Click on the <b>Show Advanced Settings</b> button to show the fields describe below.	
Cipher Type	Select an encryption cipher type from the list.  <ul style="list-style-type: none"> <li><b>auto</b> - This automatically chooses the best available cipher based on the cipher in use by the WiFi client that is attempting to make a connection.</li> <li><b>aes</b> - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all WiFi clients may support this.</li> </ul>
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
Management Frame Protection	This field is configurable only when you select <b>wpa2</b> in the <b>Security Mode</b> field and set <b>Cipher Type</b> to <b>aes</b> .  Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks.  Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. This option is always enabled if you select <b>enhanced-open</b> or <b>WPA3</b> as the <b>Security Mode</b> .  If <b>Optional</b> is selected, WiFi clients will not be required to support MFP. Management frames will be encrypted if the clients support MFP.  If <b>Required</b> is selected, WiFi clients must support MFP in order to join the Zyxel Device's WiFi network.
Radius Settings	

Table 47 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: wpa2 (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external authentication server.  Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

**Figure 78** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix

**Edit Security Profile WIZ\_SEC\_Profile\_1**

☐ Hide Advanced Settings

**General Settings**

Profile Name: WIZ\_SEC\_Profile\_1

Security Mode: wpa2-mix

**Authentication Settings**

☒ Enterprise

ReAuthentication Timer: 30 (30-30000 seconds, 0 is unlimited)

☐ Personal

☒ Advanced

Client Type: auto

Idle Timeout: 300 (30-30000 seconds)

Group Key Update Timer: 30000 (30-30000 seconds)

**Radius Settings**

☒ Primary Radius Server Activate

Radius Server IP Address: [Red Error]

Radius Server Port: [Red Error] (1-65535)

Radius Server Secret: [Red Error]

☐ Secondary Radius Server Activate

☒ Primary Accounting Server Activate

Accounting Server IP Address: [Red Error]

Accounting Server Port: [Red Error] (1-65535)

Accounting Share Secret: [Red Error]

☐ Secondary Accounting Server Activate

☒ Accounting Interim Update

Interim Update Interval: 10 (1-1440 minutes)

**General Server Settings:**

NAS IP Address: [Optional]

NAS Identifier: [Optional]

OK Cancel

The following table describes the labels in this screen.

**Table 48** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	



Table 48 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: wpa2-mix (continued)

Label	Description
Enterprise	Select this to enable 802.1X secure authentication with a RADIUS server.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Personal	This field is available when you select the <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> security mode.  Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Advance	
Note: Click on the <b>Show Advanced Settings</b> button to show the fields describe below.	
Cipher Type	Select an encryption cipher type from the list. <ul style="list-style-type: none"> <li><b>auto</b> - This automatically chooses the best available cipher based on the cipher in use by the WiFi client that is attempting to make a connection.</li> <li><b>aes</b> - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all WiFi clients may support this.</li> </ul>
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
Radius Settings	
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external authentication server.  Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.

Table 48 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: wpa2-mix (continued)

LABEL	DESCRIPTION
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

**Figure 79** Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3

**Edit Security Profile WIZ\_SEC\_Profile\_1**

☐ Hide Advanced Settings

**General Settings**

Profile Name: WIZ\_SEC\_Profile\_1

Security Mode: wpa3

**Authentication Settings**

☒ Enterprise

ReAuthentication Timer: 30 (30~30000 seconds, 0 is unlimited)

☐ Personal

☒ Advance

Idle timeout: 300 (30~30000 seconds)

Group Key Update Timer: 30000 (30~30000 seconds)

☒ Management Frame Protection ☒ Optional ☐ Required

**Radius Settings**

☒ Primary Radius Server Activate

Radius Server IP Address: [Redacted]

Radius Server Port: [Redacted] (1~65535)

Radius Server Secret: [Redacted]

☐ Secondary Radius Server Activate

☒ Primary Accounting Server Activate

Accounting Server IP Address: [Redacted]

Accounting Server Port: [Redacted] (1~65535)

Accounting Share Secret: [Redacted]

☐ Secondary Accounting Server Activate

☒ Accounting Interim Update

Interim Update Interval: 10 (1~1440 minutes)

**General Server Settings**

NAS IP Address: [Redacted] (Optional)

NAS Identifier: [Redacted] (Optional)

OK Cancel

The following table describes the labels in this screen.

Table 49 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: <b>none</b> , <b>enhanced-open</b> , <b>wep</b> , <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> .  <b>enhanced-open</b> uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Enterprise	Select this to enable 802.1X secure authentication with a RADIUS server.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Personal	This field is available when you select the <b>wpa2</b> , <b>wpa2-mix</b> or <b>wpa3</b> security mode.  Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Transition Mode	This option only displays if you set the <b>Security Mode</b> to <b>wpa3</b> or <b>enhanced-open</b> . This option is always enabled for backwards compatibility. This creates two virtual APs (VAPs) with a primary ( <b>wpa3</b> or <b>enhanced-open</b> ) and fallback ( <b>wpa2</b> or <b>none</b> ) security method.
Advance	
Note: Click on the <b>Show Advanced Settings</b> button to show the fields describe below.	
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
Management Frame Protection	This field is configurable only when you select <b>wpa2</b> in the <b>Security Mode</b> field and set <b>CipherType</b> to <b>aes</b> .  Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks.  Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. This option is always enabled if you select <b>enhanced-open</b> or <b>WPA3</b> as the <b>Security Mode</b> .  If <b>Optional</b> is selected, WiFi clients will not be required to support MFP. Management frames will be encrypted if the clients support MFP.  If <b>Required</b> is selected, WiFi clients must support MFP in order to join the Zyxel Device's WiFi network.
Radius Settings	
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.

Table 49 Configuration &gt; Object &gt; AP Profile &gt; SSID &gt; Security List &gt; Add/Edit Security Profile&gt; Security Mode: wpa3 (continued)

Label	Description
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external authentication server.  Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

## 12.5 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Note: You can have a maximum of 32 MAC filtering profiles on the Zyxel Device.

**Figure 80** Configuration > Object > AP Profile > SSID > MAC Filter List

The following table describes the labels in this screen.

**Table 50** Configuration > Object > AP Profile > SSID > MAC Filter List

LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

### 12.5.1 Add/ Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Note: Each MAC filtering profile can include a maximum of 512 MAC addresses.

**Figure 81** Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile

The following table describes the labels in this screen.

Table 51 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select <b>allow</b> to permit the WiFi client with the MAC addresses in this profile to connect to the network through the associated SSID; select <b>deny</b> to block the WiFi clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

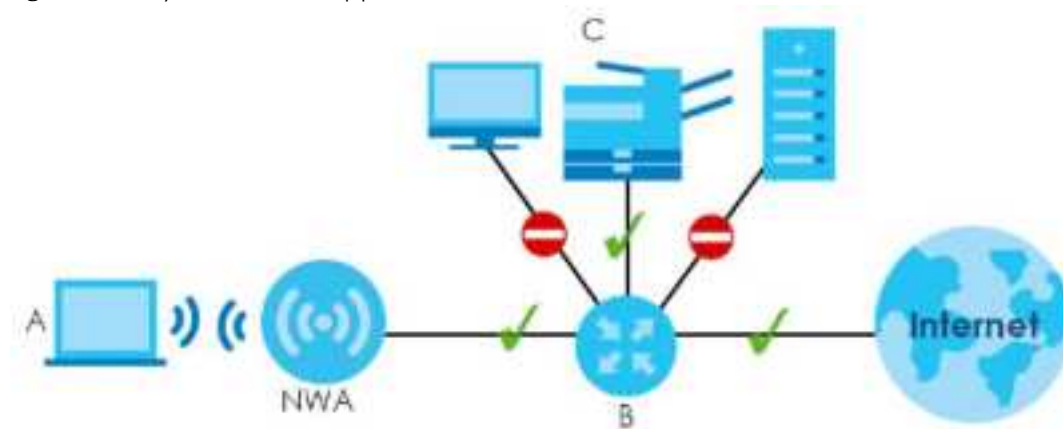
## 12.6 Layer-2 Isolation List

Layer-2 isolation is used to prevent WiFi clients associated with your Zyxel Device from communicating with other WiFi clients, APs, computers or routers in a network.

In the following example, layer-2 isolation is enabled on the Zyxel Device to allow a guest WiFi client (**A**) to access the main network router (**B**). The router provides access to the Internet and the network printer (**C**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other WiFi clients only if Intra-BSS Traffic blocking is disabled.

Note: Intra-BSS Traffic Blocking is activated when you enable layer-2 isolation.

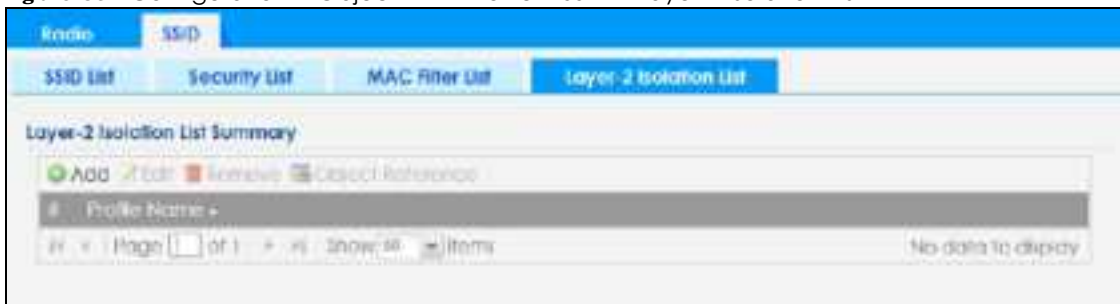
Figure 82 Layer-2 Isolation Application



MAC addresses that are not listed in the layer-2 isolation table are blocked from communicating with the Zyxel Device's WiFi clients except for broadcast packets. Layer-2 isolation does not check the traffic between WiFi clients that are associated with the same AP. Intra-BSS traffic allows WiFi clients associated with the same AP to communicate with each other.

This screen allows you to specify devices you want the users on your WiFi networks to access. To access this screen click **Configuration > Object > AP Profile > SSID > Layer-2 Isolation List**.

**Figure 83** Configuration > Object > AP Profile > SSID > Layer-2 Isolation List



The following table describes the labels in this screen.

**Table 52** Configuration > Object > AP Profile > SSID > Layer-2 Isolation List

LABEL	DESCRIPTION
Add	Click this to add a new layer-2 isolation profile.
Edit	Click this to edit the selected layer-2 isolation profile.
Remove	Click this to remove the selected layer-2 isolation profile.
Object Reference	Click this to view which other objects are linked to the selected layer-2 isolation profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the layer-2 isolation profile.

### 12.6.1 Add/ Edit Layer-2 Isolation Profile

This screen allows you to create a new layer-2 isolation profile or edit an existing one. To access this screen, click the **Add** button or select a layer-2 isolation profile from the list and click the **Edit** button.

**Note:** You need to know the MAC address of each WiFi client, AP, computer or router that you want to allow to communicate with the Zyxel Device's WiFi clients.

**Figure 84** Configuration > Object > AP Profile > SSID > Layer-2 Isolation List > Add/Edit Layer-2 Isolation Profile

The following table describes the labels in this screen.

**Table 53** Configuration > Object > AP Profile > SSID > Layer-2 Isolation List > Add/Edit Layer-2 Isolation Profile

<b>LABEL</b>	<b>DESCRIPTION</b>
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.



# CHAPTER 13

## WDS Profile

### 13.1 Overview

This chapter shows you how to configure WDS (Wireless Distribution System) profiles for the Zyxel Device to form a WDS with other APs.

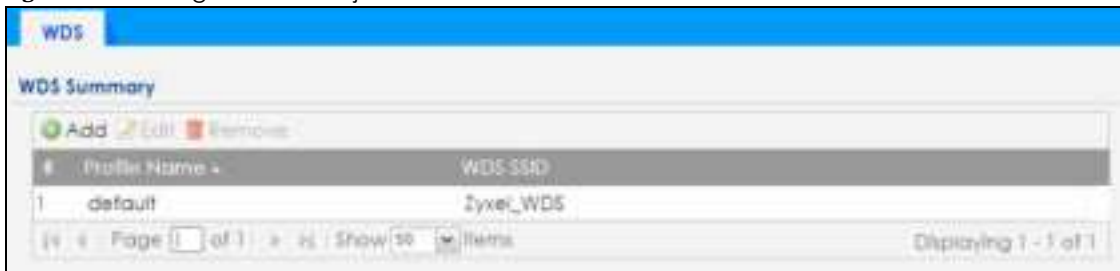
#### 13.1.1 What You Can Do in this Chapter

The **WDS Profile** screen ([Section 13.2 on page 129](#)) creates preset WDS configurations that can be used by the Zyxel Device.

### 13.2 WDS Profile

This screen allows you to manage and create WDS profiles that can be used by the APs. To access this screen, click **Configuration > Object > WDS Profile**.

**Figure 85** Configuration > Object > WDS Profile



The following table describes the labels in this screen.

**Table 54** Configuration > Object > WDS Profile

LABEL	DESCRIPTION
Add	Click this to add a new profile.
Edit	Click this to edit the selected profile.
Remove	Click this to remove the selected profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the profile.
WDS SSID	This field shows the SSID specified in this WDS profile.

### 13.2.1 Add/ Edit WDS Profile

This screen allows you to create a new WDS profile or edit an existing one. To access this screen, click the **Add** button or select an existing profile and click the **Edit** button.

**Figure 86** Configuration > Object > WDS Profile > Add/Edit WDS Profile

The following table describes the labels in this screen.

**Table 55** Configuration > Object > WDS Profile > Add/Edit WDS Profile

<b>LABEL</b>	<b>DESCRIPTION</b>
Profile Name	Enter up to 31 alphanumeric characters for the profile name.
WDS SSID	Enter the SSID with which you want the Zyxel Device to connect to a root AP or repeater to form a WDS.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. The key is used to encrypt the traffic between the APs.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to exit this screen without saving your changes.

# CHAPTER 14

## Certificates

### 14.1 Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

#### 14.1.1 What You Can Do in this Chapter

- The **My Certificates** screens ([Section 14.2 on page 134](#)) generate and export self-signed certificates or certification requests and import the Zyxel Device's CA-signed certificates.
- The **Trusted Certificates** screens ([Section 14.3 on page 141](#)) save CA certificates and trusted remote host certificates to the Zyxel Device. The Zyxel Device trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

#### 14.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else.

This process works as follows:

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Zyxel Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Zyxel Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

### **Advantages of Certificates**

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

### **Self-signed Certificates**

You can have the Zyxel Device act as a certification authority and sign its own certificates.

### **Factory Default Certificate**

The Zyxel Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

### **Certificate File Formats**

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

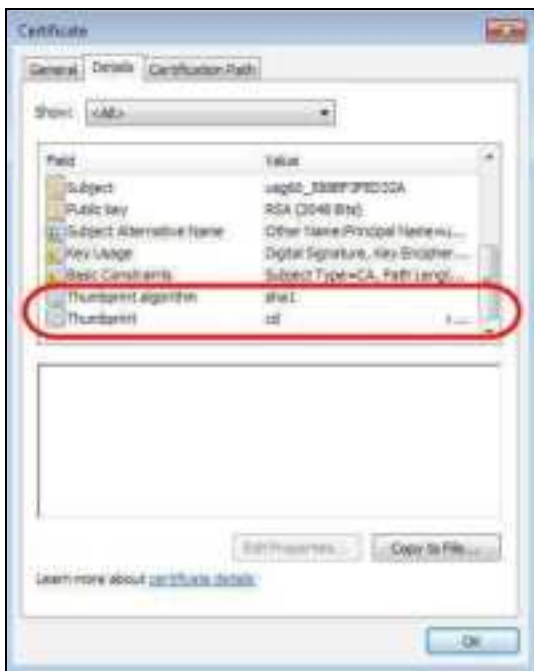
### 14.1.3 Verifying a Certificate

Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

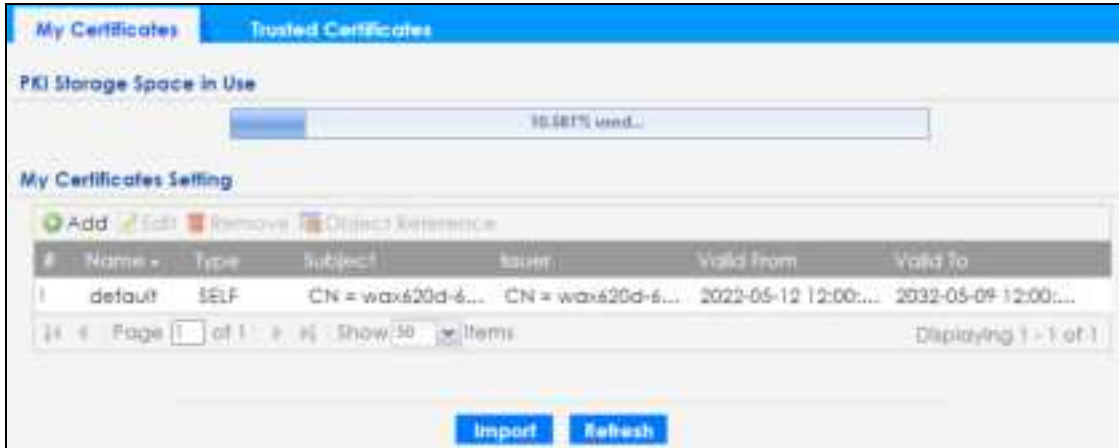


- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

## 14.2 My Certificates

Click **Configuration > Object > Certificate > My Certificates** to open this screen. This is the Zyxel Device's summary list of certificates and certification requests.

**Figure 87** Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

**Table 56** Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the Zyxel Device generate a certificate or a certification request.
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click <b>Remove</b> . The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click <b>Object Reference</b> to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is.  <b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.  <b>SELF</b> represents a self-signed certificate.  <b>CERT</b> represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

Table 56 Configuration &gt; Object &gt; Certificate &gt; My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click <b>Import</b> to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click <b>Refresh</b> to display the current validity status of the certificates.

### 14.2.1 Add My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **Add My Certificates** screen. Use this screen to have the Zyxel Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 88 Configuration &gt; Object &gt; Certificate &gt; My Certificates &gt; Add

**Add My Certificates**

**Configuration**

Name:

**Subject Information**

☒ Host IP Address

☐ Host Domain Name

☐ E-Mail

Organizational Unit:  (Optional)

Organization:  (Optional)

Town/City:  (Optional)

State/Province:  (Optional)

Country:  (Optional)

Key Type: RSA-SHA256

Key Length: 2048 bits

**Extended Key Usage**

☐ Server Authentication

☐ Client Authentication

☒ Create a self-signed certificate

☐ Create a certification request and save it locally for later manual enrollment

OK Cancel

The following table describes the labels in this screen.

Table 57 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',.- characters.
Subject Information	<p>Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a <b>Host IP Address</b>, <b>Host Domain Name</b>, or <b>E-Mail</b>. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.</p> <p>Select a radio button to identify the certificate's owner by IP address, domain name or email address. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An email address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p>
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	<p>The Zyxel Device uses the RSA (Rivest, Shamir and Adleman) public-key encryption algorithm. SHA1 (Secure Hash Algorithm) and SHA2 are hash algorithms used to authenticate packet data. SHA2-256 or SHA2-512 are part of the SHA2 set of cryptographic functions and they are considered even more secure than SHA1.</p> <p>Select a key type from <b>RSA-SHA256</b> and <b>RSA-SHA512</b>.</p>
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (1024 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	<p>Select <b>Server Authentication</b> to allow a web server to send clients the certificate to authenticate itself.</p> <p>Select <b>Client Authentication</b> to use the certificate's key to authenticate clients to the secure gateway.</p>
	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the Zyxel Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	<p>Select this to have the Zyxel Device generate and store a request for a certificate. Use the <b>My Certificate Edit</b> screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the <b>My Certificate Edit</b> screen and then send it to the certification authority.</p>



Table 57 Configuration &gt; Object &gt; Certificate &gt; My Certificates &gt; Add (continued)

LABEL	DESCRIPTION
OK	Click <b>OK</b> to begin certificate or certification request generation.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

If you configured the **Add My Certificates** screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **Add My Certificates** screen. Click **Return** and check your information in the **Add My Certificates** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Zyxel Device to enroll a certificate online.

### 14.2.2 Edit My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

**Figure 89** Configuration > Object > Certificate > My Certificates > Edit

**Edit My Certificates**

---

### Configuration

Name:

### Certification Path

N = wax620d-6e\_1071831B72E5

**Refresh**

### Certificate Information

Type:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	22:2d:69:46:1b:0a:bef6:3d:f4:f8:01:c6:66:d2:b0:cb:8f:2c:da
Subject:	CN = wax620d-6e_1071831B72E5
Issuer:	CN = wax620d-6e_1071831B72E5
Signature Algorithm:	sha256WithRSASignatureEncryption
Valid From:	2022-05-12 12:00:07 GMT
Valid To:	2032-05-09 12:00:07 GMT
Key Algorithm:	rsaEncryption (2048 bit)
Subject Alternative Name:	wax620d-6e_1071831B72E5
Key Usage:	Digital Signature, Key Encipherment, Data Encipherment, Certificate Sign
Extended Key Usage:	
Basic Constraint:	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint:	7A:0A:54:7C:2C:05:EC:3E:E0:AC:EE:04:D0:C8:84:CC
SHA1 Fingerprint:	45:40:2E:13:60:9A:7B:8A:51:EE:06:7D:ED:67:02:CE:78:A3:D9:B0

### Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIDZJCCKAk6gAwIBAgIUl1pRhsKvYy99PgBxmbSsMuPLNowDQYJKoZIhvcNAQEL
BQAw[EqMB4GA1UEAwXxd2F4NjIwZC02ZV8wMDcxQjMxQjcyRTUwHhcNMjIwNTEx
MTIwMDA3WhcNMzIwNTA5MTIwMDA3WjAIMSAwHgYDVGQGDDB3ZXgyMjBkLTZIXzEw
NzFCMzFCNzJFNTCCASUwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANYrWnO
4+nRq3dzs+cBM5L/SWD/XglSVZEgNQEBNTIwHUWgFYBOM6/yyltR+9W06vZmac
nIL1xfcwAQIIYxe8eYD37NDXgnagMlz5xDG3530Fxm+HEIGrLJXncIFPYF7
PPYmyuOahAbSU9Mnh6X6bjdwzGbQz0fyDEObkrqTvdBMRKKehCsqqjn3zlG3y0w
RihbcC8wOidukAnOCmTsdBsf8RocEnltssalcdTctLeudeRCOLeMYNWkXTCC4YMAAozPQ
-----END X509 CERTIFICATE-----
```

Password:

**Export Certificate Only**      **Export Certificate with Private Key**

**OK**      **Cancel**

The following table describes the labels in this screen.

Table 58 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.- characters.
Certification Path  This field displays for a certificate, not a certification request.  Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).  If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Zyxel Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.	
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information  These read-only fields display detailed information about the certificate.	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Zyxel Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.  With self-signed certificates, this is the same as the <b>Subject Name</b> field.  "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate.
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays for what EKU (Extended Key Usage) functions the certificate's key can be used.

Table 58 Configuration &gt; Object &gt; Certificate &gt; My Certificates &gt; Edit

LABEL	DESCRIPTION
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an email that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an email to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
OK	Click <b>OK</b> to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

### 14.2.3 Import Certificates

Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

Note: You can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces in the certificate's filename before you can import it.

**Figure 90** Configuration > Object > Certificate > My Certificates > Import

The following table describes the labels in this screen.

**Table 59** Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.  You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click <b>OK</b> to save the certificate on the Zyxel Device.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 14.3 Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the Zyxel Device to accept as trusted. The Zyxel Device also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

**Figure 91** Configuration > Object > Certificate > Trusted Certificates

The following table describes the labels in this screen.

**Table 60** Configuration > Object > Certificate > Trusted Certificates

<b>LABEL</b>	<b>DESCRIPTION</b>
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click <b>Remove</b> . The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click <b>Object Reference</b> to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click <b>Import</b> to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Zyxel Device.
Refresh	Click this button to display the current validity status of the certificates.

### 14.3.1 Edit Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the Zyxel Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification



The following table describes the labels in this screen.

Table 61 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Configuration	
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',.- characters.
Certification Path  Click the <b>Re fresh</b> button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The Zyxel Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.	
Refresh	Click <b>Re fresh</b> to display the certification path.
Certificate Validation	
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the Zyxel Device check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The Zyxel Device may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The Zyxel Device may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information  These read-only fields display detailed information about the certificate.	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.  With self-signed certificates, this is the same information as in the <b>Subject Name</b> field.



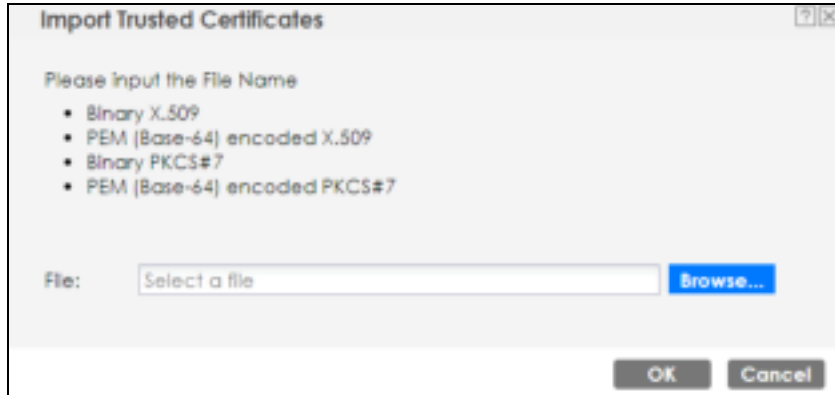
Table 61 Configuration &gt; Object &gt; Certificate &gt; Trusted Certificates &gt; Edit (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form.  You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
OK	Click <b>OK</b> to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted Certificates</b> screen.

### 14.3.2 Import Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Import Trusted Certificates** screen. Follow the instructions in this screen to save a trusted certificate to the Zyxel Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 93** Configuration > Object > Certificate > Trusted Certificates > Import

The following table describes the labels in this screen.

**Table 62** Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.  You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
OK	Click <b>OK</b> to save the certificate on the Zyxel Device.
Cancel	Click <b>Cancel</b> to quit and return to the previous screen.

## 14.4 Technical Reference

The following section contains additional technical information about the features described in this chapter.

### OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the Zyxel Device checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the Zyxel Device only gets information on the certificates that it needs to verify, not a huge list. When the Zyxel Device requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

# CHAPTER 15

## System

### 15.1 Overview

Use the system screens to configure general Zyxel Device settings.

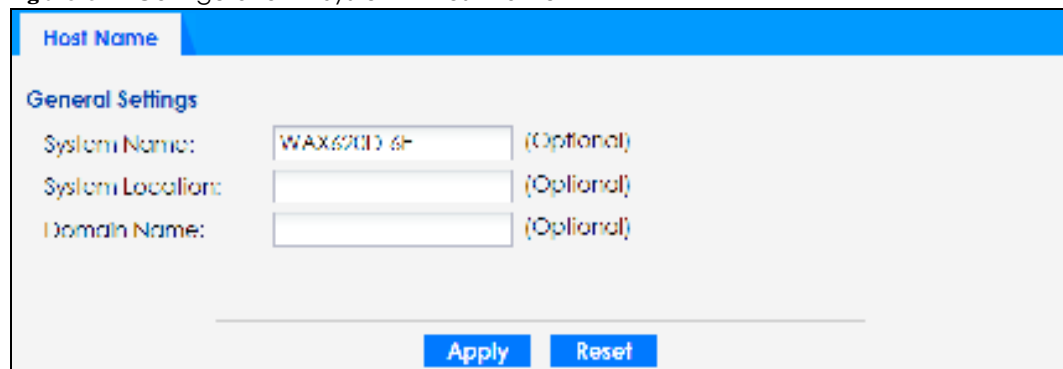
#### 15.1.1 What You Can Do in this Chapter

- The **Host Name** screen ([Section 15.2 on page 147](#)) configures a unique name for the Zyxel Device in your network.
- The **Date/Time** screen ([Section 15.3 on page 148](#)) configures the date and time for the Zyxel Device.
- The **WWW** screens ([Section 15.4 on page 152](#)) configure settings for HTTP or HTTPS access to the Zyxel Device.
- The **SSH** screen ([Section 15.5 on page 160](#)) configures SSH (Secure SHell) for securely accessing the Zyxel Device's command line interface.
- The **FTP** screen ([Section 15.6 on page 164](#)) specifies FTP server settings. You can upload and download the Zyxel Device's firmware and configuration files using FTP. Please also see [Chapter 17 on page 172](#) for more information about firmware and configuration files.

### 15.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open this screen.

**Figure 94** Configuration > System > Host Name



Host Name

General Settings

System Name: WAX6201D-GE (Optional)

System Location: (Optional)

Domain Name: (Optional)

Apply Reset

The following table describes the labels in this screen.

Table 63 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Choose a descriptive name to identify your Zyxel Device device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
System Location	Specify the name of the place where the Zyxel Device is located. You can enter up to 60 alphanumeric and '() ' ,;?! +-* / = # \$ % @ characters. Spaces and underscores are allowed. The name should start with a letter.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

## 15.3 Date and Time

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

To change your Zyxel Device's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the Zyxel Device's time and date or have the Zyxel Device get the date and time from a time server.

**Figure 95** Configuration > System > Date/Time

The following table describes the labels in this screen.

**Table 64** Configuration > System > Date/Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your ZyXel Device.
Current Date	This field displays the present date of your ZyXel Device.
Time and Date Setup	
Manual	Select this radio button 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 ZyXel Device uses the new setting once you click <b>Apply</b> .
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 <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the ZyXel Device get the time and date from the time server you specify below. The ZyXel Device requests time and date settings from the time server under the following circumstances. <ul style="list-style-type: none"> <li>When the ZyXel Device starts up.</li> <li>When you click <b>Apply</b> or <b>Sync Now</b> in this screen.</li> <li>24-hour intervals after starting up.</li> </ul>

Table 64 Configuration &gt; System &gt; Date/Time (continued)

Label	Description
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from a time server (see the <b>Time Server Address</b> field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
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 this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b> . The <b>at</b> 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 <b>Second, Sunday, March</b> and type 2 in the <b>at</b> 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 <b>Last, Sunday, March</b> . The time you type in the <b>at</b> 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 selected <b>Enable Daylight Saving</b> . The <b>at</b> 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 <b>First, Sunday, November</b> and type 2 in the <b>at</b> 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 <b>Last, Sunday, October</b> . The time you type in the <b>at</b> 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).
Offset	Specify how much the clock changes when daylight saving begins and ends.  Enter a number from 1 to 5.5 (by 0.5 increments).  For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

### 15.3.1 Pre-defined NTP Time Servers List

When you turn on the Zyxel Device for the first time, the date and time start at 2003-01-01 00:00:00. The Zyxel Device then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The Zyxel Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 65 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

When the Zyxel Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Zyxel Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

### 15.3.2 Time Server Synchronization

Click the **Sync. Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading** message appears, you may have to wait up to one minute.

Figure 96 Loading



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the Zyxel Device date and time:

- 1 Click **System > Date/Time**.
- 2 Select **Manual** under **Time and Date Setup**.
- 3 Enter the Zyxel Device's time in the **New Time** field.
- 4 Enter the Zyxel Device's date in the **New Date** field.
- 5 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 6 As an option you can select the **Enable Daylight Saving** check box to adjust the Zyxel Device clock for daylight savings.
- 7 Click **Apply**.

To get the Zyxel Device date and time from a time server:

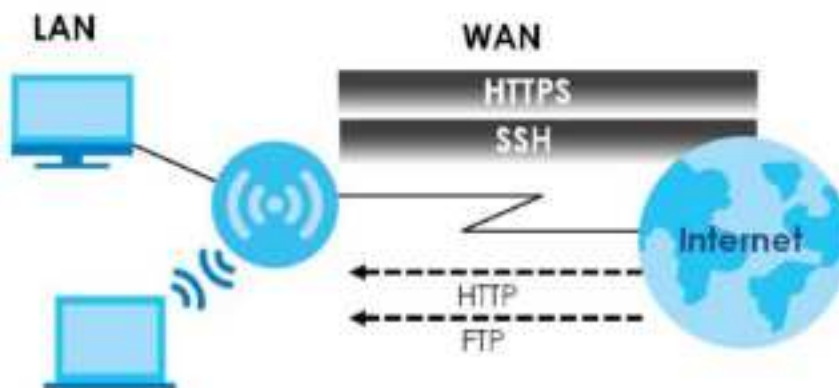
- 1 Click **System > Date/Time**.
- 2 Select **Get from Time Server** under **Time and Date Setup**.

- 3 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 4 Under **Time and Date Setup**, enter a **Time Server Address**.
- 5 Click **Apply**.

## 15.4 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and FTP management access are not secure.

**Figure 97** Secure and Insecure Service Access From the WAN



### 15.4.1 Service Access Limitations

A service cannot be used to access the Zyxel Device when you have disabled that service in the corresponding screen.

### 15.4.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User** screens.

### 15.4.3 HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the



transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

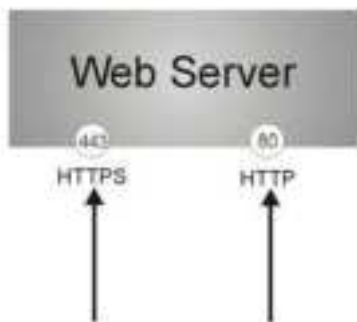
It relies upon certificates, public keys, and private keys (see [Chapter 14 on page 131](#) for more information).

HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the Zyxel Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Zyxel Device.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Zyxel Device's web server.
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the Zyxel Device's web server.

**Figure 98** HTTP/HTTPS Implementation



Note: If you disable **HTTP** in the **WWW** screen, then the Zyxel Device blocks all HTTP connection attempts.

#### 15.4.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify HTTP or HTTPS settings.

**Figure 99** Configuration > System > WWW > Service Control

The screenshot shows the 'Service Control' configuration page. It has a blue header bar with the text 'Service Control'. Below the header, there are two sections: 'HTTPS' and 'HTTP'. The 'HTTPS' section contains a checked 'Enable' checkbox, a 'Server Port' input field with the value '443', an unchecked 'Authenticate Client Certificates' checkbox with a link '(See Trusted CAs)', a 'Server Certificate' dropdown menu with 'default' selected, and a checked 'Redirect HTTP to HTTPS' checkbox. The 'HTTP' section contains a checked 'Enable' checkbox and a 'Server Port' input field with the value '80'. At the bottom of the page, there are two blue buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 66 Configuration &gt; System &gt; WWW &gt; Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the <b>Service Control</b> table to access the Zyxel Device Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use "https://Zyxel Device IP Address:8443" as the URL.
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself to the Zyxel Device by sending the Zyxel Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device.  Click <b>Trusted CAs</b> to go to the <b>Configuration &gt; Object &gt; Certificate &gt; Trusted Certificates</b> screen and check for the trusted certificates settings.
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the <b>My Certificates</b> screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the <b>Service Control</b> table to access the Zyxel Device Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the Zyxel Device.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

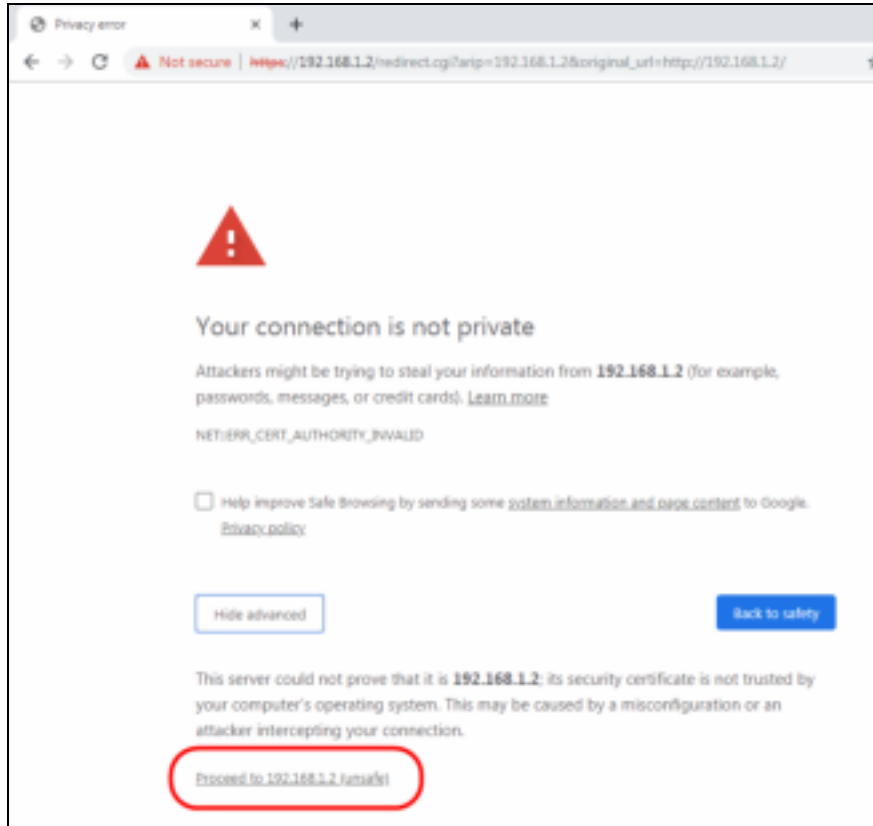
### 15.4.5 HTTPS Example

If you have not changed the default HTTPS port on the Zyxel Device, then in your browser enter "https://Zyxel Device IP Address/" as the web site address where "Zyxel Device IP Address" is the IP address or domain name of the Zyxel Device you wish to access.

#### 15.4.5.1 Google Chrome Warning Messages

When you attempt to access the Zyxel Device HTTPS server, you will see the error message shown in the following screen.

**Figure 100** Security Alert Dialog Box (Google Chrome)

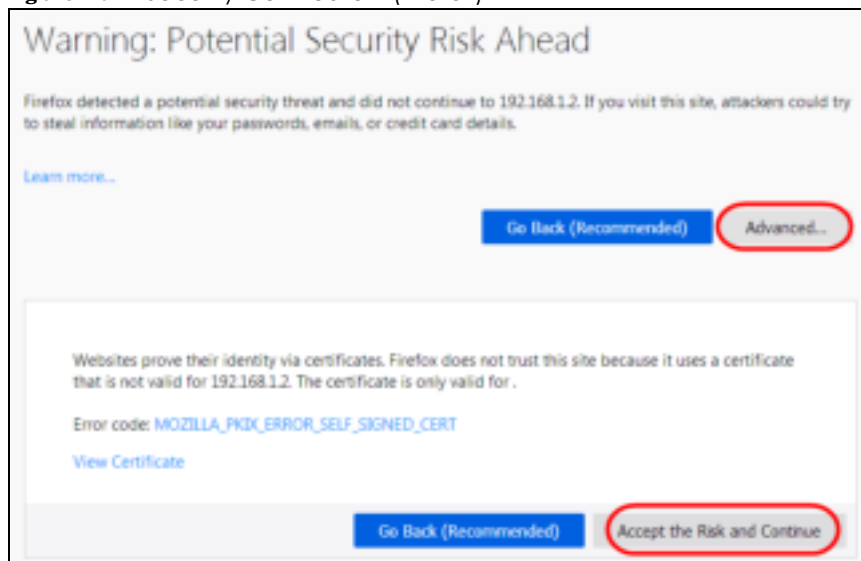


Select **Advanced > Proceed to 192.168.1.2 (unsafe)** to proceed to the Web Configurator login screen.

#### 15.4.5.2 Mozilla Firefox Warning Messages

When you attempt to access the Zyxel Device HTTPS server, a Warning screen appears as shown in the following screen. Click **Learn More...** if you want to verify more information about the certificate from the Zyxel Device.

Click **Advanced > Accept the Risk and Continue**.

**Figure 101** Security Certificate 1 (Firefox)

### 15.4.5.3 Avoiding Browser Warning Messages

Here are the main reasons your browser displays warnings about the Zyxel Device's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the Zyxel Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Zyxel Device's factory default certificate is the Zyxel Device itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to [Appendix A on page 211](#) for details.

### 15.4.5.4 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Zyxel Device.

You must have imported at least one trusted CA to the Zyxel Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Zyxel Device (see the Zyxel Device's **Trusted Certificates** Web Configurator screen).

**Figure 102** Trusted Certificates

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

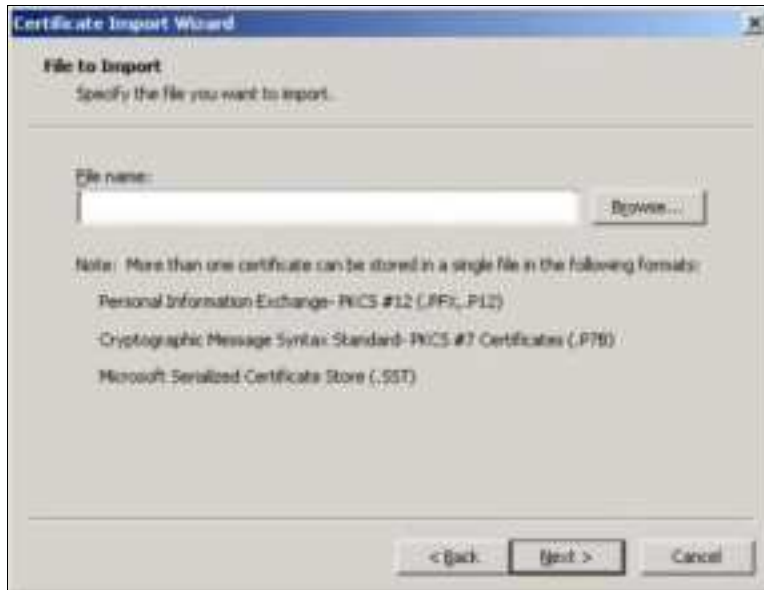
#### 15.4.5.5 Installing a Personal Certificate

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next.

- 1 Click **Next** to begin the wizard.



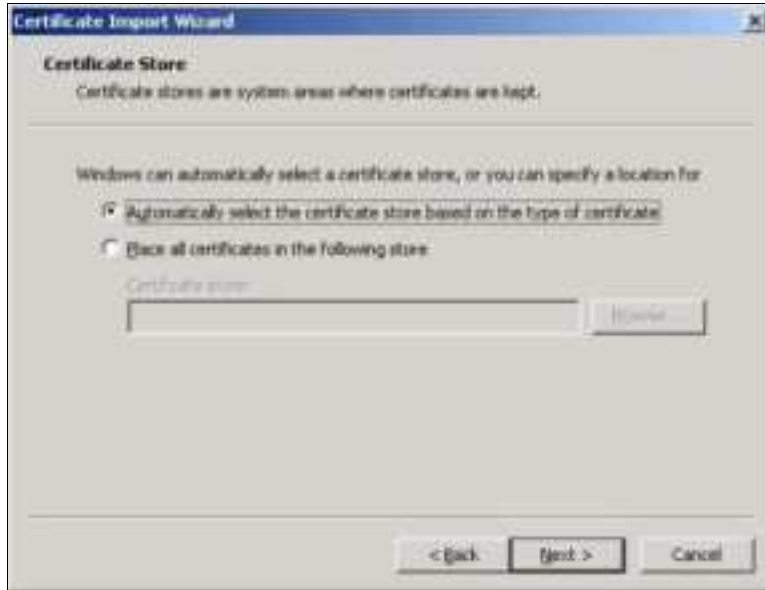
- 2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.



- 3 Enter the password given to you by the CA.



- 4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.



- 5 Click **Finish** to complete the wizard and begin the import process.



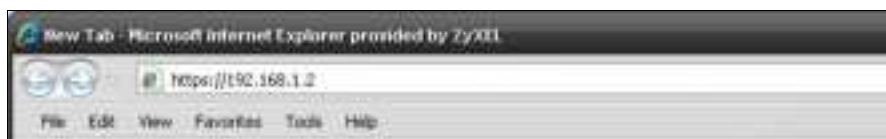
- 6 You should see the following screen when the certificate is correctly installed on your computer.



#### 15.4.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device via HTTPS:

- 1 Enter 'https://Zyxel Device IP Address/' in your browser's web address field.



- 2 When **Authenticate Client Certificates** is selected on the Zyxel Device, the following screen asks you to select a personal certificate to send to the Zyxel Device. This screen displays even if you only have a single certificate as in the example.



- 3 You next see the Web Configurator login screen.

## 15.5 SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer B on the Internet uses SSH to securely connect to the Zyxel Device (A) for a management session.

**Figure 103** SSH Communication Over the WAN Example

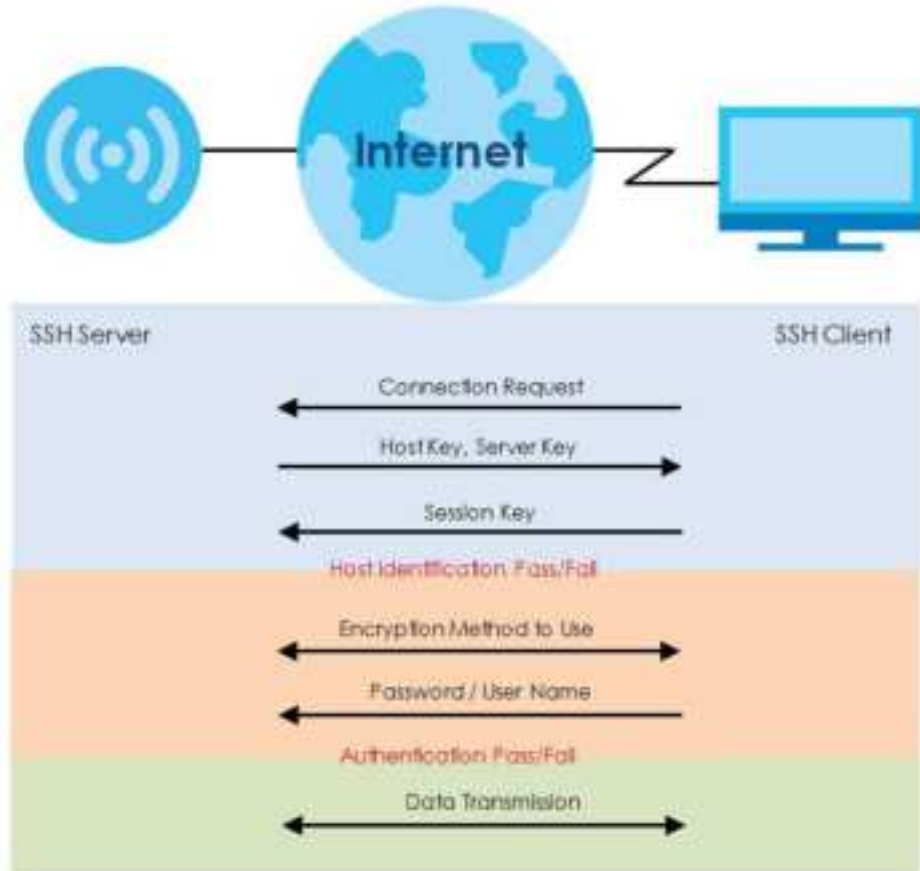




### 15.5.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

**Figure 104** How SSH v1 Works Example



#### 1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

#### 2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

#### 3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

### 15.5.2 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the Zyxel Device for management using port 22 (by default).

### 15.5.3 Requirements for Using SSH

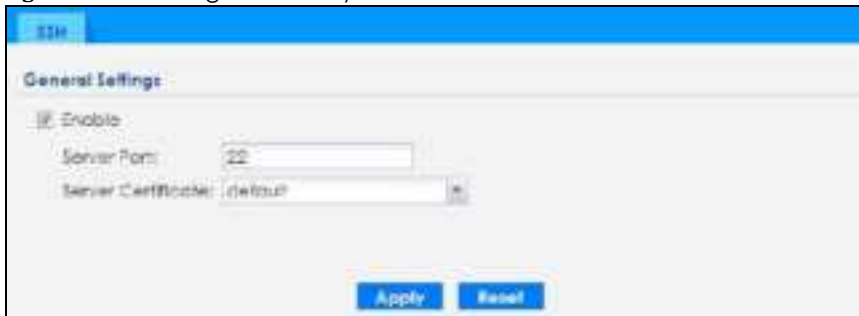
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

### 15.5.4 Configuring SSH

Click **Configuration > System > SSH** to open the following screen. Use this screen to configure your Zyxel Device's Secure Shell settings.

Note: It is recommended that you disable FTP when you configure SSH for secure connections.

**Figure 105** Configuration > System > SSH



The following table describes the labels in this screen.

Table 67 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the <b>Service Control</b> table to access the Zyxel Device CLI using this service.  Note: The Zyxel Device uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. You must have certificates already configured in the <b>My Certificates</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

### 15.5.5 Examples of Secure Telnet Using SSH

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Zyxel Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

#### 15.5.5.1 Example 1: Microsoft Windows

This section describes how to access the Zyxel Device using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number) for the Zyxel Device.
- 2 Configure the SSH client to accept connection using SSH version 2.
- 3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

**Figure 106** SSH Example 1: Store Host Key



Enter the password to log in to the Zyxel Device. The CLI screen displays next.

#### 15.5.5.2 Example 2: Linux

This section describes how to access the Zyxel Device using the OpenSSH client program that comes with most Linux distributions.

- 1 Enter "`ssh -2 192.168.1.2`" at a terminal prompt and press [ENTER]. This command forces your computer to connect to the Zyxel Device using SSH version 1. If this is the first time you are connecting to the Zyxel Device using SSH, a message displays prompting you to save the host information of the Zyxel Device. Type "yes" and press [ENTER].

Then enter the password to log in to the Zyxel Device.

**Figure 107** SSH Example 2: Log in

```
$ ssh -2 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (RSA1) to the list of known hosts.
Administrator@192.168.1.2's password:
```

- 2 The CLI screen displays next.

## 15.6 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. See [Chapter 17 on page 172](#) for more information about firmware and configuration files.

To change your Zyxel Device's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify FTP settings.

**Figure 108** Configuration > System > FTP

The following table describes the labels in this screen.

Table 68 Configuration &gt; System &gt; FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the <b>Service Control</b> table to access the Zyxel Device using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections. You must have certificates already configured in the <b>My Certificates</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.



# CHAPTER 16

## Log and Report

### 16.1 Overview

Use the system screens to configure daily reporting and log settings.

#### 16.1.1 What You Can Do In this Chapter

- The **Log Setting** screens ([Section 16.2 on page 166](#)) specify which logs are emailed, where they are emailed, and how often they are emailed.

### 16.2 Log Setting

These screens control log messages and alerts. A log message stores the information for viewing (for example, in the **Monitor > View Log** screen). Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The **Log Setting** screen provides a summary of all the settings. You can use the **Edit Log Setting** screen to maintain the detailed settings (such as log categories, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

#### 16.2.1 Log Setting Screen

To access this screen, click **Configuration > Log & Report > Log Setting**.

**Figure 109** Configuration > Log & Report > Log Setting



The following table describes the labels in this screen.

Table 69 Configuration > Log & Report > Log Setting

<b>LABEL</b>	<b>DESCRIPTION</b>
Edit	Double-click an entry or select it and click <b>Edit</b> to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click <b>Activate</b> .
Inactivate	To turn off an entry, select it and click <b>Inactivate</b> .
#	This field is a sequential value, and it is not associated with a specific log.
Status	This field shows whether the log is active or not.
Name	This field displays the name of the log (system log or one of the remote servers).
Log Format	This field displays the format of the log.  <b>Internal</b> - system log; you can view the log on the <b>View Log</b> tab.  <b>VRPT Syslog</b> - Zyxel's Vantage Report, syslog-compatible format.  <b>CEF Syslog</b> - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.
Active Log Summary	Click this button to open the <b>Active Log Summary</b> screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

### 16.2.2 Edit Remote Server

This screen controls the settings for each log in the remote server (syslog). Select a remote server entry in the **Log Setting** screen and click the **Edit** icon.

**Figure 110** Configuration > Log & Report > Log Setting > Edit Remote Server

The following table describes the labels in this screen.

**Table 70** Configuration > Log & Report > Log Setting > Edit Remote Server

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the <b>Active Log</b> section.
Log Format	This field displays the format of the log information. It is read-only. <b>VRPT Syslog</b> - Zyxel's Vantage Report, syslog-compatible format. <b>CEF Syslog</b> - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	



Table 70 Configuration &gt; Log &amp; Report &gt; Log Setting &gt; Edit Remote Server (continued)

LABEL	DESCRIPTION
Selection	<p>Use the <b>Selection</b> drop-down list to change the log settings for all of the log categories.</p> <p><b>disable all logs</b> (red X) - do not send the remote server logs for any log category.</p> <p><b>enable normal logs</b> (green check mark) - send the remote server log messages and alerts for all log categories.</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.</p>
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the <b>Display</b> and <b>Category</b> fields in the <b>View Log</b> tab. The <b>Default</b> category includes debugging messages generated by open source software.
Selection	<p>Select what information you want to log from each <b>Log Category</b> (except <b>All Logs</b>; see below). Choices are:</p> <p><b>disable all logs</b> (red X) - do not log any information from this category</p> <p><b>enable normal logs</b> (green checkmark) - log regular information and alerts from this category</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - log regular information, alerts, and debugging information from this category</p>
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

### 16.2.3 Active Log Summary

This screen allows you to view and to edit what information is included in the system log and remote servers at the same time. It does not let you change other log settings. To access this screen, go to the **Log Setting** screen, and click the **Active Log Summary** button.

**Figure 111** Active Log Summary

The screenshot shows the 'Active Log Summary' window. At the top, there are tabs for 'System Log', 'Remote Server 1', 'Remote Server 2', 'Remote Server 3', and 'Remote Server 4'. Below the tabs is a table with columns for 'Log Category', 'System Log', 'Remote Server 1', 'Remote Server 2', 'Remote Server 3', and 'Remote Server 4'. Each cell in the table contains a set of three small circular icons (blue, green, and red) representing different log statuses. The table lists 34 log categories, including Account, Authentication Server, Bluetooth, Bulletin Service, Cloud Auth, Connectivity Check, Daily Report, Default, Device HA, Dynamic Frequency, DHCP, File Manager, Force Authentication, Interface, Interface Statistics, PG, Real-Time Location, Smart Mail, Site Roaming, Station Info Collection, System, System Monitoring, Traffic Log, User, Wireless Health, Wireless LAN, WLAN Band Select, WLAN Dynamic Chg, AP Load Balancing, WLAN Rogue AP Det, WLAN Station Info, Zero One Network, ZyMesh, and ZyRR. At the bottom of the window, there is a pagination bar showing 'Page 1 of 1' and 'Showing 1 - 34 of 34'. There are also 'OK' and 'Cancel' buttons at the bottom right.

Log Category	System Log	Remote Server 1	Remote Server 2	Remote Server 3	Remote Server 4
1 Account					
2 Authentication Server					
3 Bluetooth					
4 Bulletin Service					
5 Cloud Auth					
6 Connectivity Check					
7 Daily Report					
8 Default					
9 Device HA					
10 Dynamic Frequency					
11 DHCP					
12 File Manager					
13 Force Authentication					
14 Interface					
15 Interface Statistics					
16 PG					
17 Real-Time Location					
18 Smart Mail					
19 Site Roaming					
20 Station Info Collection					
21 System					
22 System Monitoring					
23 Traffic Log					
24 User					
25 Wireless Health					
26 Wireless LAN					
27 WLAN Band Select					
28 WLAN Dynamic Chg					
29 AP Load Balancing					
30 WLAN Rogue AP Det					
31 WLAN Station Info					
32 Zero One Network					
33 ZyMesh					
34 ZyRR					

This screen provides a different view and a different way of indicating which messages are included in each log and each alert. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 71 Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	If the Zyxel Device is set to controller mode, the AC section controls logs generated by the controller and the AP section controls logs generated by the managed APs.
System log	<p>Use the <b>System Log</b> drop-down list to change the log settings for all of the log categories.</p> <p><b>disable all logs</b> (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2.</p> <p><b>enable normal logs</b> (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them.</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.</p>
Remote Server 1~4	<p>For each remote server, use the <b>Selection</b> drop-down list to change the log settings for all of the log categories.</p> <p><b>disable all logs</b> (red X) - do not send the remote server logs for any log category.</p> <p><b>enable normal logs</b> (green check mark) - send the remote server log messages and alerts for all log categories.</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.</p>
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the <b>Display</b> and <b>Category</b> fields in the <b>View Log</b> tab. The <b>Default</b> category includes debugging messages generated by open source software.
System log	<p>Select which events you want to log by <b>Log Category</b>. There are three choices:</p> <p><b>disable all logs</b> (red X) - do not log any information from this category</p> <p><b>enable normal logs</b> (green checkmark) - create log messages and alerts from this category</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.</p>
Remote Server 1~4 Syslog	<p>For each remote server, select what information you want to log from each <b>Log Category</b> (except <b>All Logs</b>; see below). Choices are:</p> <p><b>disable all logs</b> (red X) - do not log any information from this category</p> <p><b>enable normal logs</b> (green checkmark) - log regular information and alerts from this category</p> <p><b>enable normal logs and debug logs</b> (yellow check mark) - log regular information, alerts, and debugging information from this category</p>
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

# CHAPTER 17

## File Manager

### 17.1 Overview

Configuration files define the Zyxel Device's settings. Shell scripts are files of commands that you can store on the Zyxel Device and run when you need them. You can apply a configuration file or run a shell script without the Zyxel Device restarting. You can store multiple configuration files and shell script files on the Zyxel Device. You can edit configuration files or shell scripts in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension and shell scripts use a .zysh extension.

#### 17.1.1 What You Can Do in this Chapter

- The **Configuration File** screen ([Section 17.2 on page 173](#)) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen ([Section 17.3 on page 178](#)) checks your current firmware version and uploads firmware to the Zyxel Device.
- The **Shell Script** screen ([Section 17.4 on page 180](#)) stores, names, downloads, uploads and runs shell script files.

#### 17.1.2 What you Need to Know

The following terms and concepts may help as you read this chapter.

##### Configuration Files and Shell Scripts

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the Zyxel Device only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

**Figure 112** Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
#configure default radio profile, change 2GHz channel to 11 & Tx output
power # to 50%
wlan-radio-profile default
2g-channel 11
output-power 50%
exit
write
```

While configuration files and shell scripts have the same syntax, the Zyxel Device applies configuration files differently than it runs shell scripts. This is explained below.

Table 72 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
<ul style="list-style-type: none"> <li>Resets to default configuration.</li> <li>Goes into CLI <b>C</b>onfiguration mode.</li> <li>Runs the commands in the configuration file.</li> </ul>	<ul style="list-style-type: none"> <li>Goes into CLI <b>P</b>rivilege mode.</li> <li>Runs the commands in the shell script.</li> </ul>

You have to run the aforementioned example as a shell script because the first command is run in **P**rivilege mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **C**onfiguration mode.

### Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the Zyxel Device treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the Zyxel Device exit sub command mode.

Note: “exit” or “!” must follow sub commands if it is to make the Zyxel Device exit sub command mode.

In the following example lines 1 and 2 are comments. Line 7 exits sub command mode.

```
! this is from Joe
# on 2010/12/05
wlan-ssid-profile default
ssid Joe-AP
qos wmm
security default
!
```

### Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the Zyxel Device processes the file line-by-line. The Zyxel Device checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the Zyxel Device finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The Zyxel Device ignores any errors in the configuration file or shell script and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

## 17.2 Configuration File

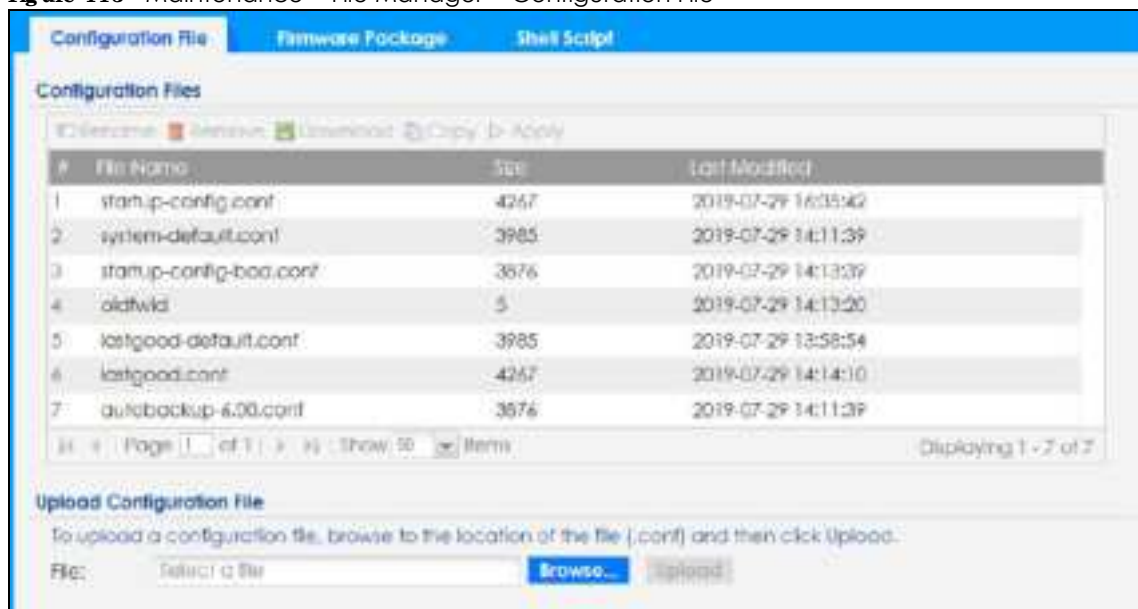
Click **Maintenance > File Manager > Configuration File** to open this screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.

Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

### Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

**Figure 113** Maintenance > File Manager > Configuration File



**Do not turn off the Zyxel Device while configuration file upload is in progress.**

The following table describes the labels in this screen.

Table 73 Maintenance > File Manager > Configuration File

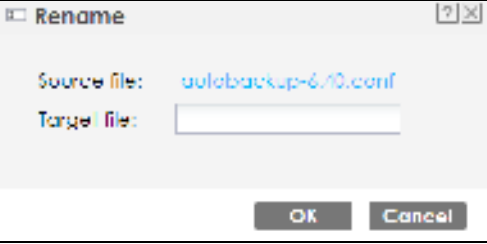

LABEL	DESCRIPTION
Configuration Files	
Rename	<p>Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the <b>lastgood.conf</b>, <b>system-default.conf</b> and <b>startup-config.conf</b> files.</p> <p>You cannot rename a configuration file to the name of another configuration file in the Zyxel Device.</p> <p>Click a configuration file's row to select it and click <b>Rename</b> to open the <b>Rename File</b> screen.</p>  <p>Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&amp;()_+[]{}',.-).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a configuration file's row to select it and click <b>Remove</b> to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the <b>system-default.conf</b>, <b>startup-config.conf</b> and <b>lastgood.conf</b> files.</p> <p>A pop-up window asks you to confirm that you want to delete the configuration file. Click <b>OK</b> to delete the configuration file or click <b>Cancel</b> to close the screen without deleting the configuration file.</p>
Download	<p>Click a configuration file's row to select it and click <b>Download</b> to save the configuration to your computer.</p>
Copy	<p>Use this button to save a duplicate of a configuration file on the Zyxel Device.</p> <p>Click a configuration file's row to select it and click <b>Copy</b> to open the <b>Copy File</b> screen.</p>  <p>Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&amp;()_+[]{}',.-).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>

Table 73 Maintenance &gt; File Manager &gt; Configuration File (continued)

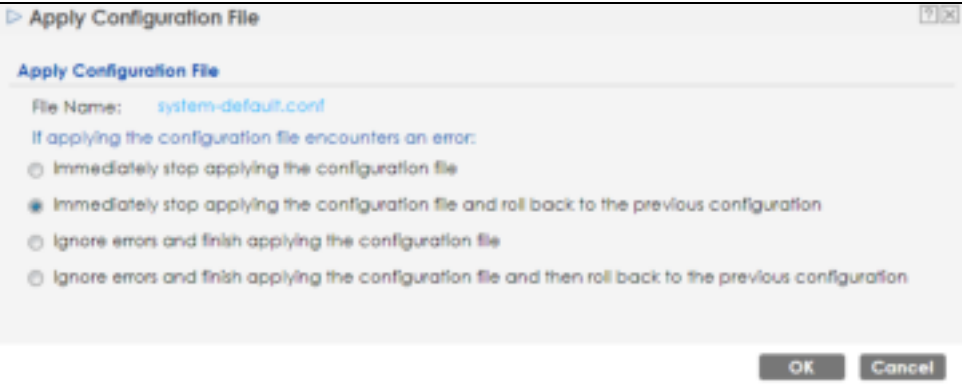
LABEL	DESCRIPTION
Apply	<p>Use this button to have the Zyxel Device use a specific configuration file.</p> <p>Click a configuration file's row to select it and click <b>Apply</b> to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.</p> <p>The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file.</p>  <p><b>Immediately stop applying the configuration file</b> - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the Zyxel Device.</p> <p><b>Immediately stop applying the configuration file and roll back to the previous configuration</b> - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible.</p> <p><b>Ignore errors and finish applying the configuration file</b> - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix.</p> <p><b>Ignore errors and finish applying the configuration file and then roll back to the previous configuration</b> - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the Zyxel Device with a fully valid configuration file.</p> <p>Click <b>OK</b> to have the Zyxel Device start applying the configuration file or click <b>Cancel</b> to close the screen.</p>
#	<p>This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.</p>
File Name	<p>This column displays the label that identifies a configuration file.</p> <p>You cannot delete the following configuration files or change their file names.</p> <p>The <b>system-default.conf</b> file contains the Zyxel Device's default settings. Select this file and click <b>Apply</b> to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package.</p> <p>The <b>startup-config.conf</b> file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click <b>Apply</b> or <b>OK</b>. It applies configuration changes made through CLI commands when you use the <code>write</code> command.</p> <p>The <b>lastgood.conf</b> is the most recently used (valid) configuration file that was saved when the Zyxel Device last restarted. If you upload and apply a configuration file with an error, you can apply <b>lastgood.conf</b> to return to a valid configuration.</p>
Size	<p>This column displays the size (in KB) of a configuration file.</p>



Table 73 Maintenance &gt; File Manager &gt; Configuration File (continued)

LABEL	DESCRIPTION
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File  The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device.  You cannot upload a configuration file named <b>system-default.conf</b> or <b>lastgood.conf</b> .  If you upload <b>startup-config.conf</b> , it will replace the current configuration and immediately apply the new settings.	
File	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a file of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

### 17.2.1 Example of Configuration File Download Using FTP

The following example gets a configuration file named startup-config.conf from the Zyxel Device and saves it on the computer.

- 1 Connect your computer to the Zyxel Device.
- 2 The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.
- 3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.
- 4 Enter your user name when prompted.
- 5 Enter your password as requested.
- 6 Use "cd" to change to the directory that contains the files you want to download.
- 7 Use "dir" or "ls" if you need to display a list of the files in the directory.
- 8 Use "get" to download files. Transfer the configuration file on the Zyxel Device to your computer. Type `get` followed by the name of the configuration file. This examples uses `get startup-config.conf`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> cd conf
250 OK. Current directory is /conf
ftp> ls
200 PORT command successful
150 Connecting to port 5001
lastgood.conf
startup-config.conf
system-default.conf
226 3 matches total
ftp: 57 bytes received in 0.33Seconds 0.17Kbytes/sec.
ftp> get startup-config.conf
200 PORT command successful
150 Connecting to port 5002
226-File successfully transferred
226 0.002 seconds (measured here), 1.66 Mbytes per second
ftp: 2928 bytes received in 0.02Seconds 183.00Kbytes/sec.
ftp>
```

- 9 Wait for the file transfer to complete.
- 10 Enter "quit" to exit the ftp prompt.

## 17.3 Firmware Package

Click **Maintenance > File Manager > Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the Zyxel Device.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses a .bin extension.

**The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!**

**Figure 114** Maintenance > File Manager > Firmware Package

The following table describes the labels in this screen.

**Table 74** Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Zyxel Device again.

Note: The Zyxel Device automatically reboots after a successful upload.

The Zyxel Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 115** Network Temporarily Disconnected

After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

### 17.3.1 Example of Firmware Upload Using FTP

This procedure requires the Zyxel Device's firmware. Download the firmware package from [www.zyxel.com](http://www.zyxel.com) and unzip it. The firmware file uses a .bin extension, for example, "600ABFH0C0.bin". Do the following after you have obtained the firmware file.

- 1 Connect your computer to the Zyxel Device.
- 2 The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.
- 3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.

- 4 Enter your user name when prompted.
- 5 Enter your password as requested.
- 6 Enter "hash" for FTP to print a '#' character for every 1024 bytes of data you upload so that you can watch the file transfer progress.
- 7 Enter "bin" to set the transfer mode to binary.
- 8 Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This example uses `put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin
```

Note: The Zyxel Device will not upgrade the firmware if the firmware file you upload is incompatible with the Zyxel Device.

- 9 Wait for the file transfer to complete.
- 10 Enter "quit" to exit the ftp prompt.

## 17.4 Shell Script

Use shell script files to have the Zyxel Device use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

**Figure 116** Maintenance > File Manager > Shell Script

Each field is described in the following table.

**Table 75** Maintenance > File Manager > Shell Script

Label	Description
Rename	<p>Use this button to change the label of a shell script file on the ZyXel Device.</p> <p>You cannot rename a shell script to the name of another shell script in the ZyXel Device.</p> <p>Click a shell script's row to select it and click <b>Rename</b> to open the <b>Rename File</b> screen.</p> <p>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;~!@#%&amp;()_+[]{}',.=).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a shell script file's row to select it and click <b>Delete</b> to delete the shell script file from the ZyXel Device.</p> <p>A pop-up window asks you to confirm that you want to delete the shell script file. Click <b>OK</b> to delete the shell script file or click <b>Cancel</b> to close the screen without deleting the shell script file.</p>
Download	Click a shell script file's row to select it and click <b>Download</b> to save the configuration to your computer.
Copy	<p>Use this button to save a duplicate of a shell script file on the ZyXel Device.</p> <p>Click a shell script file's row to select it and click <b>Copy</b> to open the <b>Copy File</b> screen.</p> <p>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;~!@#%&amp;()_+[]{}',.=).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>
Apply	<p>Use this button to have the ZyXel Device use a specific shell script file.</p> <p>Click a shell script file's row to select it and click <b>Apply</b> to have the ZyXel Device use that shell script file. You may need to wait awhile for the ZyXel Device to finish applying the commands.</p>
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ZyXel Device.
File	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.

Table 75 Maintenance &gt; File Manager &gt; Shell Script (continued)

LABEL	DESCRIPTION
Browse...	Click <b>Browse...</b> to find the .zysh file you want to upload.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to several minutes.

# CHAPTER 18

## Diagnostics

### 18.1 Overview

Use the diagnostics screen for troubleshooting.

#### 18.1.1 What You Can Do in this Chapter

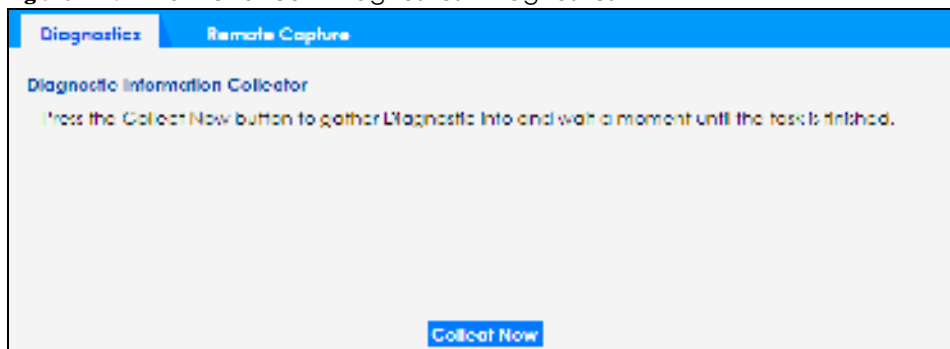
- The **Diagnostics** screen (Section 18.2 on page 183) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Remote Capture** screen (Section 18.3 on page 184) enables remote packet captures on wired or wireless interfaces through an external packet analyzer.

### 18.2 Diagnostics

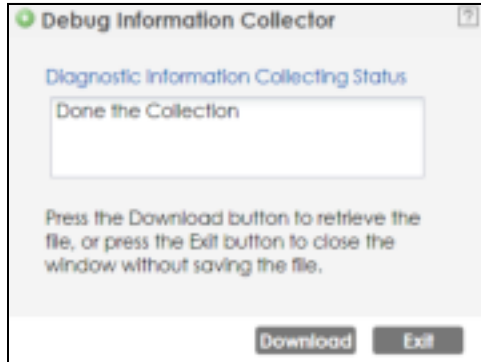
This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

Click **Maintenance > Diagnostics > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

**Figure 117** Maintenance > Diagnostics > Diagnostics



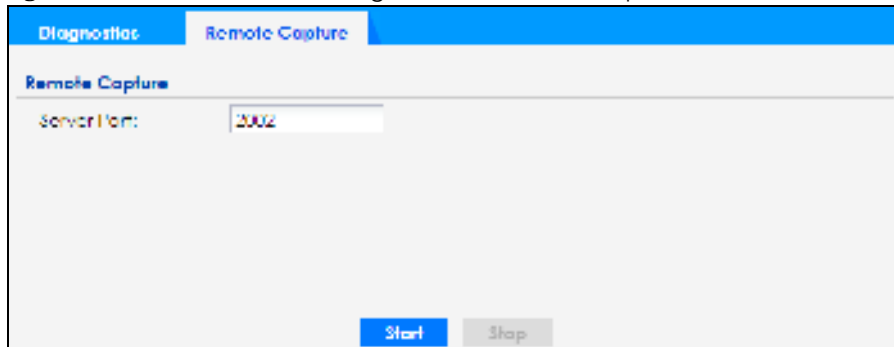
The **Debug Information Center** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

**Figure 118** Maintenance > Diagnostics: Debug Information Collector

## 18.3 Remote Capture

Use this screen to capture network traffic going through the Zyxel Device and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark. If the Zyxel Device is connected to the Zyxel gateway or ZyWALL, you might need to configure the Zyxel gateway or ZyWALL to allow remote capture on the Zyxel Device.

Click **Maintenance > Diagnostics > Remote Capture** to open the **Remote Capture** screen.

**Figure 119** Maintenance > Diagnostics > Remote Capture

The following table describes the labels in this screen.

Table 76 Maintenance &gt; Diagnostics &gt; Remote Capture

LABEL	DESCRIPTION
Server Port	Enter the number of the server port you want the packet analyzer to connect to in order to capture traffic going through the Zyxel Device. The default port number is 2002.
Start	Click this button to allow the packet analyzer to start capturing traffic going through the Zyxel Device.
Stop	Click this button to stop the packet analyzer from capturing traffic going through the Zyxel Device.



# CHAPTER 19

## LEDs

### 19.1 Overview

The LEDs of your Zyxel Device can be controlled such that they stay lit (ON) or OFF after the Zyxel Device is ready. There are two features that control the LEDs of your Zyxel Device - **Locator** and **Suppression** (see [Section 1.2 on page 12](#)).

Note: Not all Zyxel Devices have LEDs; see [Section 3.1.1 on page 30](#) for more information.

#### 19.1.1 What You Can Do in this Chapter

- The **Suppression** screen ([Section 19.2 on page 185](#)) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The **Locator** screen ([Section 19.3 on page 186](#)) allows users to see the actual location of the Zyxel Device between several devices in the network.

### 19.2 Suppression Screen

The LED Suppression feature allows you to control how the LEDs of your Zyxel Device behave after it's ready. The default LED suppression setting of your AP is different depending on your Zyxel Device model.

You can go to the **Maintenance > LEDs > Suppression** screen to see the default LED behavior and change the LED suppression setting. After you make changes in the suppression screen, it will be stored as the default when the Zyxel Device is restarted. See ([Section 3.1 on page 30](#)) for information on default values for different models.

Note: When the Zyxel Device is booting or performing firmware upgrade, the LEDs will light up regardless of the setting in LED suppression.

To access this screen, click **Maintenance > LEDs > Suppression**.

**Figure 120** Maintenance > LEDs > Suppression

The following table describes fields in the above screen.

**Table 77** Maintenance > LED > Suppression

LABEL	DESCRIPTION
Suppression On	If the <b>Suppression On</b> check box is checked, the LEDs of your Zyxel Device will turn off after it's ready.  If the check box is unchecked, the LEDs will stay lit after the Zyxel Device is ready.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

## 19.3 Locator Screen

The Locator feature identifies the location of your Zyxel Device among several devices in the network. You can run this feature and set a timer in this screen.

To run the locator feature, enter a number of minutes and click **Turn On** button to have the Zyxel Device find its location. The Locator LED will start to blink for the number of minutes set in the **Locator** screen. The default setting is 10 minutes. While the locator is running, the turn on button will gray out and return after it's finished. If you make changes to the time default setting, it will be stored as the default when the Zyxel Device restarts.

Note: The Locator feature is not affected by the Suppression setting.

To access this screen, click **Maintenance > LEDs > Locator**.

**Figure 121** Maintenance > LEDs > Locator

The following table describes fields in the above screen.

**Table 78** Maintenance > LED > Locator

LABEL	DESCRIPTION
Turn On Turn Off	Click <b>Turn On</b> button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network.  Otherwise, click <b>Turn Off</b> to disable the locator feature.
Automatically Extinguish After	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. Default is 10 minutes.
Apply	Click <b>Apply</b> to save changes in this screen.
Refresh	Click <b>Refresh</b> to update the information in this screen.

# CHAPTER 20

## Reboot

### 20.1 Overview

Use this screen to restart the Zyxel Device.

#### 20.1.1 What You Need To Know

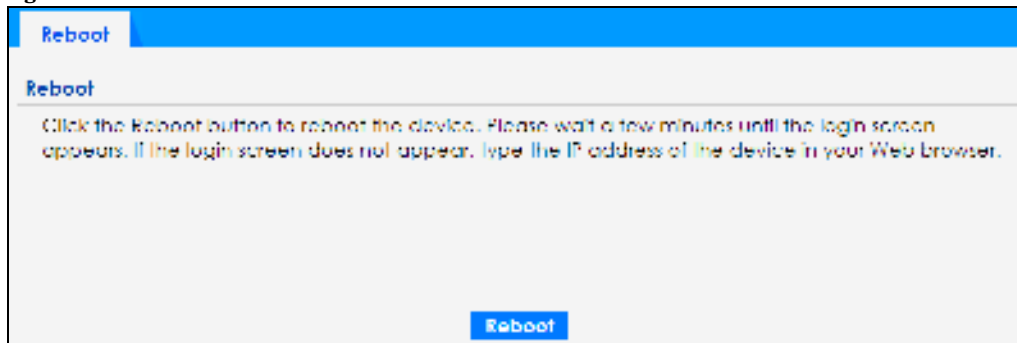
If you applied changes in the Web Configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

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

### 20.2 Reboot

This screen allows remote users can restart the Zyxel Device. To access this screen, click **Maintenance > Reboot**.

**Figure 122** Maintenance > Reboot



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

You can also use the CLI command `reboot` to restart the Zyxel Device.

# CHAPTER 21

## Shutdown

### 21.1 Overview

Use this screen to shut down the Zyxel Device.

**Always use Maintenance > Shutdown > Shutdown or the shutdown command before you turn off the Zyxel Device or remove the power. Not doing so can cause the firmware to become corrupt.**

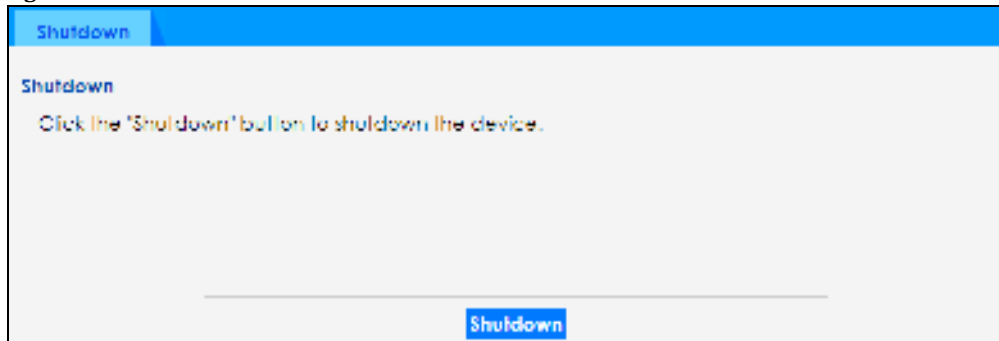
#### 21.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes. Shutdown is different to reset; reset returns the Zyxel Device to its default configuration.

### 21.2 Shutdown

To access this screen, click **Maintenance > Shutdown**.

**Figure 123** Maintenance > Shutdown



Click the **Shutdown** button to shut down the Zyxel Device. Wait for the Zyxel Device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shut down the Zyxel Device.

---

# **PART II**

## **Local Configuration in Cloud Mode**

---

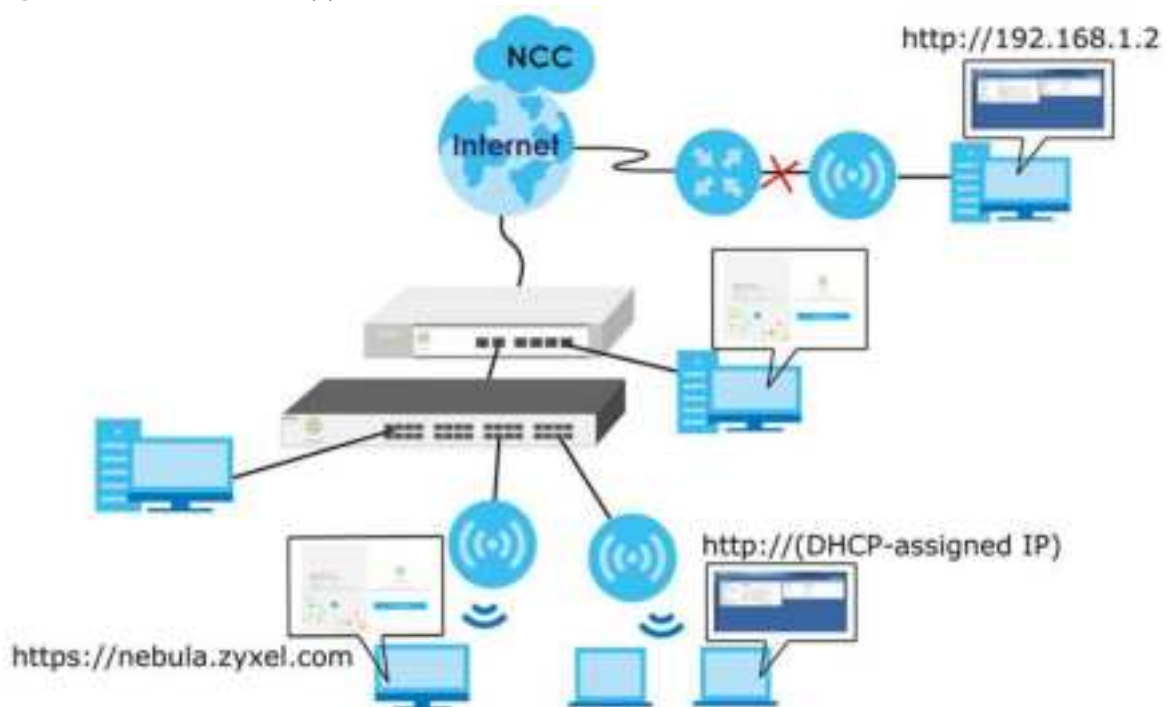
# CHAPTER 22

## Cloud Mode

### 22.1 Overview

The Zyxel Device is managed and provisioned automatically by the *NCC (Nebula Control Center)* when it is connected to the Internet and has been registered in the NCC. If you need to change the Zyxel Device's VLAN setting or manually set its IP address, access its simplified web configurator. You can check the NCC's **Access Point > Monitor > Access Points** screen or the connected gateway for the Zyxel Device's current LAN IP address. Alternatively, disconnect the gateway or disable its DHCP server function and use the Zyxel Device's default static LAN IP address (192.168.1.2).

**Figure 124** Cloud Mode Application



### 22.2 Cloud Mode Web Configurator Screens

When your Zyxel Device is managed through NCC, you can access only the following screens through the Web Configurator:

- **Dashboard**
- **Configuration > Network > IP Setting**
- **Configuration > Network > VLAN**
- **Maintenance > Shell Script**

- Maintenance > Diagnostics > Diagnostics
- Maintenance > Log

These screens also have fewer options than those in standalone Zyxel Devices. The rest of the Zyxel Device's features must be configured through the NCC.

## 22.3 Dashboard

This screen displays general AP information, and client information in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

**Figure 125** Dashboard



The following table describes the labels in this screen.

Table 79 Dashboard

Label	Description
AP Information	
MAC Address	This field displays the MAC address of the Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Product Model	This field displays the model name of the Zyxel Device.
2.4G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 2.4 GHz spectrum. This shows <b>Not activated</b> if the wireless LAN is disabled.
5G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 5 GHz spectrum. This shows <b>Not activated</b> if the wireless LAN is disabled.
Use Proxy to Access NCC	This displays whether the NAP uses a proxy server to access the NCC (Nebula Control Center).



Table 79 Dashboard (continued)

LABEL	DESCRIPTION
Cloud Control Status	<p>This field displays:</p> <ul style="list-style-type: none"> <li>The Zyxel Device Internet connection status.</li> <li>The connection status between the Zyxel Device and NCC.</li> <li>The Zyxel Device registration status on NCC.</li> </ul> <p>Mouse over the circles to display detailed information.</p> <p>To pass your Zyxel Device management to NCC, first make sure your Zyxel Device is connected to the Internet. Then go to NCC and register your Zyxel Device.</p> <p><b>1. Internet</b></p> <p>Green - The Zyxel Device is connected to the Internet.</p> <p>Orange - The Zyxel Device is not connected to the Internet.</p> <p><b>2. Nebula</b></p> <p>Green - The Zyxel Device is connected to NCC.</p> <p>Orange - The Zyxel Device is not connected to NCC.</p> <p><b>3. Registration</b></p> <p>Green - The Zyxel Device is registered on NCC.</p> <p>Gray - The Zyxel Device is not registered on NCC.</p>
Nebula Discovery	<p>Slide the switch to the right to enable NCC discovery on the Zyxel Device. The Zyxel Device will connect to NCC and change to the NCC management mode if it:</p> <ul style="list-style-type: none"> <li>is connected to the Internet.</li> <li>has been registered on NCC.</li> </ul> <p>Note: The switch is always on and cannot be disabled when the Zyxel Device is in Cloud mode.</p>

If the Zyxel Device cannot connect to the Internet or to NCC, move the mouse over the status circle to check the error message.



# CHAPTER 23

## Network

### 23.1 Overview

This chapter describes how you can configure the management IP address and VLAN settings of your Zyxel Device in cloud mode.

See [Section 9.1 on page 71](#) for information about IP addresses.

Note: Make sure your VLAN settings allow the Zyxel Device to connect to the Internet so you could manage it with NCC.

#### 23.1.1 What You Can Do in this Chapter

- The **IP Setting** screen ([Section 23.2 on page 194](#)) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen ([Section 23.3 on page 196](#)) configures the Zyxel Device's VLAN settings.

### 23.2 IP Setting

Use this screen to configure the IP address for your Zyxel Device. To access this screen, click **Configuration > Network > IP Setting**.

**Figure 126** Configuration > Network > IP Setting

Each field is described in the following table.

**Table 80** Configuration > Network > IP Setting

<b>LABEL</b>	<b>DESCRIPTION</b>
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
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.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
Use Proxy to Access Internet	If the Zyxel Device is behind a proxy server, you need to select this option and configure the proxy server settings so that the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter service port number used by the proxy server.
Authentication	Select this option if the proxy server requires authentication before it grants access to the Internet.
User Name	Enter your proxy user name.
Password	Enter your proxy password.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

## 23.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings. See [Section 9.3 on page 73](#) for more information about VLAN.

Use this screen to configure the VLAN settings for your Zyxel Device. To access this screen, click **Configuration > Network > VLAN**.

**Figure 127** Configuration > Network > VLAN

Each field is described in the following table.

Table 81 Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device.
Untagged/Tagged	Set whether the Zyxel Device adds the VLAN ID to outbound traffic transmitted through its Ethernet port.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Reset	Click <b>Reset</b> to return the screen to its last-saved settings.

# CHAPTER 24

## Maintenance

### 24.1 Overview

When the Zyxel Device is set to work in cloud mode, the **Maintenance** screens let you manage shell script files on the Zyxel Device, generate a diagnostic file, or view log messages.

See [Chapter 17 on page 172](#) for information about shell scripts.

#### 24.1.1 What You Can Do in this Chapter

- The **Shell Script** screen ([Section 24.2 on page 197](#)) stores, names, downloads, and uploads shell script files.
- The **Diagnostics** screen ([Section 24.3 on page 198](#)) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Log > View Log** screen ([Section 24.4 on page 199](#)) displays the Zyxel Device's current log messages when it is disconnected from the NCC.

### 24.2 Shell Script

Use shell script files to have the Zyxel Device use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, and upload shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

**Figure 128** Maintenance > Shell Script



Each field is described in the following table.

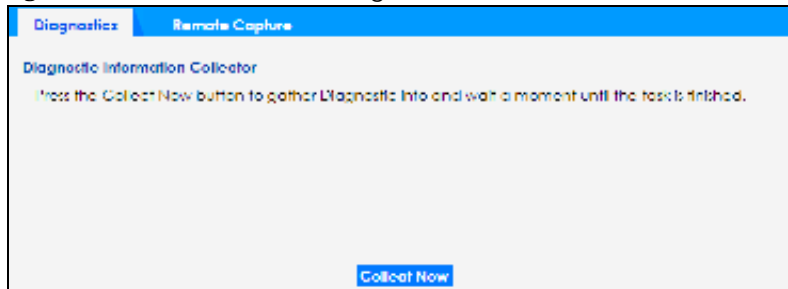
Table 82 Maintenance > Shell Script

LABEL	DESCRIPTION
Rename	<p>Use this button to change the label of a shell script file on the Zyxel Device.</p> <p>You cannot rename a shell script to the name of another shell script in the Zyxel Device.</p> <p>Click a shell script's row to select it and click <b>Rename</b> to open the <b>Rename File</b> screen.</p> <p>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9; '~!@#\$%^&amp;()_+[]{}',.-).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a shell script file's row to select it and click <b>Delete</b> to delete the shell script file from the Zyxel Device.</p> <p>A pop-up window asks you to confirm that you want to delete the shell script file. Click <b>OK</b> to delete the shell script file or click <b>Cancel</b> to close the screen without deleting the shell script file.</p>
Download	<p>Click a shell script file's row to select it and click <b>Download</b> to save the configuration to your computer.</p>
Copy	<p>Use this button to save a duplicate of a shell script file on the Zyxel Device.</p> <p>Click a shell script file's row to select it and click <b>Copy</b> to open the <b>Copy File</b> screen.</p> <p>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9; '~!@#\$%^&amp;()_+[]{}',.-).</p> <p>Click <b>OK</b> to save the duplicate or click <b>Cancel</b> to close the screen without saving a duplicate of the configuration file.</p>
#	<p>This column displays the number for each shell script file entry.</p>
File Name	<p>This column displays the label that identifies a shell script file.</p>
Size	<p>This column displays the size (in KB) of a shell script file.</p>
Last Modified	<p>This column displays the date and time that the individual shell script files were last changed or saved.</p>
Upload Shell Script	<p>The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.</p>
File	<p>Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.</p>
Browse...	<p>Click <b>Browse...</b> to find the .zysh file you want to upload.</p>
Upload	<p>Click <b>Upload</b> to begin the upload process. This process may take up to several minutes.</p>

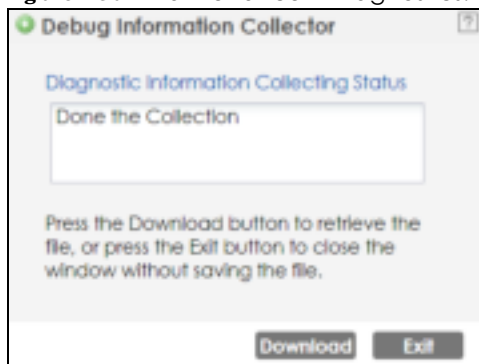
## 24.3 Diagnostics

This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

Click **Maintenance > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

**Figure 129** Maintenance > Diagnostics

The **Debug Information Center** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

**Figure 130** Maintenance > Diagnostics: Debug Information Collector

## 24.4 View Log

The NCC periodically gathers log files from the devices being managed by it. Before the NCC pulls logs from the Zyxel Device or when the Zyxel Device is disconnected from the NCC, you can use this screen to view its current log messages. To access this screen, click **Maintenance > Log**.

Note: 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.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 131** Maintenance > Log > View Log

**View Log**

☐ Hide Filter

**Log**

Log will be displayed when this access point is not connected to the Nebula.

Display:  Priority:

Source Address:  Destination Address:

Source Interface:  Destination Interface:

Protocol:  Keyword:

Time	Message	Source	Destination	Note
2019-11-27 06:4...	Port 0 is up! The link speed is 1000M/full.			
2019-11-27 06:4...	Port 0 is down!			
2019-11-27 06:3...	Enterprise WLAN is configured successfully with s...			
2019-11-27 06:3...	Port 0 is up! The link speed is 1000M/full.			
2019-11-27 06:3...	Port 0 is down!			

Page 1 of 1 Showing 5 items

The following table describes the labels in this screen.

**Table 83** Maintenance > Log > View Log

Label	Description
Show Filter / Hide Filter	Click this button to show or hide the filter settings.  If the filter settings are hidden, the <b>Display</b> , <b>Email Log Now</b> , <b>Refresh</b> , and <b>Clear Log</b> fields are available.  If the filter settings are shown, the <b>Display</b> , <b>Priority</b> , <b>Source Address</b> , <b>Destination Address</b> , <b>Source Interface</b> , <b>Destination Interface</b> , <b>Protocol</b> , <b>Keyword</b> , and <b>Search</b> fields are available.
Display	Select the category of log message(s) you want to view. You can also view <b>All Logs</b> at one time, or you can view the <b>Debug Log</b> .
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: <b>any</b> , <b>emerg</b> , <b>alert</b> , <b>crit</b> , <b>error</b> , <b>warn</b> , <b>notice</b> , and <b>info</b> , from highest priority to lowest priority. This field is read-only if the <b>Category</b> is <b>Debug Log</b> .
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the <b>Message</b> , <b>Source</b> , <b>Destination</b> and <b>Note</b> fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ( ) ' , ; : ? ! + - * / = # \$ % @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.



Table 83 Maintenance &gt; Log &gt; View Log (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the <b>Priority</b> field above.
Category	This field displays the log that generated the log message. It is the same value used in the <b>Display</b> and (other) <b>Category</b> fields.
Message	This field displays the reason the log message was generated. The text "[count=x]", where <i>x</i> is a number, appears at the end of the <b>Message</b> field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.
Protocol	This field displays the service protocol in the event that generated the log message.
Note	This field displays any additional information about the log message.

---

# **PART III**

## **Appendices and Troubleshooting**

---

# CHAPTER 25

## Troubleshooting

### 25.1 Overview

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

- [Power, Hardware Connections, and LED](#)
- [Zyxel Device Management, Access, and Login](#)
- [Internet Access](#)
- [WiFi Network](#)
- [Resetting the Zyxel Device](#)

### 25.2 Power, Hardware Connections, and LED

---

[The Zyxel Device does not turn on. The LED is not on.](#)

---

- 1 Make sure you are using the power adapter included with the Zyxel Device or a PoE power injector/switch.
- 2 Make sure the power adapter or PoE power injector/switch is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adapter or PoE power injector/switch.
- 4 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 5 If none of these steps work, you may have faulty hardware and should contact your Zyxel Device vendor.

---

[The LED does not behave as expected.](#)

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 3.1 on page 30](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

- 4 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.
- 5 If the problem continues, contact the vendor.

## 25.3 Zyxel Device Management, Access, and Login

---

### I forgot the IP address for the Zyxel Device.

---

- 1 The default in-band IP address in standalone mode is **http://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.2**.
- 2 If you changed the IP address and have forgotten it, you have to reset the Zyxel Device to its factory defaults. See [Section 25.6 on page 210](#).
- 3 If your Zyxel Device is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- 4 If the NCC has managed the Zyxel Device, you can also check the NCC's **AP > Monitor > Access Point** screen for the Zyxel Device's current LAN IP address.

### 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 (in standalone mode) is 192.168.1.2.
  - 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 Zyxel Device](#).
- 2 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and [Section 3.1 on page 30](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 Make sure your computer is in the same subnet as the Zyxel Device. (If you know that there are routers between your computer and the Zyxel Device, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the Zyxel Device.
- 5 Reset the Zyxel Device to its factory defaults, and try to access the Zyxel Device with the default IP address. See [Section 25.6 on page 210](#).

- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Try to access the Zyxel Device using another service, such as SSH. If you can access the Zyxel Device, check the remote management settings to find out why the Zyxel Device does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

---

**I forgot the password.**

---

- 1 The default password is **1234**. If the Zyxel Device is connected to the NCC and registered, check the NCC for the password.
- 2 If this does not work, you have to reset the Zyxel Device to its factory defaults. See [Section 25.6 on page 210](#).

---

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

---

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.
- 3 If this does not work, you have to reset the Zyxel Device to its factory defaults. See [Section 25.6 on page 210](#).

---

**I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.**

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the Web Configurator](#). Ignore the suggestions about your browser.

---

**I cannot access the Zyxel Device directly anymore after switching to NCC management.**

---

- Check the Zyxel Device IP address and login credentials using the NCC and use them to access the Zyxel Device. Note that the built-in Web Configurator will have limited functionality when managed through NCC.

---

I enabled **NCC Discovery**, but the Zyxel Device is still in standalone mode.

---

Make sure your Zyxel Device is registered to the NCC.

---

The Zyxel Device is already registered with NCC, but it is still in standalone mode; it cannot connect to the NCC.

---

- 1 Make sure that NCC Discovery is enabled (see [Section 9.4 on page 76](#)).
- 2 Check your network's firewall/security settings. Make sure the following TCP ports are allowed: 443, 4335, and 6667.
- 3 Make sure your Zyxel Device can access the Internet.
- 4 Check your network's VLAN settings (see [Section 9.3 on page 73](#)). You may have to change the Management VLAN settings of the Zyxel Device to allow it to connect to the Internet and access the NCC.

Note: Changing the management VLAN and IP address settings on the Zyxel Device also pushes these changes to the NCC. Do this only if your device cannot otherwise connect to the NCC.

- 5 Make sure your Zyxel Device does not have to go through network authentication such as a captive portal. If your network uses a captive portal, the network administrator may have to create a new VLAN without this requirement. Change your Zyxel Device's management VLAN settings as necessary.

---

Some features I set using the NCC do not work as expected.

---

- 1 Make sure your Zyxel Device can access the Internet.
- 2 Check your network's firewall/security settings. Make sure the following ports are allowed:
  - TCP: 443, 4335, and 6667
  - UDP: 123
- 3 After changing your Zyxel Device settings using the NCC, wait 1-2 minutes for the changes to take effect.

---

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

---

When a log reaches the maximum number of log messages (see [Section 1.2 on page 12](#)), new log messages automatically overwrite the oldest log messages.

---

### The commands in my configuration file or shell script are not working properly.

---

- In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the Zyxel Device treat the line as a comment.
- Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the Zyxel Device exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Note: “exit” or “!” must follow sub commands if it is to make the Zyxel Device exit sub command mode.

---

### I cannot upload the firmware uploaded using FTP.

---

The Web Configurator is the recommended method for uploading firmware in standalone mode. For managed Zyxel Devices, using the NCC or AC is recommended. You only need to use FTP if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

## 25.4 Internet Access

---

### Clients cannot access the Internet through the Zyxel Device.

---

- 1 Check the Zyxel Device's hardware connections, and make sure the LEDs are behaving as expected (refer to [Section 3.1 on page 30](#)). See the Quick Start Guide and [Section 25.1 on page 203](#).
- 2 Make sure the Zyxel Device is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- 3 If clients are trying to access the Internet wirelessly, make sure the WiFi settings on the WiFi clients are the same as the settings on the Zyxel Device.
- 4 Disconnect all the cables from your Zyxel Device, and follow the directions in the Quick Start Guide again.
- 5 Reboot the client and reconnect to the Zyxel Device.
- 6 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. Look at the LEDs, and check [Section 3.1 on page 30](#). If the Zyxel Device 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 using the NCC, AC, Zyxel Device Web Configurator, or the client device itself. If the signal is weak, try moving the client closer to the Zyxel Device (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
- 3 Reboot the Zyxel Device using the Web Configurator/CLI or the NCC or AC.
- 4 Check the settings for QoS. If it is disabled, activate it. When enabled, raise or lower the priority for some applications.
- 5 If the problem continues, contact the network administrator or vendor.

## 25.5 WiFi Network

---

[The WiFi connection is slow or intermittent.](#)

---

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your WiFi device closer to the Zyxel Device if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the wireless client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

---

[I cannot access the Zyxel Device or ping any computer from the WLAN.](#)

---

- 1 Make sure the wireless LAN (wireless radio) is enabled on the Zyxel Device.
- 2 Make sure the radio or at least one of the Zyxel Device's radios is operating in AP mode.
- 3 Make sure the wireless adapter (installed on your computer) is working properly.
- 4 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the Zyxel Device's active radio.



- 5 Make sure your computer (with a wireless adapter installed) is within the transmission range of the Zyxel Device.
- 6 Check that both the Zyxel Device 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.

---

### The wireless security is not following the re-authentication timer setting I specified.

---

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

---

### I cannot import a certificate into the Zyxel Device.

---

- 1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.
- 2 You must remove any spaces from the certificate's filename before you can import the certificate.
- 3 Any certificate that you want to import has to be in one of these file formats:
  - Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
  - PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
  - Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKCS#7 file that contains a single certificate.
  - PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
  - Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

## 25.6 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following procedure to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

- 1 Make sure the Power LED is on and not blinking.
- 2 Press the **RESET** button and hold it until the Power LED begins to blink. (This usually takes about ten seconds.)
- 3 Release the **RESET** button, and wait for the Zyxel Device to restart.

You should be able to access the Zyxel Device in standalone mode using the default settings.

## 25.7 Getting More Troubleshooting Help

Search for support information for your model at [www.zyxel.com](http://www.zyxel.com) for more troubleshooting suggestions.




# APPENDIX A

## Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many Zyxel products, such as the Zyxel Device, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the Zyxel-created certificate into your web browser and flag that certificate as a trusted authority.

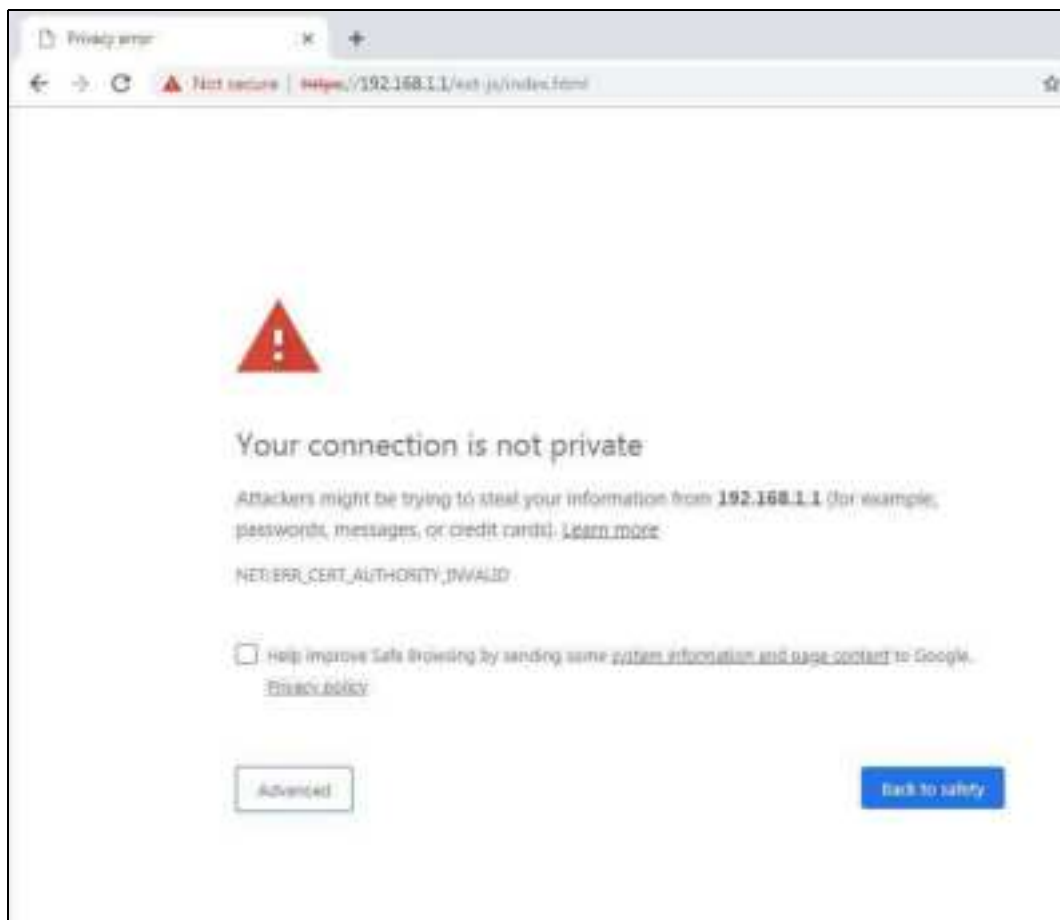
Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (  ) somewhere in the main browser window (not all browsers show the padlock in the same location).

### Google Chrome

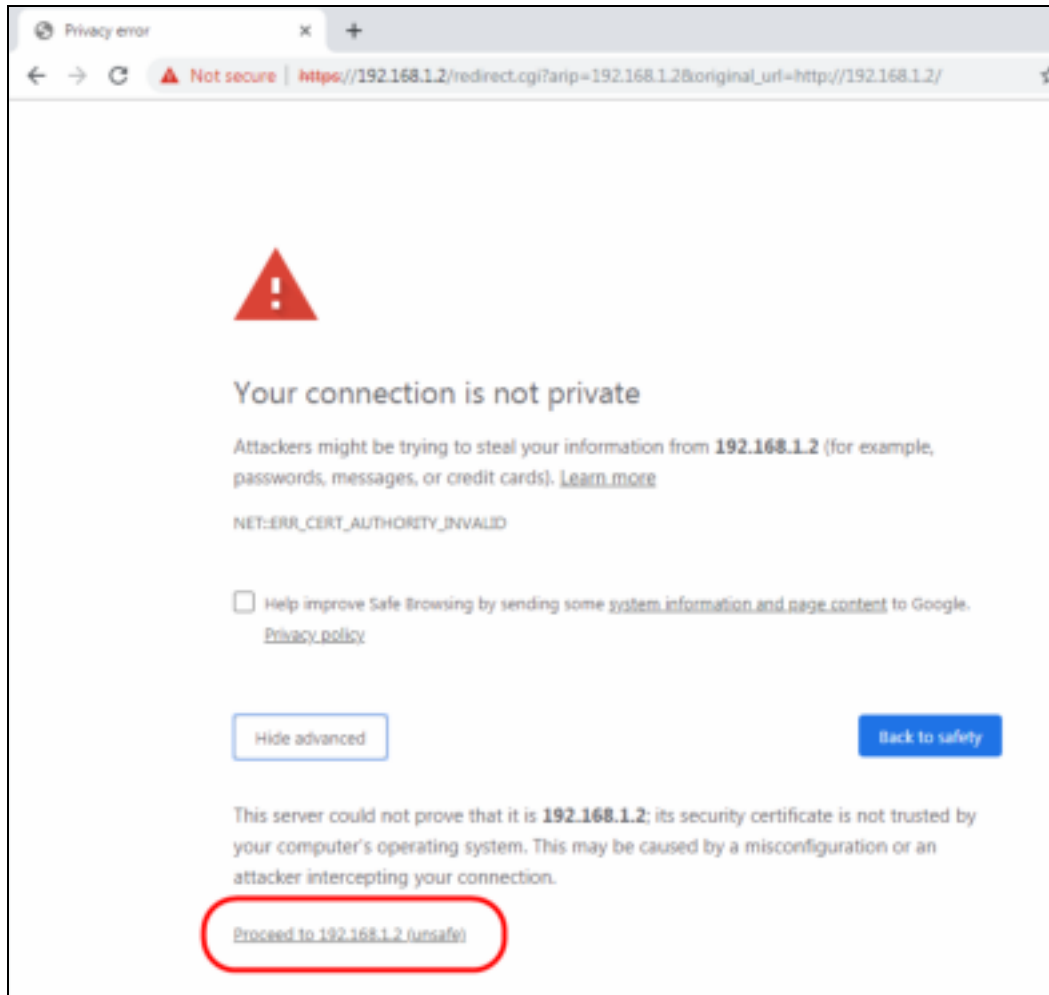
The following example uses Google Chrome on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

## Export a Certificate

- 1 If your device's Web Configurator is set to use SSL certification, then upon browsing with it for the first time, you are presented with a certification error.



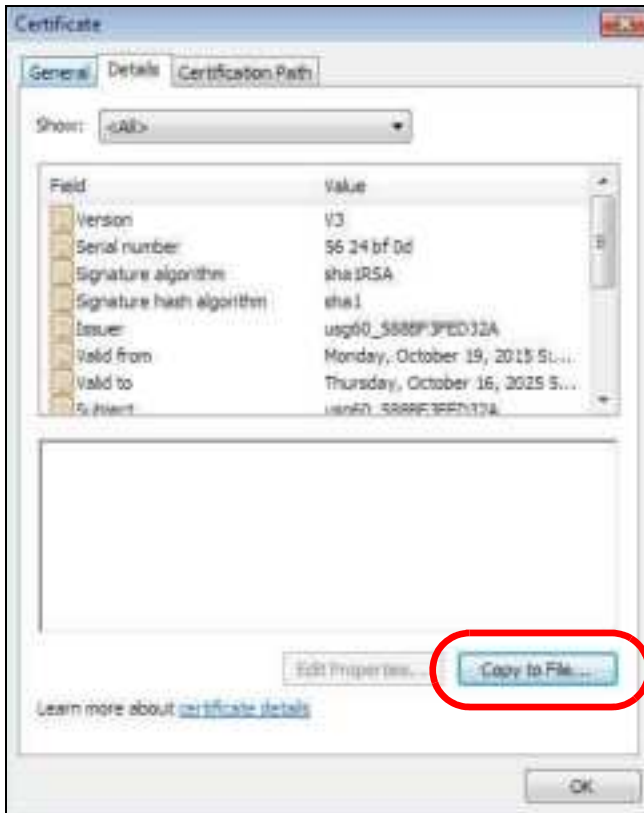
- 2 Click **Advanced** > **Proceed to x.x.x.x (unsafe)**.



- 3 In the **Address Bar**, click **Not Secure** > **Certificate (Invalid)**.



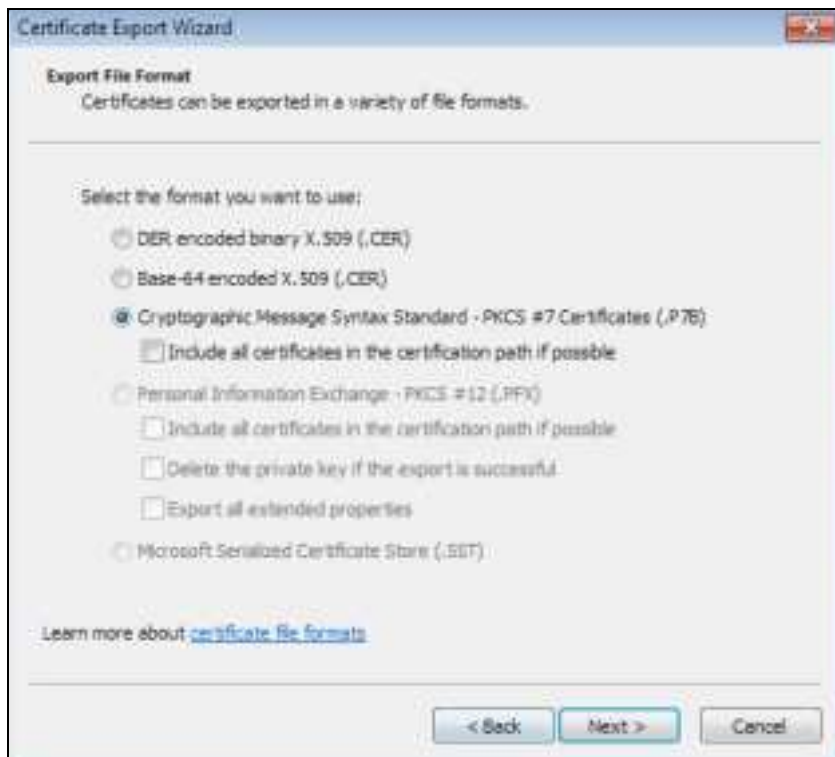
- 4 In the **Certificate** dialog box, click **Details > Copy to File**.



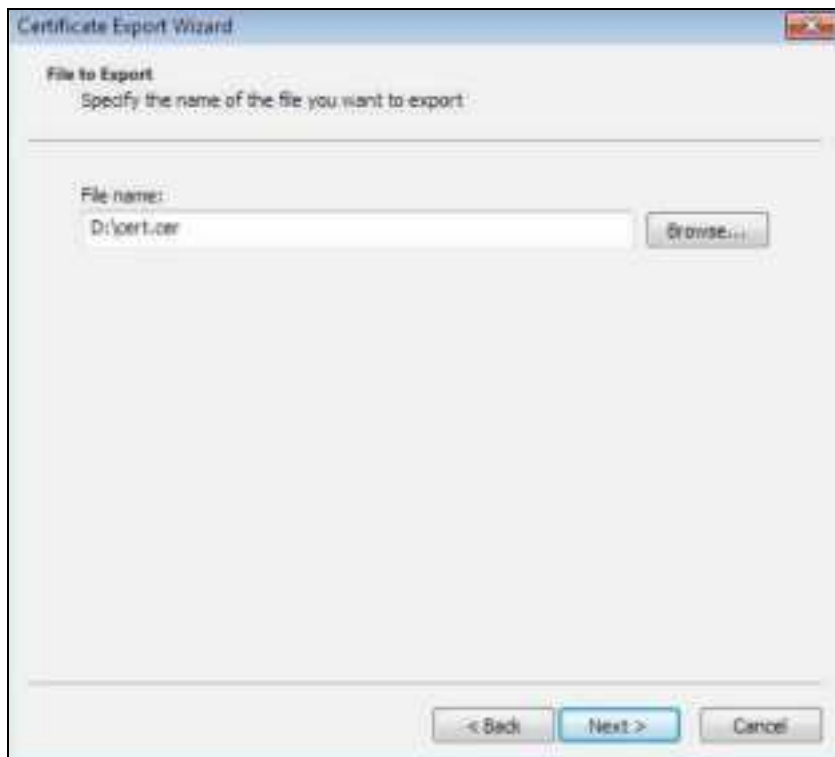
- 5 In the **Certificate Export Wizard**, click **Next**.



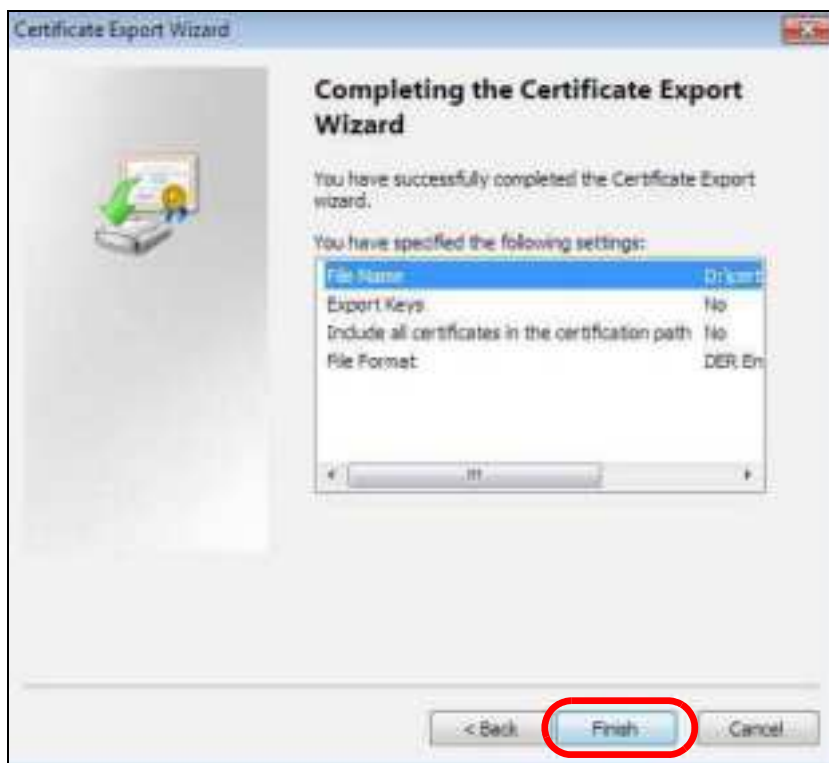
- 6 Select the format and settings you want to use and then click **Next**.



- 7 Type a filename and specify a folder to save the certificate in. Click **Next**.



- 8 In the **Completing the Certificate Export Wizard** screen, click **Finish**.



- 9 Finally, click **OK** when presented with the successful certificate export message.

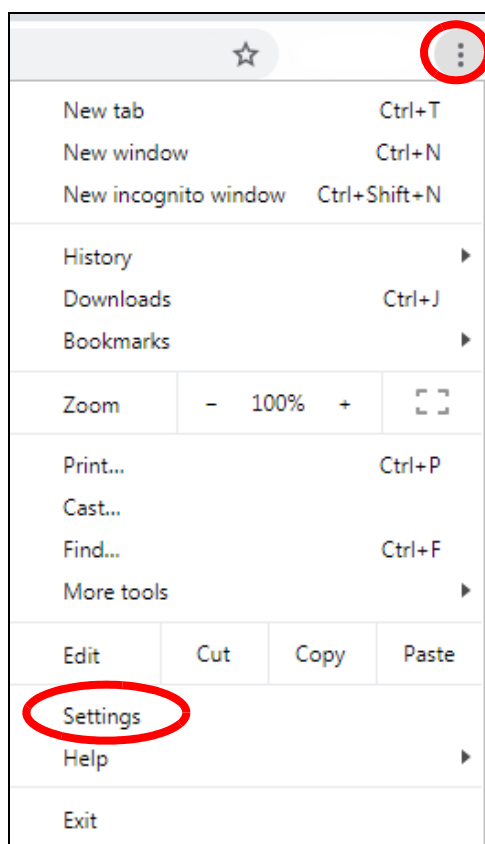


## Import a Certificate

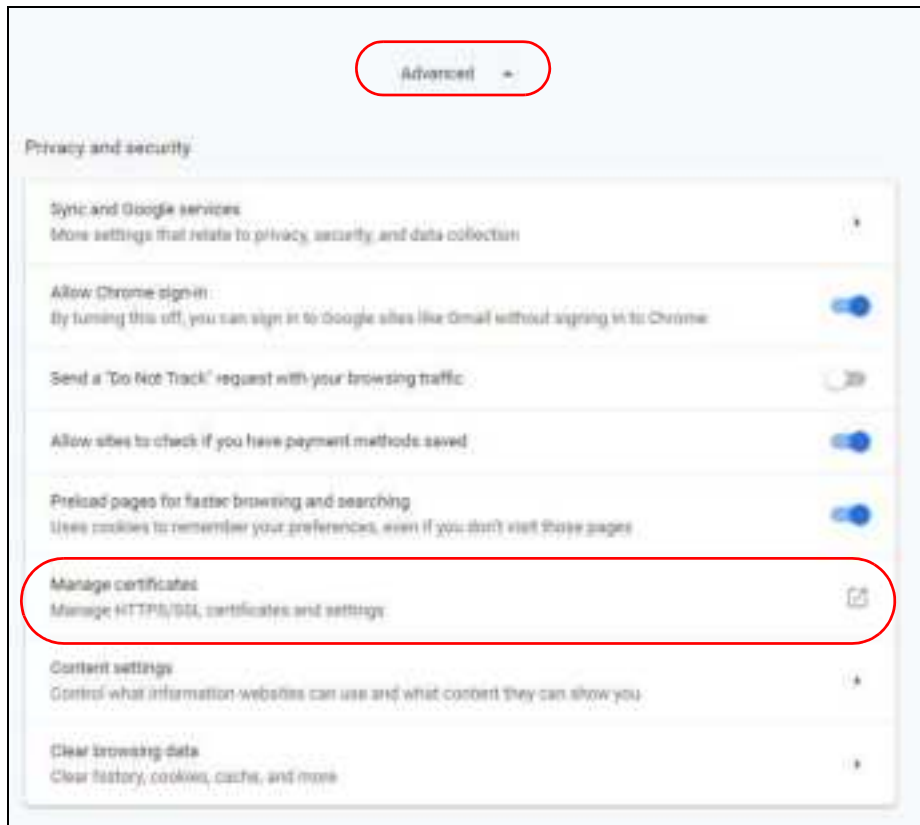
After storing the certificate in your computer (see [Export a Certificate](#)), you need to install it as a trusted root certification authority using the following steps:



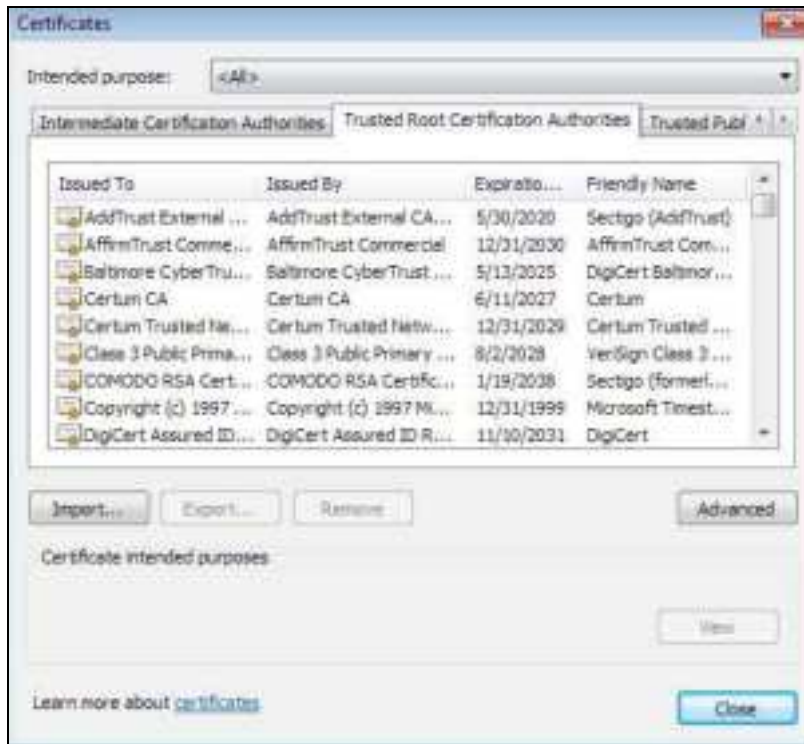
- 1 Open your web browser, click the menu icon, and click **Settings**.



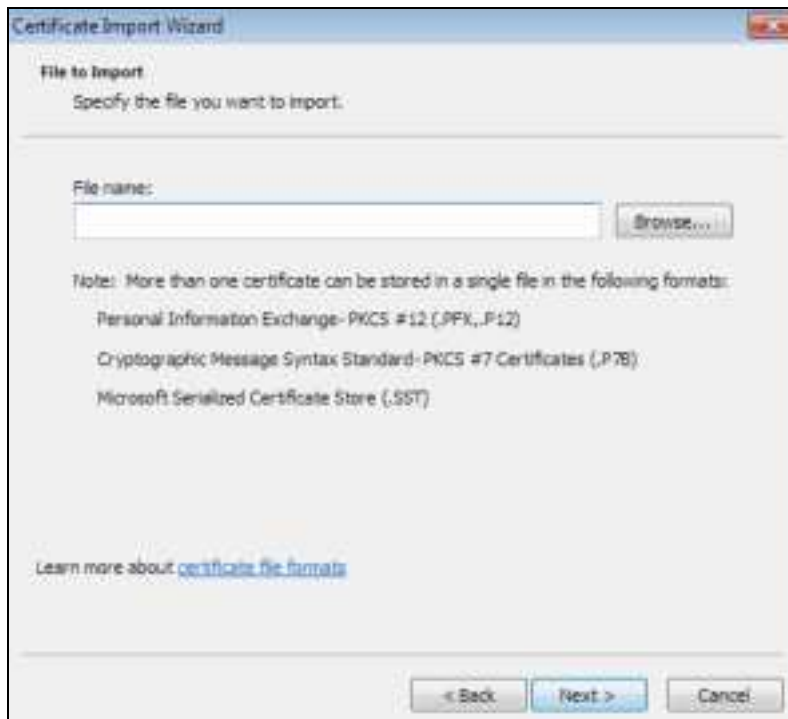
- 2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



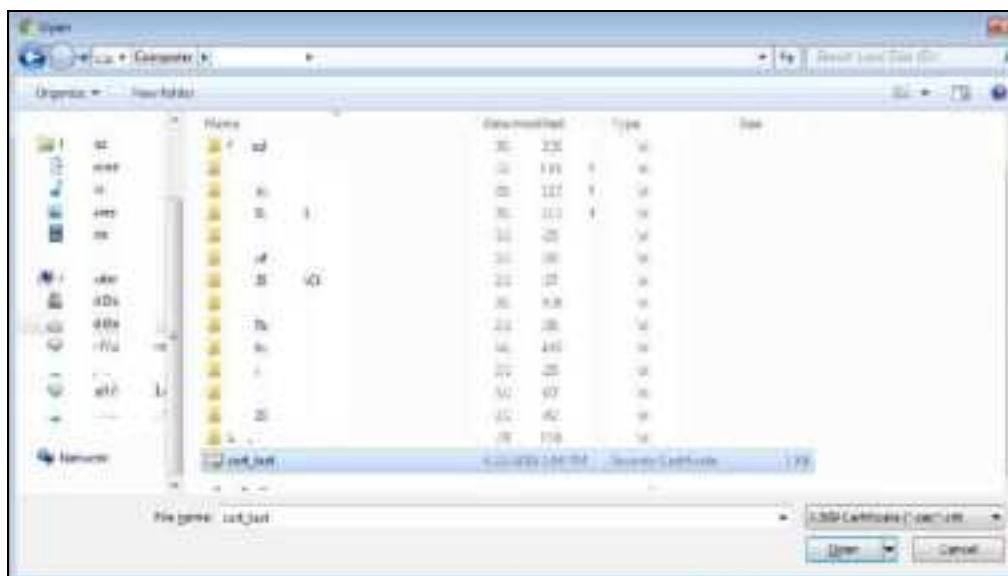
- 3 In the **Certificates** pop-up screen, click **Trusted Root Certification Authorities**. Click **Import** to start the **Certificate Import Wizard**.



- 4 Click **Next** when the wizard pops up, and then on the following screen click **Browse**.



- 5 Select the certificate file you want to import and click **Open**.



- 6 Click **Next**.



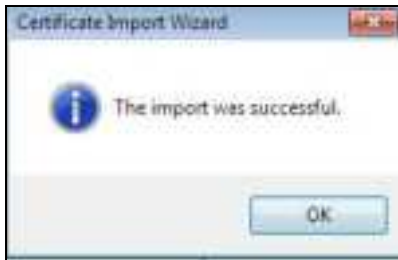
- 7 Confirm the settings displayed and click **Finish**.



- 8 If presented with a security warning, click **Yes**.



- 9 Finally, click **OK** when you are notified of the successful import.



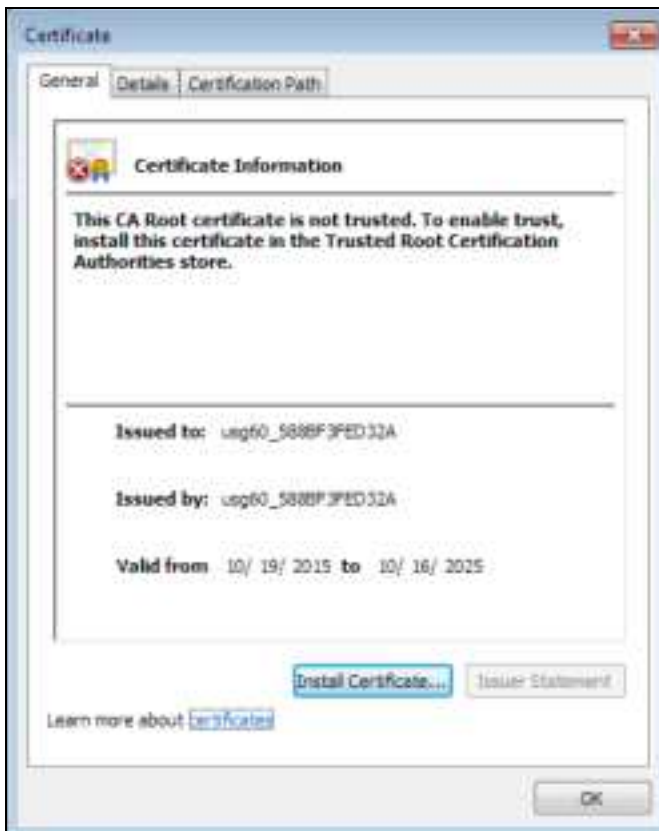
## Install a Stand-Alone Certificate File

Rather than installing a public key certificate using web browser settings, you can install a stand-alone certificate file if one has been issued to you.

- 1 Double-click the public key certificate file.



- 2 Click **Install Certificate**.



- 3 Click **Next** on the first wizard screen, click **Place all certificates in the following store**, and click **Browse**.



- 4 Select **Trusted Root Certificate Authorities** > **OK**, and then click **Next**.



- 5 Confirm the information shown on the final wizard screen and click **Finish**.



- 6 If presented with a security warning, click **Yes**.





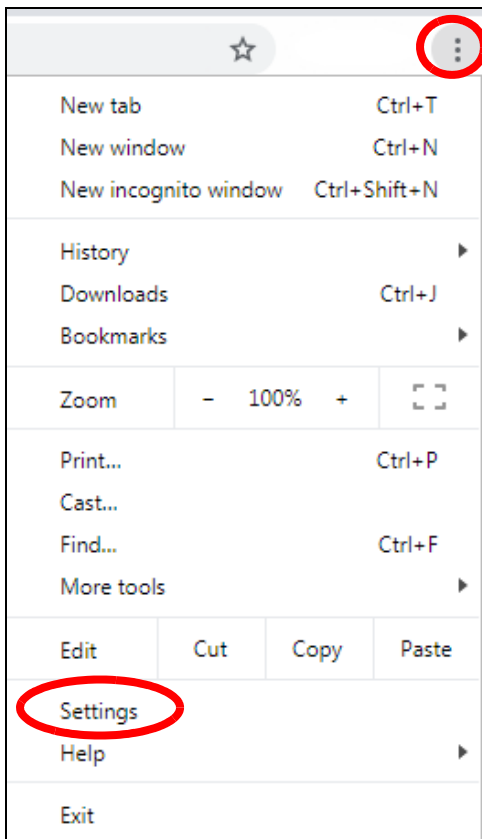
- 7 Finally, click **OK** when you are notified of the successful import.



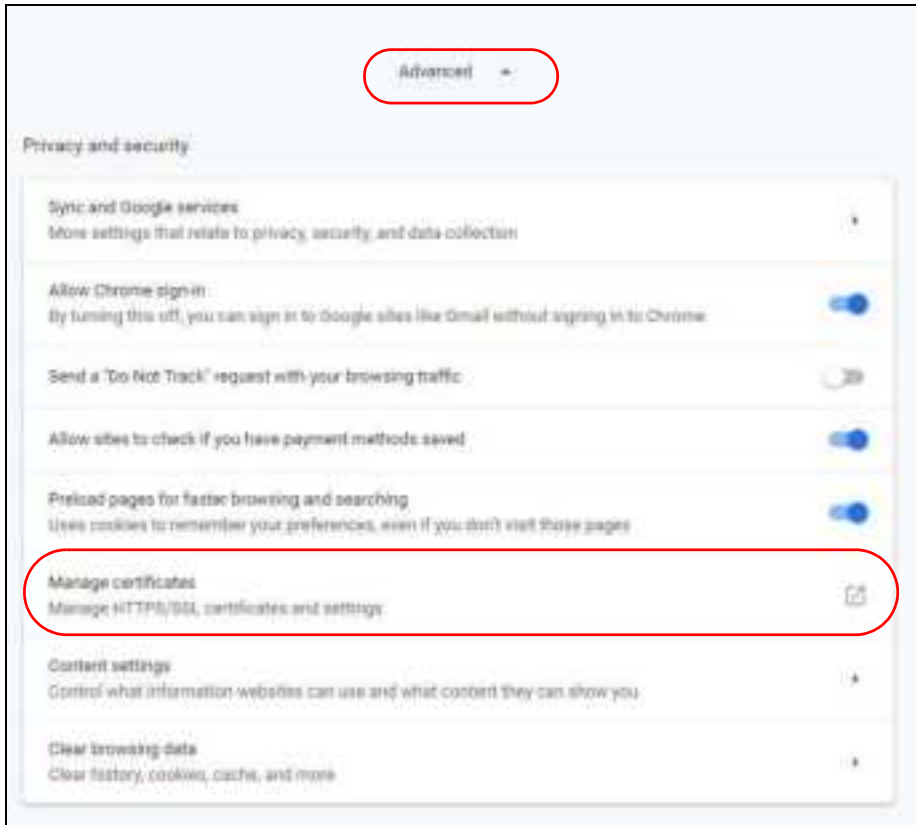
## Remove a Certificate in Google Chrome

This section shows you how to remove a public key certificate in Google Chrome on Windows 7.

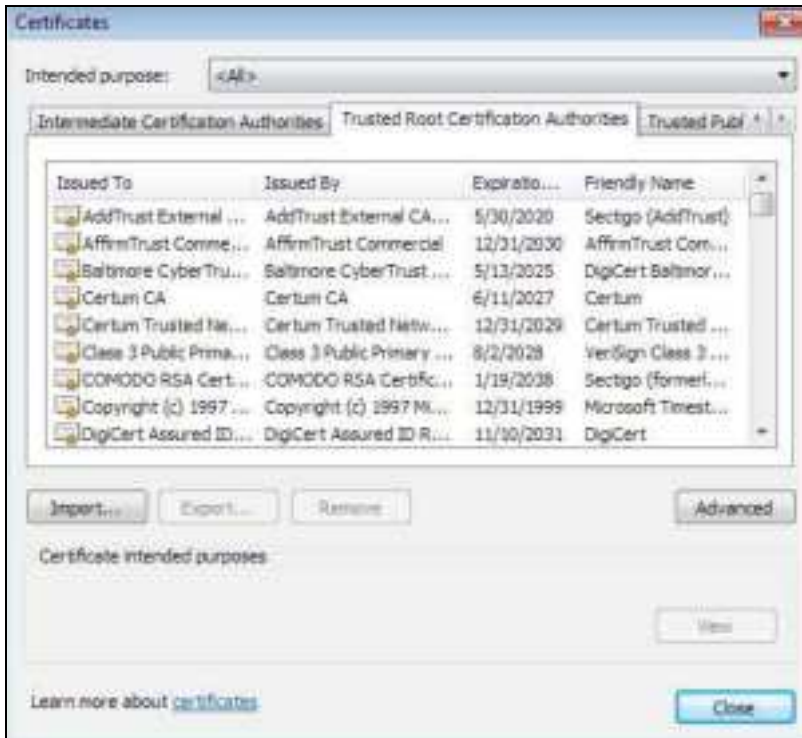
- 1 Open your web browser, click the menu icon, and click **Settings**.



- 2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



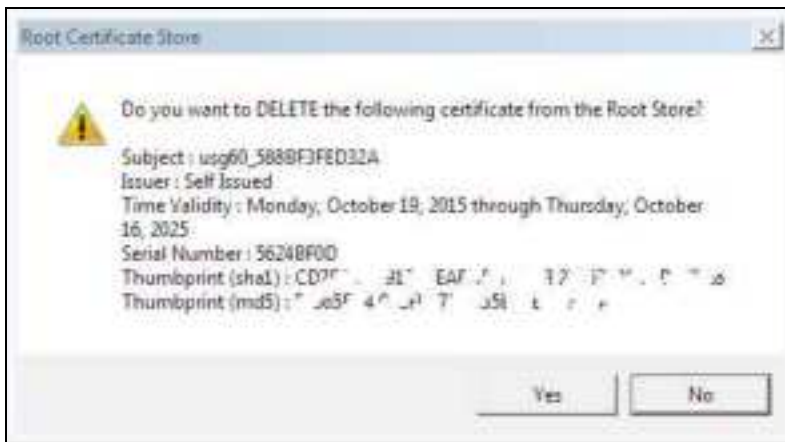
- 3 In the Certificates pop-up screen, click **Trusted Root Certification Authorities**.



- 4 Select the certificate you want to remove and click **Remove**.
- 5 Click **Yes** when you see the following warning message.



- 6 Confirm the details displayed in the warning message and click **Yes**.

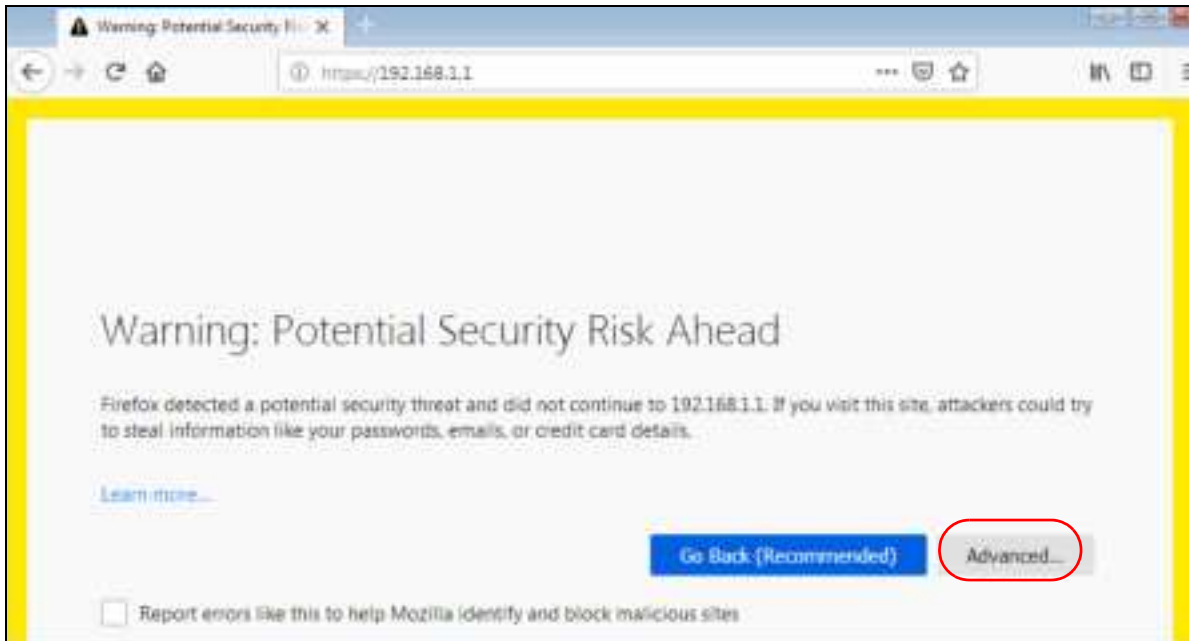


## Fire fo x

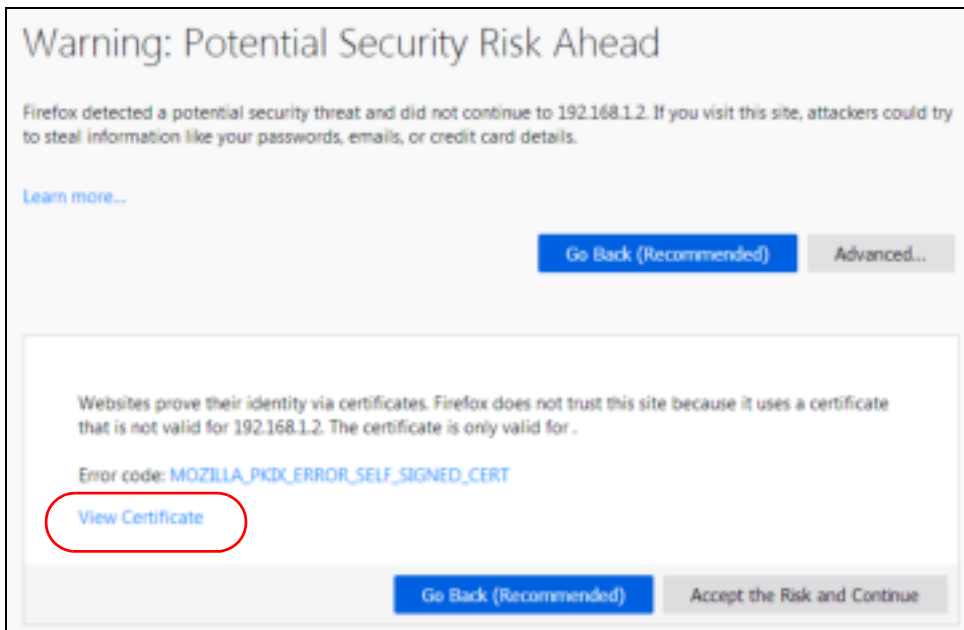
The following example uses Mozilla Firefox on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

## Export a Certificate

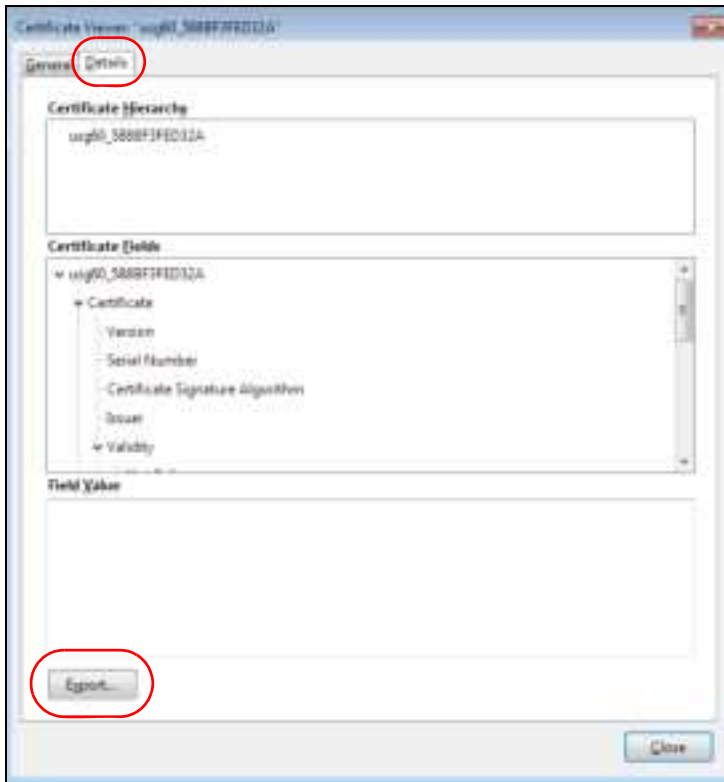
- 1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error. Click **Advanced**.



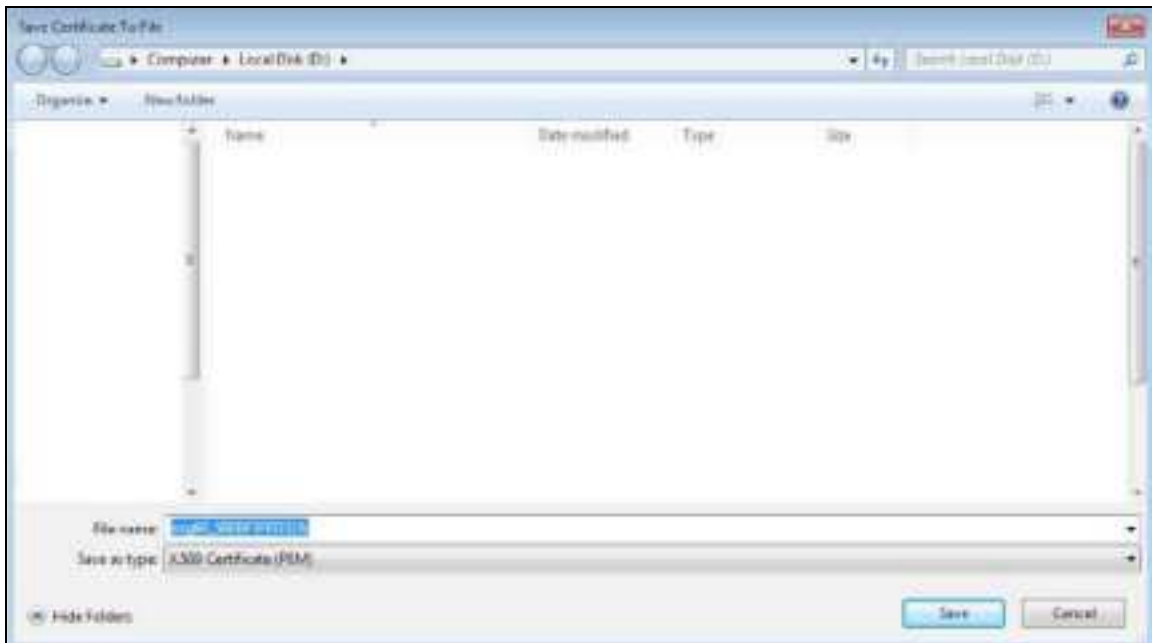
- 2 Click **View Certificate**.



- 3 Click **Details** > **Export**.



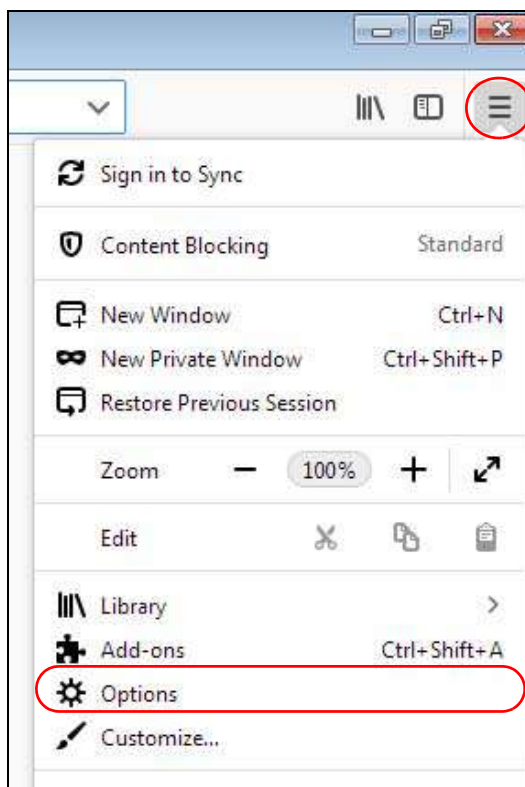
- 4 Type a filename and click **Save**.



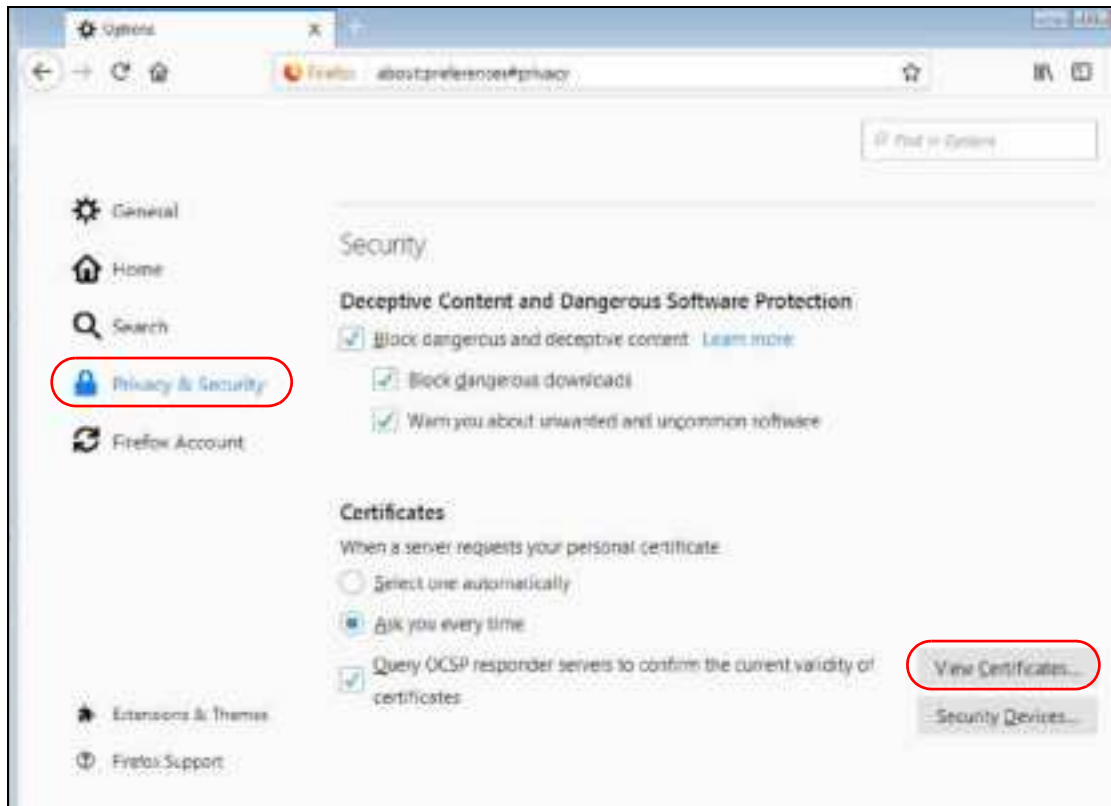
## Import a Certificate

After storing the certificate in your computer, you need to import it in trusted root certification authorities using the following steps:

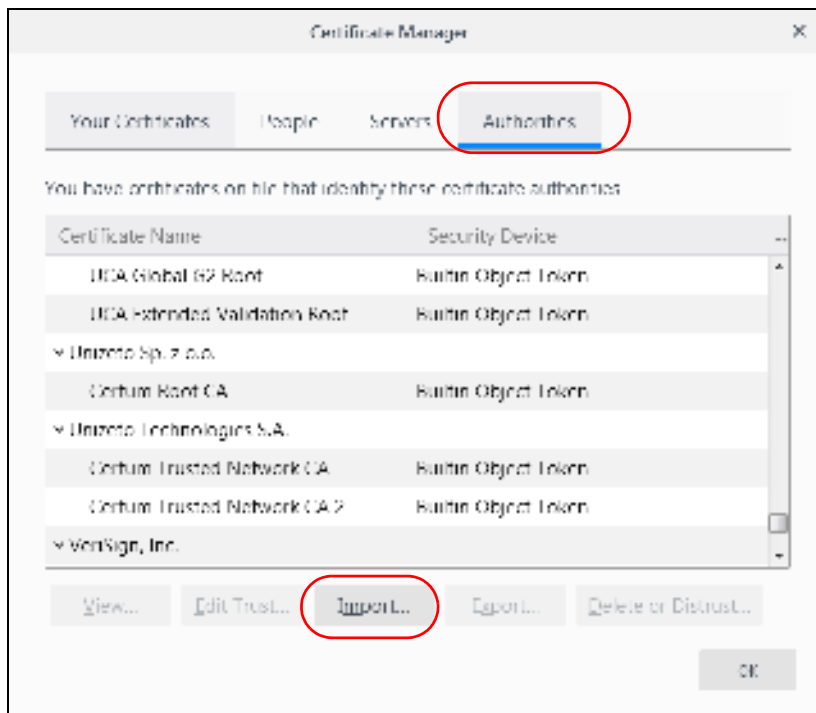
- 1 Open **Firefox** and click **Tools > Options**.



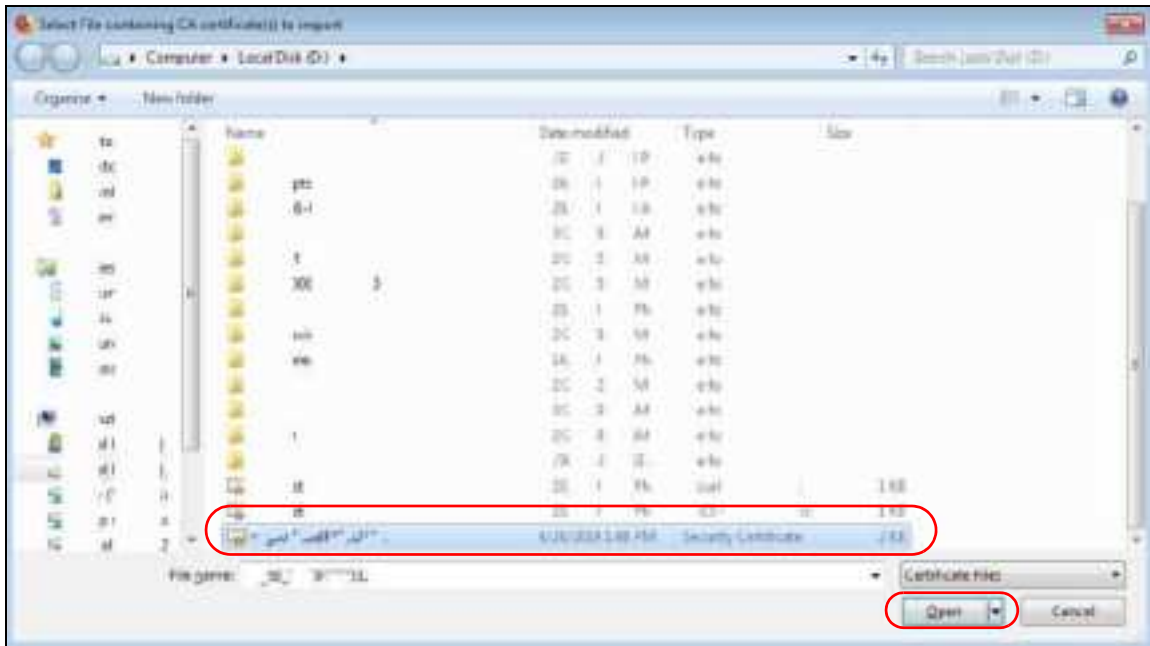
- 2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



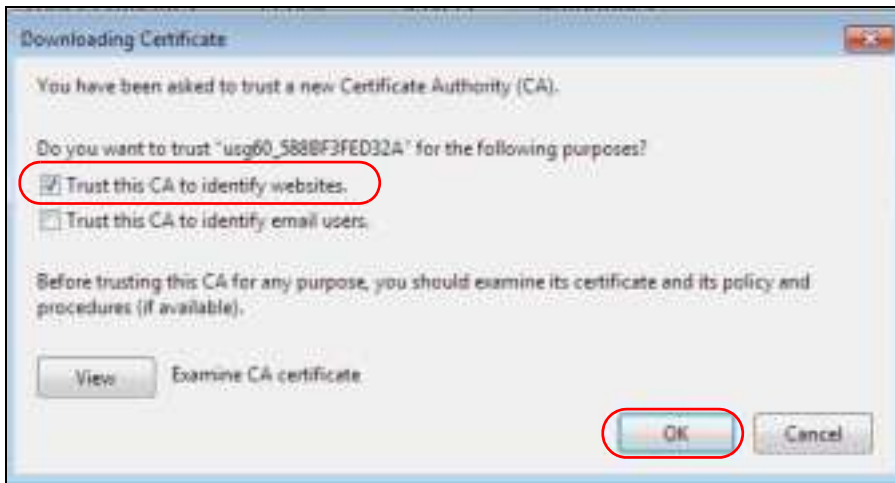
- 3 In the **Certificate Manager**, click **Authorities > Import**.



- 4 Use the **Select File** dialog box to locate the certificate and then click **Open**.



- 5 Select **Trust this CA to identify websites** and click **OK**.

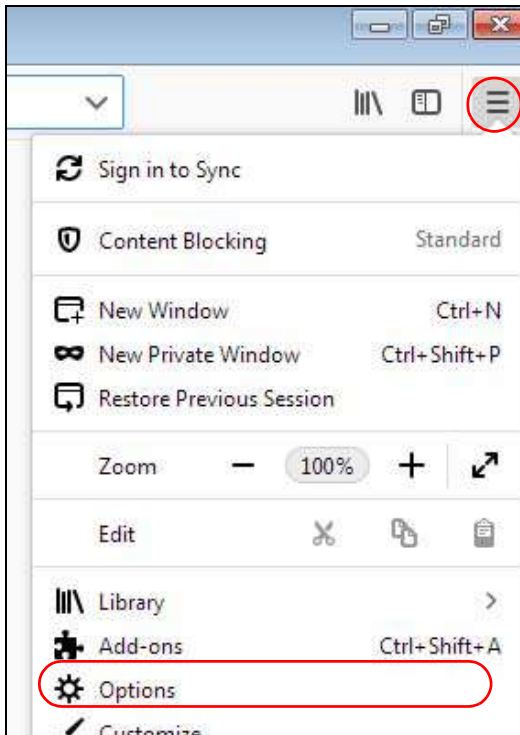


## Removing a Certificate in Firefox

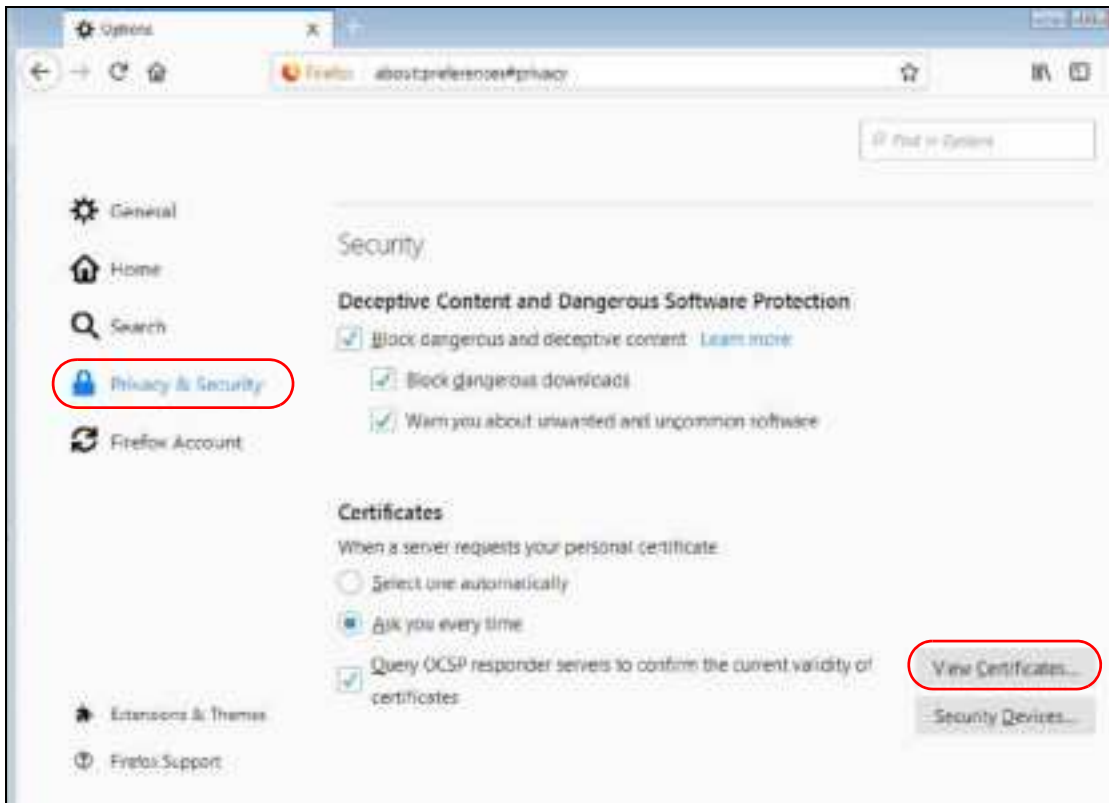
This section shows you how to remove a public key certificate in Firefox.



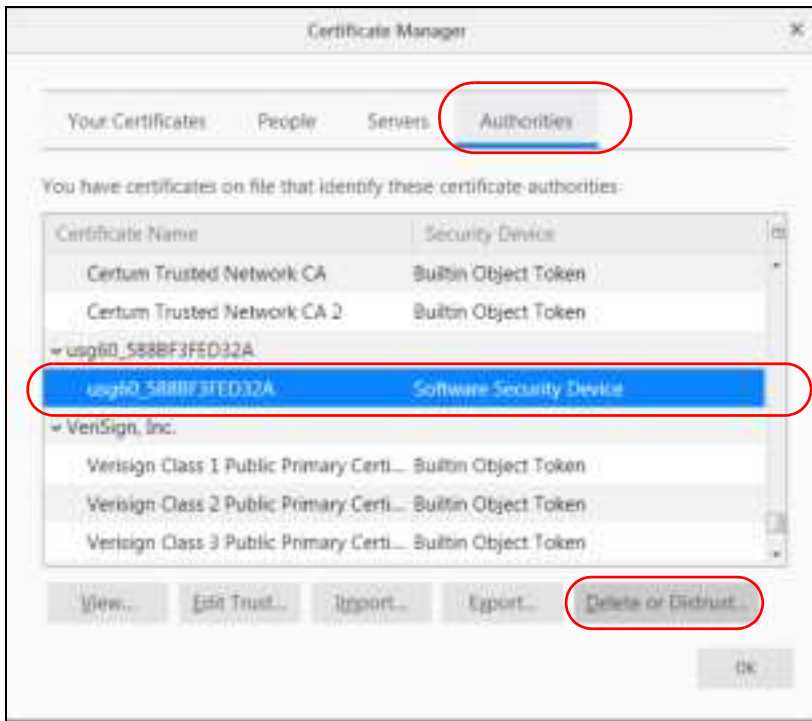
- 1 Open **Firefox** and click **Tools > Options**.



- 2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



- 3 In the **Certificate Manager**, click **Authorities** and select the certificate you want to remove. Click **Delete or Distrust**.



- 4 In the following dialog box, click **OK**.



- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

# APPENDIX B

## IPv6

### Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses.

### IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` Or `2001:db8:0:0:1a2f::15`.

### Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

### Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of `fe80::/10`. The link-local unicast address format is as follows.

Table 84 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

### Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

## Unspecified Address

An unspecified address (0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

## Loopback Address

A loopback address (0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

## Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 85 Predefined Multicast Address

MULTICASTADDRESS	DESCRIPTION
FF01:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 86 Reserved Multicast Address

MULTICASTADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

## Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

## Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 87

<b>MAC</b>	00	:	13	:	49	:	12	:	34	:	56
------------	----	---	----	---	----	---	----	---	----	---	----

Table 88

<b>EUI-64</b>	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56
---------------	----	---	----	---	----	---	----	---	----	---	----	---	----	---	----

## Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see [Interface ID](#) and [EUI-64](#)) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Zyxel Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates <sup>1</sup>another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

## DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

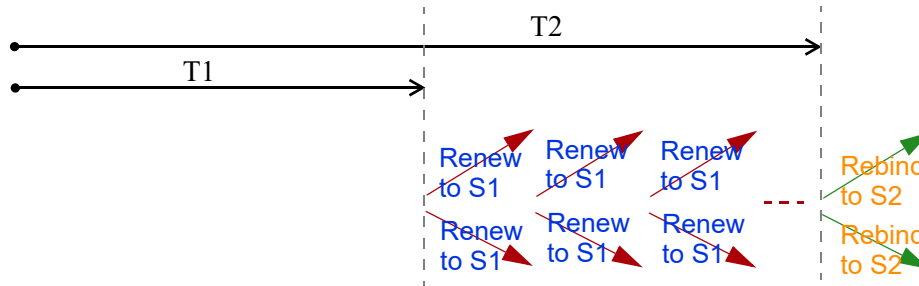
1. In IPv6, all network interfaces can be associated with several addresses.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

## Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA\_NA means an identity association for non-temporary addresses and IA\_TA is an identity association for temporary addresses. An IA\_NA option contains the T1 and T2 fields, but an IA\_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA\_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA\_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA\_TA, the client may send a Renew or Rebind message at the client's discretion.



## DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

## Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

## ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

## Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

## IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive

multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

## MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

## Example - Enabling IPv6 on Windows XP/ 2003/ Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

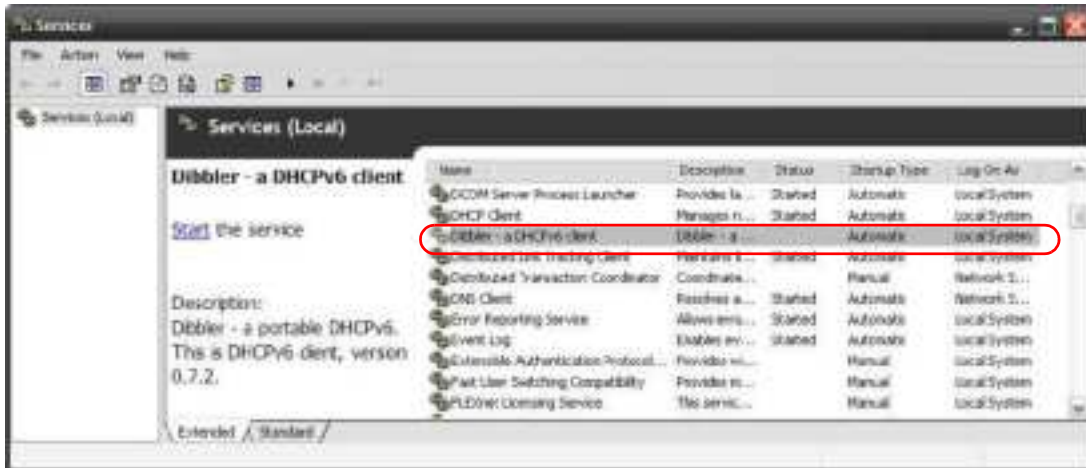
## Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

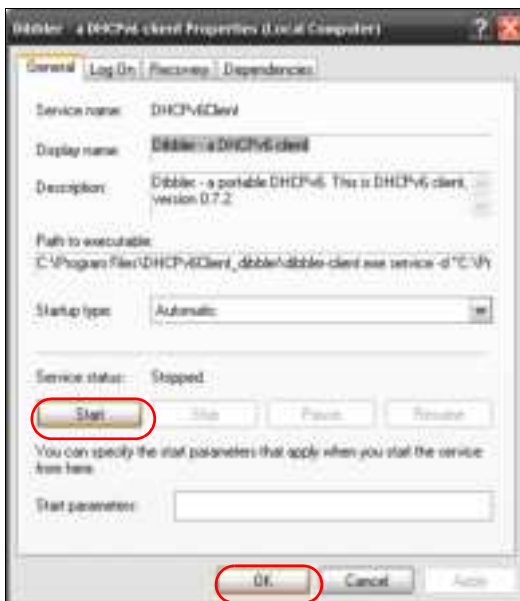
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:



- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click **Dibbler - a DHCPv6 client**.



- 5 Click **Start** and then **OK**.



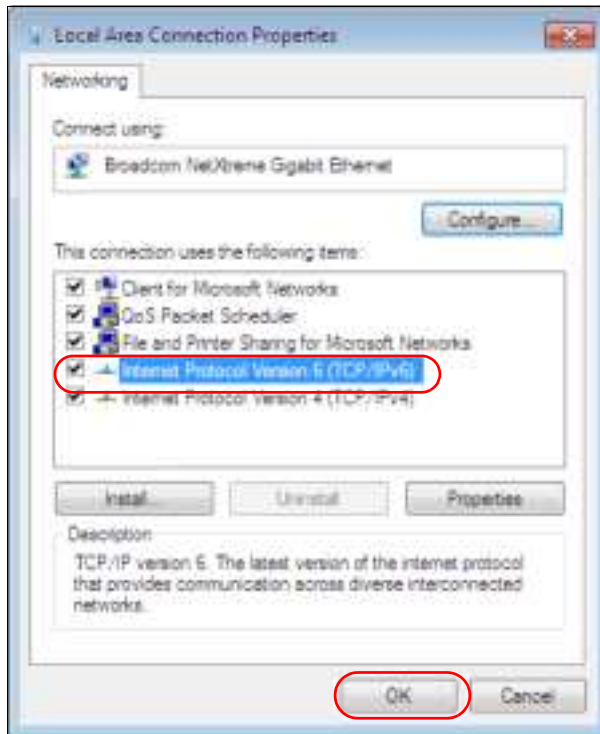
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

## Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

# APPENDIX C

## 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.

For Zyxel Communications offices, see <https://service-provide.rzyxel.com/global/en/contact-us> for the latest information.

For Zyxel Networks offices, see <https://www.zyxel.com/index.shtml> for the latest information.

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
- <https://www.zyxel.com>

### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

#### India

- Zyxel Technology India Pvt Ltd
- <https://www.zyxel.com/in/en/>

#### Kazakhstan

- Zyxel Kazakhstan
- <https://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
- <https://www.zyxel.com/tw/zh/>

### **Thailand**

- Zyxel Thailand Co., Ltd
- <https://www.zyxel.com/th/th/>

### **Vietnam**

- Zyxel Communications Corporation-Vietnam Office
- <https://www.zyxel.com/vn/vi>

## **Europe**

### **Belarus**

- Zyxel BY
- <https://www.zyxel.by>

### **Bulgaria**

- Zyxel България
- <https://www.zyxel.com/bg/bg/>

### **Czech Republic**

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

### **Denmark**

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

### **Finland**

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

### **France**

- Zyxel France
- <https://www.zyxel.fr>

### **Germany**

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

### **Hungary**

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

### **Italy**

- Zyxel Communications Italy
- <https://www.zyxel.com/it/it/>

### **Netherlands**

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

### **Norway**

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

### **Poland**

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl/>

### **Romania**

- Zyxel Romania

- <https://www.zyxel.com/ro/ro>

### **Russia**

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

### **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

### **Spain**

- Zyxel Communications ES Ltd
- <https://www.zyxel.com/es/es/>

### **Sweden**

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

### **Switzerland**

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

### **Turkey**

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

### **UK**

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

### **Ukraine**

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

## **South America**

### **Argentina**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **Bra zil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

### **Colombia**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **Ec uador**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

### **South America**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **Middle East**

### **Isra el**

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

## **North America**

### **USA**

- Zyxel Communications, Inc. - North America Headquarters
- <https://www.zyxel.com/us/en/>

# APPENDIX D

## Legal Information

### Copyright

Copyright © 2023 by Zyxel and/or its affiliates

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 and/or its affiliates.

Published by Zyxel and/or its affiliates. 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 Zyxel Device 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

#### UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

#### FCC EMC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  - (1) This device may not cause harmful interference, and
  - (2) this device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

#### FCC Radiation Exposure Statement (for outdoor model - NWA55AXE)

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 21 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.

#### FCC Radiation Exposure Statement (for indoor model - NWA50AX/ NWA90AX)

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 21 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only.



**FCC Radiation Exposure Statement (for indoor model - NWA50AX PRO/ NWA90AX PRO)**

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only.

**BRAZIL**

The following applies if you use the product within Brazil.

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

**CANADA**

The following information applies if you use the product within Canada area.

**Innovation, Science and Economic Development Canada ICES statement**

CAN ICES-3 (B)/NMB-3(B)

**Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement (for indoor model - NWA50AX/ NWA90AX/ NWA50AX PRO/ NWA90AX PRO)**

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- For indoor use only.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the produce with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Pour une utilisation en intérieur uniquement.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz et 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

**Industry Canada radiation exposure statement (for indoor model - NWA50AX/ NWA90AX)**

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 24 cm between the radiator and your body.

**Déclaration d'exposition aux radiations: (for indoor model - NWA50AX/ NWA90AX)**

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 24 cm de distance entre la source de rayonnement et votre corps.

**Industry Canada radiation exposure statement (for indoor model - NWA50AX PRO/ NWA90AX PRO)**

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

**Déclaration d'exposition aux radiations: (for indoor model - NWA50AX PRO/ NWA90AX PRO)**

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

**Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement (for outdoor model - NWA55AXE)**

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-11AXAP22AO) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

## Antenna Information

Ant.	Port	Brand	Model Name	Antenna Type	Connector	Gain (dBi)
1	1	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	Note 1
2	2	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	

## Note 1:

Ant.	Port	Gain (dBi)			
		2.4 GHz	5 GHz Band 2	5 GHz Band 3	5 GHz Band 4
1	1	3.74	4.24	4.24	4.58
2	2	3.74	4.24	4.24	4.58

If the product with 5G wireless function operating in 5725-5850 MHz, the following attention must be paid,

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the produce with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-11AXAP22AO) a été approuvé par Innovation, Science et Développement économique Canada pour fonctionner avec le type(s) d'antenne énuméré(s) ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

## Informations antenne

Ant.	Port	Brand	Model Name	Antenna Type	Connector	Gain (dBi)
1	1	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	Note 1
2	2	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	

## Note 1:

Ant.	Port	Gain (dBi)			
		2.4 GHz	5 GHz Band 2	5 GHz Band 3	5 GHz Band 4
1	1	3.74	4.24	4.24	4.58
2	2	3.74	4.24	4.24	4.58

Lorsque la fonction sans fil 5G fonctionnant en 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

**Industry Canada radiation exposure statement (for outdoor model - NWA55AXE)**

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 24 cm between the radiator and your body.

**Déclaration d'exposition aux radiations: (for outdoor model - NWA55AXE)**

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 24 cm de distance entre la source de rayonnement et votre corps.

**EUROPEAN UNION and UNITED KINGDOM**

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

**Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK regulation**

- Compliance information for wireless products relevant to the EU, United Kingdom and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 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 the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:

**NWA50AX/NWA90AX**

- The band 2,400 MHz to 2,483.5 MHz is 98.86 mW.
- The band 5,150 MHz to 5,350 MHz is 199.07 mW.
- The band 5,470 MHz to 5,725 MHz is 979.49 mW.

**NWA50AX PRO/NWA90AX PRO**

- The band 2,400 MHz to 2,483.5 MHz is 99 mW.
- The band 5,150 MHz to 5,350 MHz is 199 mW.
- The band 5,470 MHz to 5,725 MHz is 999 mW.

**NWA55AXE**

- The band 2,400 MHz to 2,483.5 MHz is 98.86 mW.
- The band 5,150 MHz to 5,350 MHz is 198.61 mW.
- The band 5,470 MHz to 5,725 MHz is 988.55 mW.

Български (Bulgarian)	<p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>• 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 <a href="http://www.bipt.be">http://www.bipt.be</a> for more details.</li> <li>• 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 <a href="http://www.bipt.be">http://www.bipt.be</a> voor meer gegevens.</li> <li>• 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 <a href="http://www.ibpt.be">http://www.ibpt.be</a> pour de plus amples détails.</li> </ul>
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 2014/53/UE.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>• In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.</li> <li>• I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.</li> </ul>
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.

English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>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 <a href="http://www.sviluppoeconomico.gov.it/">http://www.sviluppoeconomico.gov.it/</a> for more details.</li> <li>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 <a href="http://www.sviluppoeconomico.gov.it/">http://www.sviluppoeconomico.gov.it/</a> per maggiori dettagli.</li> </ul>
Latviešu valoda (Latvian)	<p>Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p> <p><b>National Restrictions</b></p> <ul style="list-style-type: none"> <li>The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <a href="http://www.esd.lv">http://www.esd.lv</a> for more details.</li> <li>2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <a href="http://www.esd.lv">http://www.esd.lv</a>.</li> </ul>
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU 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 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

**Notes:**

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adaptor or cord is prohibited. 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 is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. 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.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

**Environment statement****ErP (Energy-related Products)**

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published

Directive 2009/125/EC and UK regulation 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 < 8W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

For wireless setting, please refer to the chapter about wireless settings for more detail.

### Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



### 以下訊息僅適用於產品銷售至台灣地區

取得審驗證明之低功率射頻器材，非經核准，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。低功率射頻器材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。前述合法通信，指依電信管理法規規定作業之無線電通信。低功率射頻器材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。應避免影響附近雷達系統之操作。

### 以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

### 安全警告 - 為了您的安全，請先閱讀以下警告及指示：





- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝、使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。

- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

## 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](http://www.zyxel.com/web/support/warranty_info.php).

## Registration

Register your product online at [www.zyxel.com](http://www.zyxel.com) to receive email notices of firmware upgrades and related information.

## Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: [http://www.zyxel.com/form/gpl\\_license\\_software\\_notice.shtml](http://www.zyxel.com/form/gpl_license_software_notice.shtml).

# Index

## Numbers

802.11k [13, 14](#)

802.11r [13, 14](#)

802.11v [13, 14](#)

## A

access [33](#)

access privileges [19](#)

access users [91](#)

    see also users [91](#)

admin users [91](#)

    multiple logins [96](#)

    see also users [91](#)

alerts [169, 170, 171](#)

AP Controller [13, 14](#)

applications

    MBSSID [19](#)

    Repeater [17](#)

Assisted Roaming, see 802.11k/v

## B

backing up configuration files [174](#)

Basic Service Set

    see BSS

BSS [19](#)

## C

CA

    and certificates [132](#)

CA (Certificate Authority), see certificates

CEF (Common Event Format) [167, 168](#)

Certificate Authority (CA)

    see certificates

Certificate Revocation List (CRL) [132](#)

    vs OCSP [146](#)

certificates [131](#)

    advantages of [132](#)

    and CA [132](#)

    and FTP [164](#)

    and HTTPS [153](#)

    and SSH [162](#)

    and WWW [154](#)

    certification path [132, 139, 144](#)

    expired [132](#)

    factory-default [132](#)

    file formats [132](#)

    fingerprints [140, 145](#)

    importing [135](#)

    not used for encryption [132](#)

    revoked [132](#)

    self-signed [132, 136](#)

    serial number [139, 144](#)

    storage space [134, 142](#)

    thumbprint algorithms [133](#)

    thumbprints [133](#)

    used for authentication [132](#)

    verifying fingerprints [133](#)

certification requests [136](#)

certifications

    viewing [255](#)

channel [20](#)

CLI [29, 38](#)

    button [38](#)

    messages [38](#)

    popup window [38](#)

    Reference Guide [2](#)

cold start [45](#)

commands [29](#)

    sent by Web Configurator [38](#)

Common Event Format (CEF) [167, 168](#)

configuration

    information [183, 198](#)

configuration files [172](#)

    at restart [174](#)



- backing up [174](#)
- downloading [175](#)
- downloading with FTP [164](#)
- editing [172](#)
- how applied [173](#)
- lastgood.conf [174](#), [176](#)
- managing [173](#)
- startup-config.conf [176](#)
- startup-config-bad.conf [174](#)
- syntax [172](#)
- system-default.conf [176](#)
- uploading [177](#)
- uploading with FTP [164](#)
- use without restart [172](#)
- contact information [243](#)
- cookies [33](#)
- copyright [248](#)
- CPU usage [48](#), [50](#)
- current date/time [48](#), [148](#)
  - daylight savings [150](#)
  - setting manually [151](#)
  - time server [151](#)
- customer support [243](#)

## D

- date [148](#)
- daylight savings [150](#)
- DCS [79](#)
- DHCP [148](#)
  - and domain name [148](#)
- diagnostics [183](#), [198](#)
- disclaimer [248](#)
- domain name [148](#)
- dual radios [20](#)
- dual-radio application [20](#)
- dynamic channel selection [79](#)

## E

- encryption [17](#)
- ESSID [208](#)
- Extended Service Set IDentification [98](#)

## F

- Fast Roaming, see 802.11r
- FCC interference statement [248](#)
- file extensions
  - configuration files [172](#)
  - shell scripts [172](#)
- file manager [172](#)
- Firefox [33](#)
- firmware
  - and restart [178](#)
  - current version [48](#), [179](#)
  - getting updated [178](#)
  - uploading [178](#), [179](#)
  - uploading with FTP [164](#)
- flash usage [48](#)
- FTP [29](#), [164](#)
  - and certificates [164](#)
  - with Transport Layer Security (TLS) [164](#)

## G

- Guide
  - CLI Reference [2](#)

## H

- HTTP
  - over SSL, see HTTPS
  - redirect to HTTPS [154](#)
  - vs HTTPS [153](#)
- HTTPS [152](#)
  - and certificates [153](#)
  - authenticating clients [153](#)
  - avoiding warning messages [156](#)
  - example [155](#)
  - vs HTTP [153](#)
  - with Internet Explorer [155](#)
  - with Netscape Navigator [155](#)
- HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

**I**

- interface
  - status [49](#)
- interfaces
  - as DHCP servers [148](#)
- interference [20](#)
- Internet Explorer [33](#)
- Internet Protocol version 6, see IPv6
- IP Address [71](#), [194](#)
  - gateway IP address [71](#)
- IP subnet [71](#)
- IPv6 [235](#)
  - addressing [235](#)
  - EUI-64 [237](#)
  - global address [235](#)
  - interface ID [237](#)
  - link-local address [235](#)
  - Neighbor Discovery Protocol [235](#)
  - ping [235](#)
  - prefix [235](#)
  - prefix length [235](#)
  - stateless autoconfiguration [237](#)
  - unspecified address [236](#)

**J**

- Java
  - permissions [33](#)
- JavaScripts [33](#)

**K**

- key pairs [131](#)

**L**

- lastgood.conf [174](#), [176](#)
- layer-2 isolation [126](#)
  - example [126](#)
  - MAC [127](#)
- LED suppression [185](#)

- Locator LED [186](#)
- log messages
  - categories [169](#), [170](#), [171](#)
  - debugging [69](#)
  - regular [69](#)
  - types of [69](#)
- logout
  - Web Configurator [37](#)
- logs
  - formats [167](#)
  - settings [166](#)

**M**

- MAC address
  - range [48](#)
- management mode [22](#)
- Management, NCC [22](#)
- Management, Standalone [22](#)
- managing the device
  - good habits [29](#)
  - using FTP, see FTP
- MBSSID [19](#)
- memory usage [48](#), [51](#)
- messages
  - CLI [38](#)
- mode, default [22](#)
- model name [47](#)
- My Certificates, see also certificates [134](#)

**N**

- NCC, see Nebula Control Center
- Nebula Control Center [22](#)
- Netscape Navigator [33](#)
- Network Time Protocol (NTP) [150](#)

**O**

- objects
  - certificates [131](#)
  - users, account

- user [91](#)
- Online Certificate Status Protocol (OCSP) [146](#)
  - vs CRL [146](#)
- overview [45](#), [191](#)

## P

- pop-up windows [33](#)
- power off [46](#)
- power on [45](#)
- product registration [255](#)
- Public-Key Infrastructure (PKI) [132](#)
- public-private key pairs [131](#)

## R

- radio [20](#)
- reboot [45](#), [188](#)
  - vs reset [188](#)
- Reference Guide, CLI [2](#)
- registration
  - product [255](#)
- remote management
  - FTP, see FTP
  - WWW, see WWW
- reset [210](#)
  - vs reboot [188](#)
  - vs shutdown [189](#)
- RESET button [46](#), [210](#)
- restart [188](#)
- RF interference [20](#)
- Rivest, Shamir and Adleman public-key algorithm (RSA) [136](#)
- RSA [136](#), [145](#)
- RSSI threshold [105](#)

## S

- screen resolution [33](#)
- Secure Socket Layer, see SSL
- serial number [47](#)

- service control
  - and users [152](#)
  - limitations [152](#)
  - timeouts [152](#)
- Service Set [98](#)
- Service Set Identifier
  - see SSID
- shell scripts [172](#)
  - downloading [181](#), [198](#)
  - editing [180](#), [197](#)
  - how applied [173](#)
  - managing [180](#), [197](#)
  - syntax [172](#)
  - uploading [182](#), [198](#)
- shutdown [46](#), [189](#)
  - vs reset [189](#)
- SSH [160](#)
  - and certificates [162](#)
  - client requirements [162](#)
  - encryption methods [162](#)
  - for secure Telnet [163](#)
  - how connection is established [161](#)
  - versions [162](#)
  - with Linux [163](#)
  - with Microsoft Windows [163](#)
- SSID [19](#)
- SSID profile
  - pre-configured [19](#)
- SSID profiles [19](#)
- SSL [152](#)
- starting the device [45](#)
- startup-config.conf [176](#)
  - if errors [174](#)
  - missing at restart [174](#)
  - present at restart [174](#)
- startup-config-bad.conf [174](#)
- station [79](#)
- status [192](#)
- stopping the device [45](#)
- supported browsers [33](#)
- syslog [167](#), [168](#)
- system name [47](#), [148](#)
- system uptime [48](#)
- system-default.conf [176](#)

## T

- Telnet
  - with SSH [163](#)
- time [148](#)
- time servers (default) [151](#)
- trademarks [248](#)
- Transport Layer Security (TLS) [164](#)
- troubleshooting [183](#), [198](#)
- Trusted Certificates, see also certificates [141](#)

## U

- upgrading
  - firmware [178](#)
- uploading
  - configuration files [177](#)
  - firmware [178](#)
  - shell scripts [180](#), [197](#)
- usage
  - CPU [48](#), [50](#)
  - flash [48](#)
  - memory [48](#), [51](#)
  - onboard flash [48](#)
- user authentication [91](#)
- user name
  - rules [92](#)
- user objects [91](#)
- users [91](#)
  - access, see also access users
  - admin (type) [91](#)
  - admin, see also admin users
  - and service control [152](#)
  - currently logged in [48](#)
  - default lease time [95](#), [97](#)
  - default reauthentication time [95](#), [97](#)
  - lease time [94](#)
  - limited-admin (type) [91](#)
  - lockout [96](#)
  - reauthentication time [94](#)
  - types of [91](#)
  - user (type) [91](#)
  - user names [92](#)

## V

- Vantage Report (VRPT) [167](#), [168](#)
- Virtual Local Area Network [74](#)
- VLAN [74](#)
  - introduction [74](#)
- VRPT (Vantage Report) [167](#), [168](#)

## W

- warm start [45](#)
- warranty [255](#)
  - note [255](#)
- WDS [17](#)
- Web Configurator [29](#), [33](#)
  - access [33](#)
  - requirements [33](#)
  - supported browsers [33](#)
- WEP (Wired Equivalent Privacy) [99](#)
- wireless channel [208](#)
- wireless client [79](#)
- Wireless Distribution System (WDS) [17](#)
- wireless LAN [208](#)
- wireless network
  - example [78](#)
  - overview [78](#)
- wireless profile [98](#)
  - layer-2 isolation [98](#)
  - MAC filtering [98](#)
  - radio [98](#)
  - security [98](#)
  - SSID [98](#)
- wireless security [19](#), [208](#)
- wireless station [79](#)
- Wizard Setup [53](#)
- WLAN interface [20](#)
- WPA2 [99](#)
- WWW [153](#)
  - and certificates [154](#)
  - see also HTTP, HTTPS [153](#)

## Z

ZDP [24](#)

ZON Utility [24](#)