ZYXEL
Your Networking Ally

DRAFT

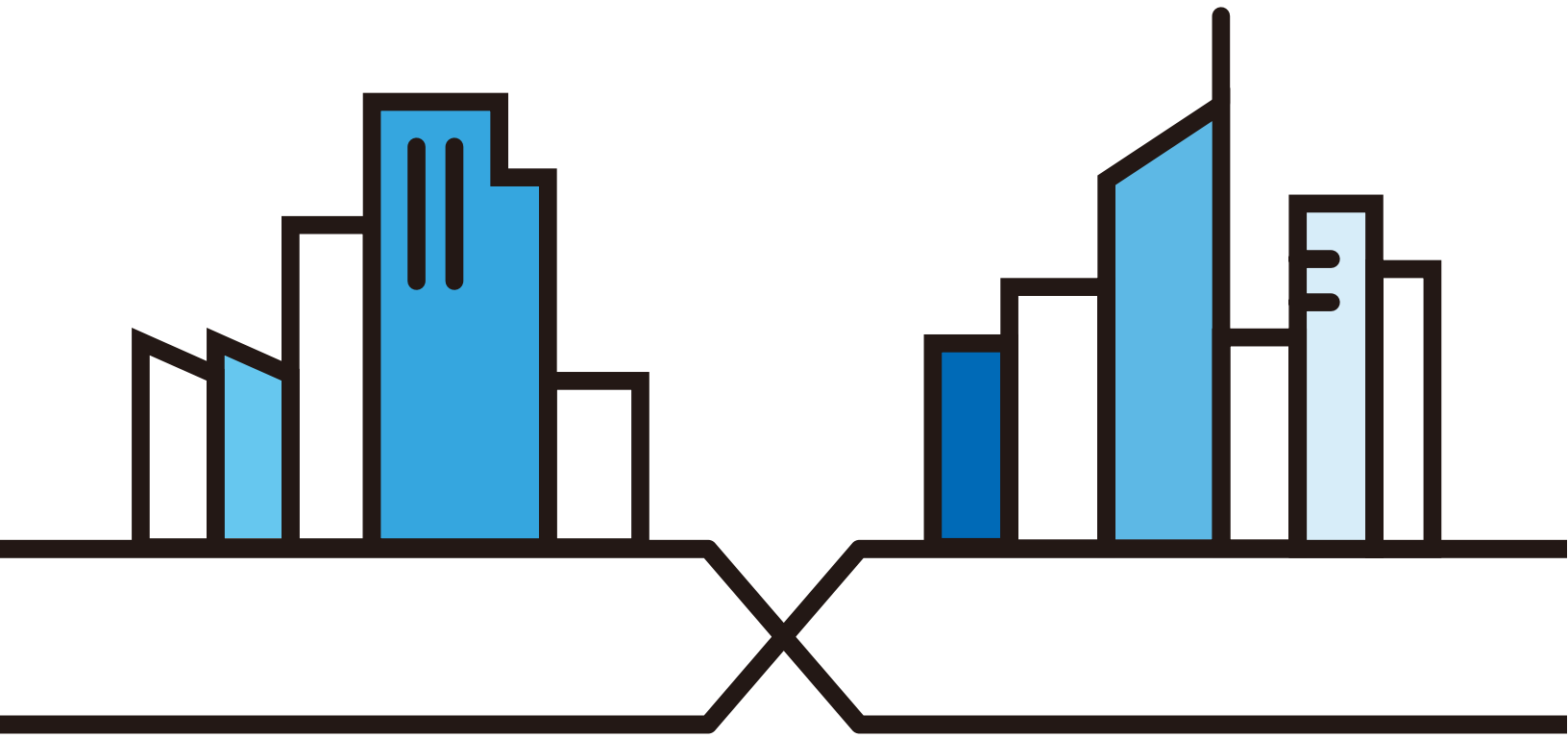
User's Guide

NWA50AX

802.11ax (WiFi6) Dual-Radio 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 6.20 Edition 1, 4/2021



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 1.4 on page 18).

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 20).

- NXC Series User's Guide

  See this User's Guide for instructions on using the NXC as an AP Controller (AC) for the Zyxel Device. This is used when the Zyxel Device is set to be managed by a Zyxel AC.

- More Information

  Go to **support.zyxel.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.

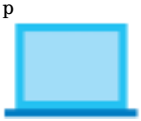
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

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 	AP Controller 
Printer 	Nebula Switch 	Nebula Gateway 	Smart T.V. 
IP Phone 			

Contents Overview

Table of Contents

CHAPTER 1
Introduction

1.1 Overview

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 20.

Use the Zyxel Device to set up a wireless 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 1.2.2 on page 13 for more information on root and repeater APs and how to set them up.

1.2 Zyxel Device Roles

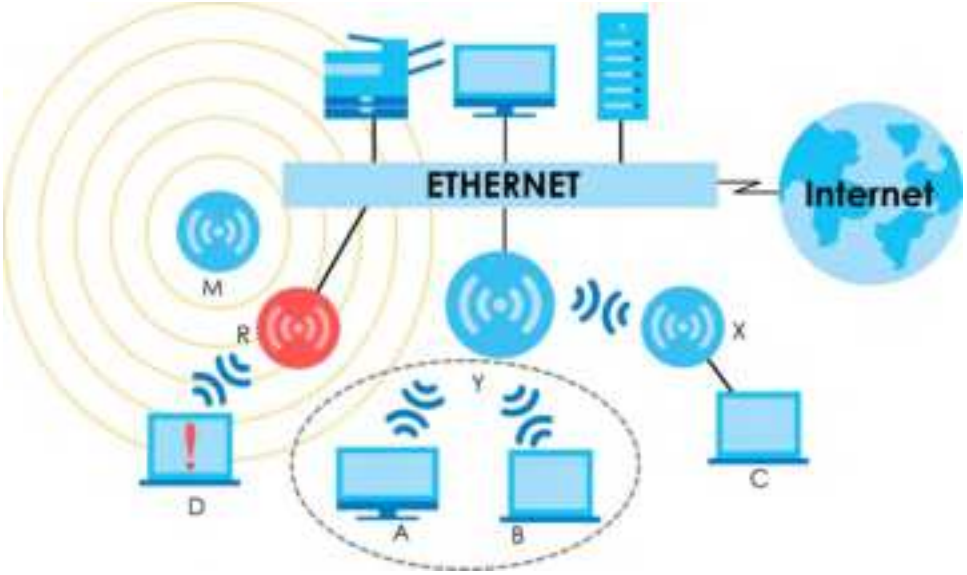
This section describes some of the different roles that your Zyxel Device can take up within a network. Not all roles are supported by all models (see Section 1.4 on page 18). The Zyxel Device can serve as a:

- Access Point (AP) - This is used to allow wireless clients to connect to the Internet.
- Radio Frequency (RF) monitor - An RF monitor searches for rogue APs to help eliminate network threats if it supports monitor mode and rogue APs detection/containment. An RF monitor cannot 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.

The following figure shows a network setup that uses these different roles to create a secure Wireless Distribution System (WDS). The root AP (**Y**) is connected to a network with Internet access and has a wireless repeater (**X**) connected to it to expand the wireless network's range. Clients (**A**, **B**, and **C**) can access the wired network through the wireless repeater and/or root AP.

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 and remove them or use the NXC to quarantine them.

Figure 1 Sample Network Setup



1.2.1 Root AP

In Root AP mode, you can have multiple SSIDs active for regular wireless connections and one SSID for the connection with a repeater (repeater SSID). Wireless 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.

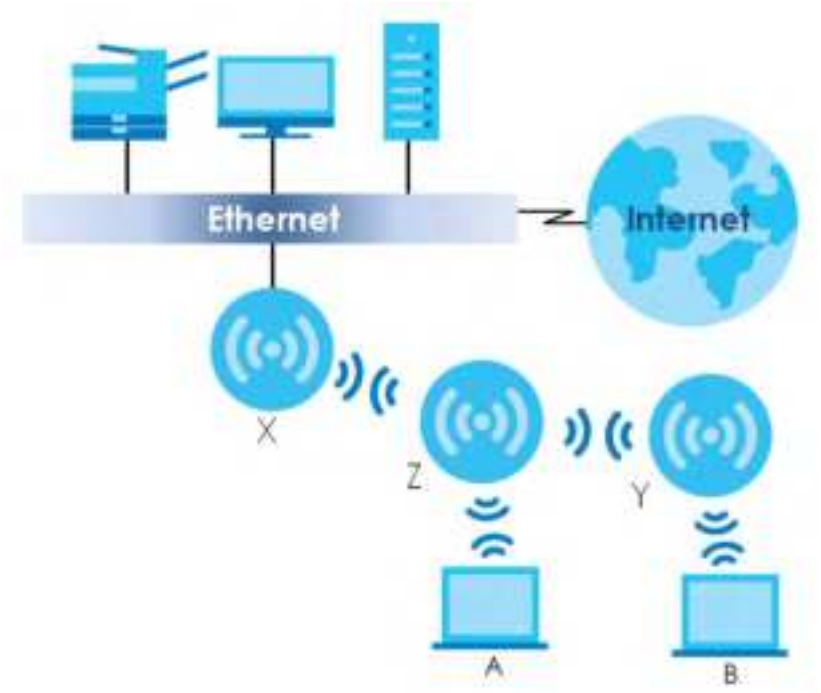
When the Zyxel Device is in Root AP mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the wireless clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 10.2 on page 76 and Section 14.2 on page 120 for more details.

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

1.2.2 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** and **Y** act as repeaters that forward traffic between associated wireless 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 2 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 wireless 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 76 and Section 14.2 on page 120 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, an SSID for the WDS, and a pre-shared key.
3. Do steps 1 and 2 for the wireless repeater using the same SSID and pre-shared key.
4. Once the security settings of peer sides match one another, the connection between the root and repeater Zyxel Devices is made.

To set up a WDS in NXC managed Zyxel Devices, see the NXC User's Guide.

1.2.3 Radio Frequency (RF) Monitor

The Zyxel Device can 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 quarantine them if the Zyxel Device is managed by the NXC (see Section 2.2 on page 22). If the Zyxel Device's radio setting is set to **MON Mode** (RF Monitor mode), it will serve as a dedicated RF monitor and its AP clients are disconnected.

The models that do not support **MON Mode** support **Rogue AP Detection** (see Section 10.3 on page 79). **Rogue AP Detection** allows the AP to scan all channels similar to **MON Mode** except that the Zyxel Device still works as an AP while it scans the environment for wireless signals. To see which Zyxel Devices support the RF Monitor feature, see Section 1.4 on page 18.

The Zyxel Device in **MON Mode** scans a range of WiFi channels that you specify in a **MON Profile**, either in the 2.4 GHz or 5 GHz band. To scan both bands, you need to set both radio 1 and radio 2 in **MON Mode**. Once a rogue AP is detected, the network administrator can manually change the network settings to limit its access to the network using its MAC address or have the device physically removed. If the Zyxel Device is managed by an NXC, the network administrator can also use **Rogue AP Containment** through the NXC.

MON Mode in Standalone Mode

To use an RF monitor in standalone mode, do the following steps:

1. Create a **MON Profile** in **Configuration > Object > MON Profile > Add**. Specify a **Channel dwell time** to determine how long the RF monitor scans a specific channel before moving to the next one.
2. To scan all 2.4 GHz and 5 GHz channels, select **auto** in **Scan Channel Mode**. Make sure that the **Activate** check box is selected and click **OK**.
3. Go to the **Configuration > Wireless > AP Management** screen and set **Radio 1 OP Mode** (2.4 GHz) and/or **Radio 2 OP Mode** (5 GHz) to **MON Mode**.
4. Select the **Radio 1(2) Profile** that you created in the previous step. Make sure that the **Radio 1(2) Activate** check box is selected and click **Apply**.
5. Go to **Monitor > Wireless > Detected Device** to see a list of APs scanned by the RF monitor.
6. Select an AP or APs in the list and click **Mark as Rogue AP** or **Mark as Friendly AP**.

MON Mode in NXC-Managed Zyxel Devices

For NXC-managed Zyxel Devices, do the following steps in the NXC Web Configurator.

1. Create a **MON Profile** in **CONFIGURATION > Object > MON Profile > Add**. Specify a **Channel dwell time** to determine how long the RF monitor scans a specific channel before moving to the next one.
2. To scan all 2.4 GHz and 5 GHz channels, select **auto** in **Scan Channel Mode**. Make sure that the **Activate** check box is selected and click **OK**.
3. Go to the **CONFIGURATION > Wireless > AP Management > Mgmt. AP List > Edit** screen and/or set **Radio 1 OP Mode** (2.4 GHz) and **Radio 2 OP Mode** (5 GHz) to **MON Mode**.
4. Select the **Radio 1(2) Profile** that you created in the previous step. Select **Override Group Radio Setting** and click **OK**.
5. Go to **MONITOR > Wireless > Detected Device** to see a list of APs scanned by the RF monitor.
6. Select an AP or APs in the list and click **Mark as Rogue AP** or **Mark as Friendly AP**.

7 To quarantine a rogue AP, go to **CONFIGURATION > Wireless > Rogue AP**, select the APs you want to quarantine, and click **Containment**. Make sure the **Enable Rogue AP Containment** check box is selected, and click **Apply**.

1.3 Sample Feature Applications

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

1.3.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless 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.

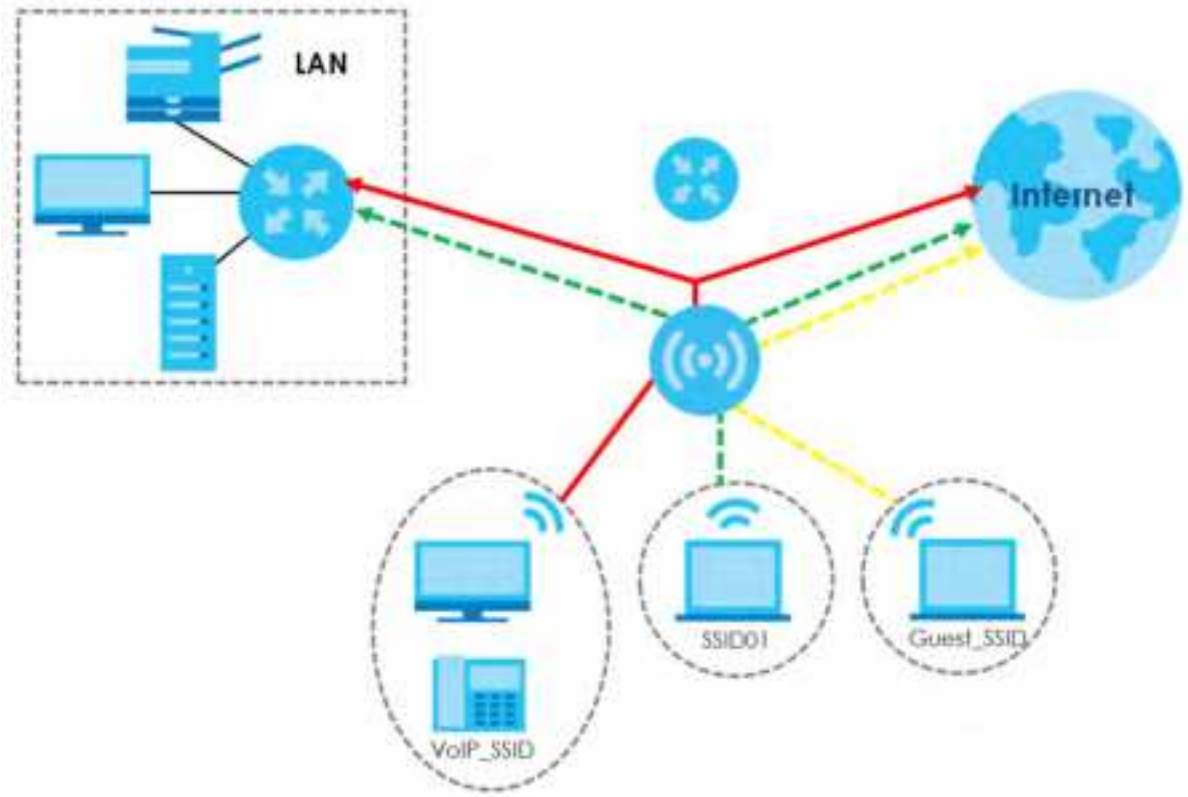
You can configure multiple SSID profiles, and have all of them active at any one time.

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 wireless clients in the network, each SSID appears to be a different access point. As in any wireless 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 wireless network in your office where Internet telephony (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **SSID01** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired Land Area Network (LAN) behind the AP and can access only the Internet.

Figure 3 Multiple BSSs



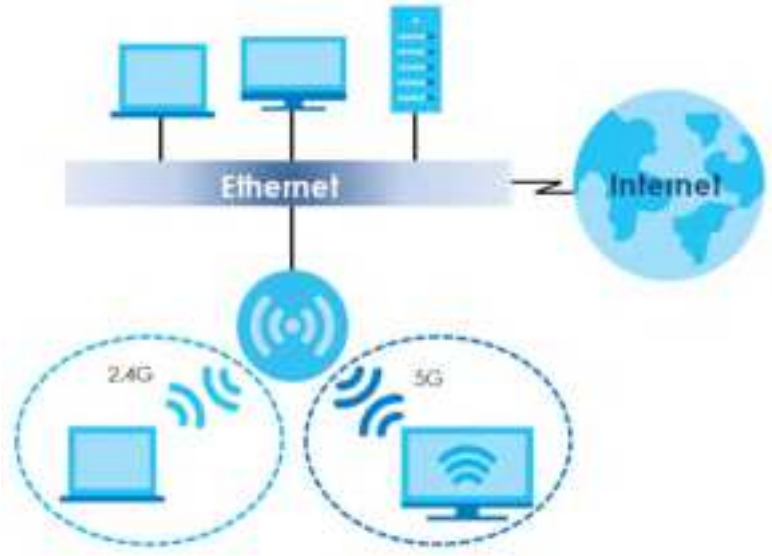
1.3.2 Dual-Radio

Some of the Zyxel Device models are equipped with dual wireless radios. This means you can configure two different wireless 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 4 Dual-Radio Application



1.4 Zyxel Device Product Feature

The following table lists the features of the Zyxel Device..

Table 1 Zyxel Device Product Feature Table

FEATURES	NWA50AX
Supported Wireless Standards	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA2-MIX WPA2-PSK WPA2-PSK-MIX Enhanced-open WPA3-personal
Number of SSID Profiles	64
Number of Wireless Radios	2
Monitor Mode & Rogue APs Containment[A]	No
Rogue AP Detection	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes
Tunnel Forwarding Mode	No
Layer-2 Isolation	No
Supported PoE Standards	IEEE 802.3at
Power Detection	Yes
External Antennas	No
Internal Antennas	Yes

Table 1 Zyxel Device Product Feature Table (continued)

FEATURES	NWA50AX
Antenna Switch	No
Console Port	4-Pin Serial
LED Locator	Yes
LED Suppression	Yes
AC (AP Controller) Discovery	No
Nebula Flex PRO	No
NCC Discovery	Yes
802.11r Fast Roaming Support	Yes
802.11k/v Assisted Roaming	Yes
Bluetooth Low Energy (BLE)	No
USB Port for BLE	No
Ethernet Storm Control	No
Grounding	No
Power Jack	Yes
Maximum number of log messages	512 event logs

A. For NXC managed devices only. See the NXC User's Guide for details.

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 1.4 on page 18 to check whether your product supports these.

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

Table 2 Zyxel Device Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP 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 42 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 23.1 on page 186 for an example NCC managed network topology.

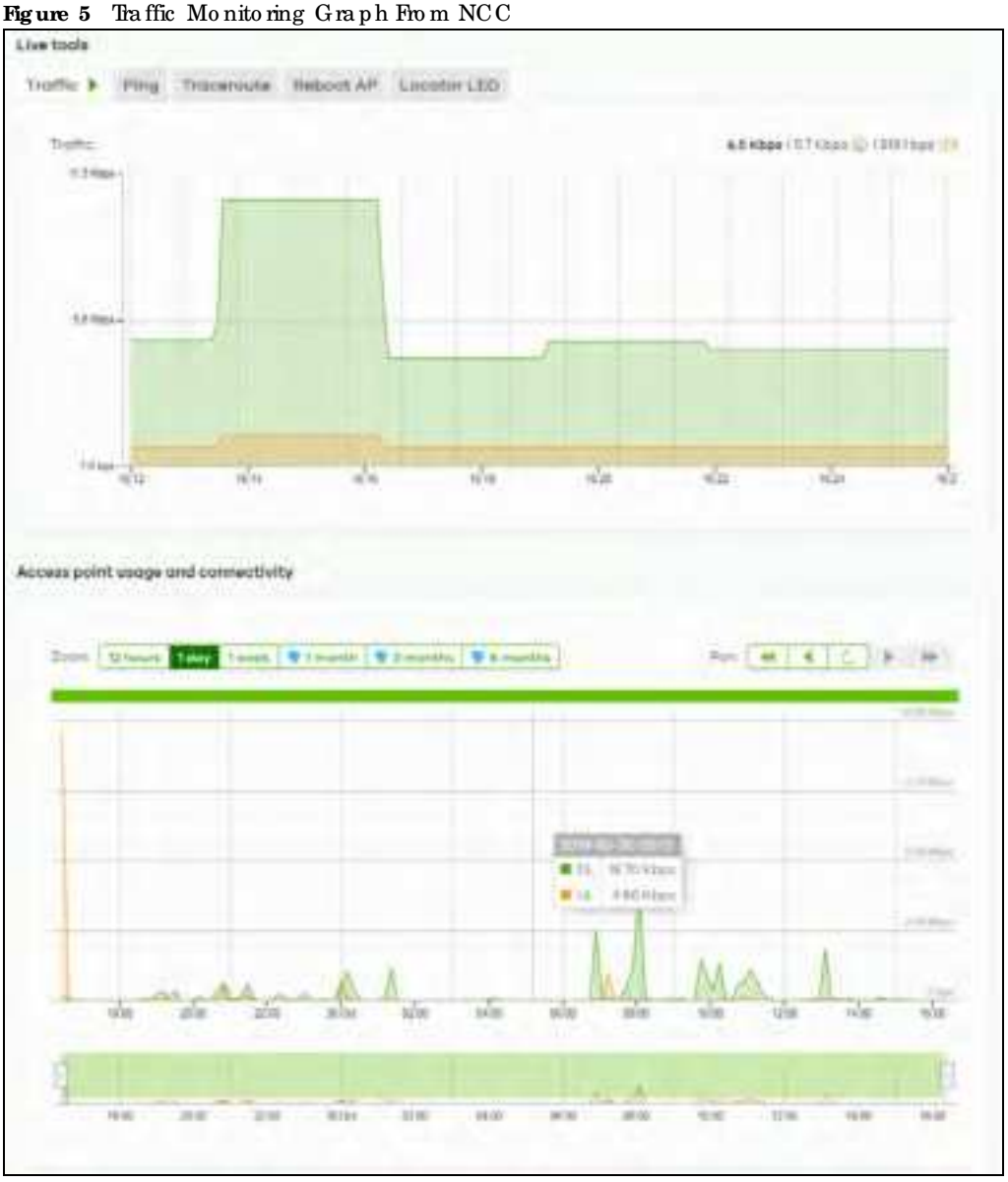
NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 3 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 5 Traffic Monitoring Graph From NCC



See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See Chapter 24 on page 189 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 and/or AC 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 73). The NCC manages the Zyxel Device automatically when it is discovered.

NCC-to-Standalone

Unregister the Zyxel Device from the NCC organization/site. Reset the Zyxel Device to factory defaults (see Section 26.6 on page 205).

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 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**. 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.

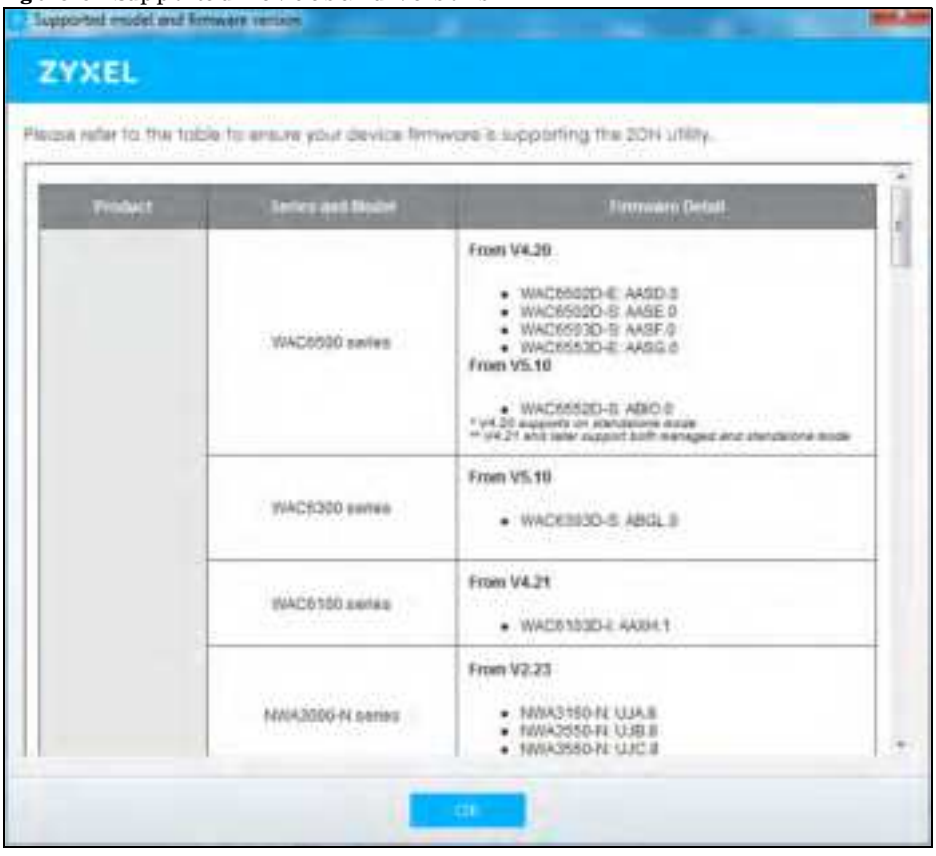
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

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 6 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 7 ZON Utility Screen

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

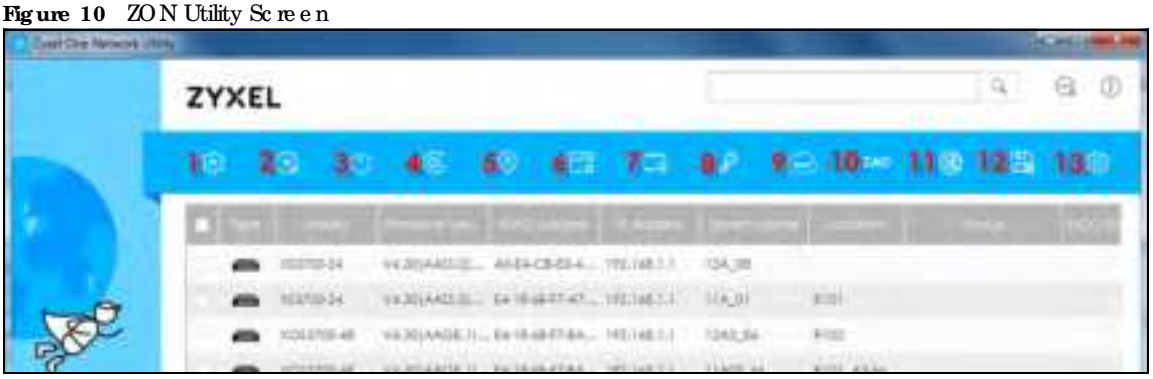
Figure 8 Network Adapter

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

Figure 9 Discovery

5 The ZON Utility screen shows the devices discovered.

Figure 10 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 11 Password Prompt

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

Table 4 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 **Locator** 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 4 ZON Utility Icons (continued)

ICON	DESCRIPTION
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management 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 5 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 **IP Configuration**, **Renew IP address** and **Flash Locator LED**, 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 it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the Nebula cloud management 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.

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 and install it on your computer (Windows operating system). For more information on ZON Utility see Section 2.3 on page 22.

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 (for example, SSH or Telnet) 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 20 on page 180 for the LED **Suppression** and **Locator** menus in standalone mode.

3.1.1 Zyxel Device LED

Figure 12 NWA50AX LED

The following are the LED descriptions for your Zyxel Device.

Table 6 Zyxel Device LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up or is connecting with NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC or an AC.
	Amber Green	Blinks amber and green alternatively 2 times and then turns solid green for 3 seconds.	The Zyxel Device is managed by an AC but the uplink is disconnected.
	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 wireless 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 wireless clients are connected to the Zyxel Device.
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless 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.

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 Internet Explorer 11, Mozilla Firefox, or Google Chrome. 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. 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 NCC mode, check the NCC's **AP> Monitor> Access Point** screen for the Zyxel Device's LAN IP address.

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

Click **Nebula Mode** to show the following screen. 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 20).

If you want to return to the login page, click **Standalone Mode** and follow the next steps.

4 Enter the username (default: "admin") and password (default: "1234"). If the Zyxel Device is being managed or has been managed by the NCC, check the NCC's **Site-Wide > Configure > General setting** 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 username and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.

The **Update Admin Info** screen appears every time you log in using the default username 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 13 The Web Configurator's Main Screen for Standalone Mode

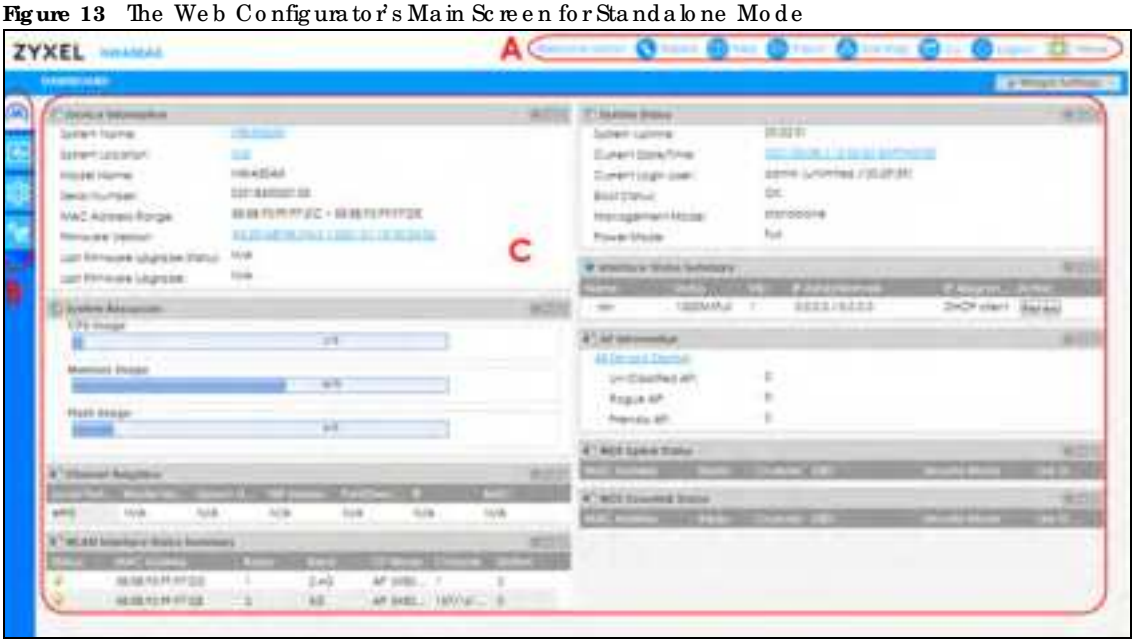


Figure 14 The Web Configurator's Main Screen for Cloud Mode

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 15 Title Bar

The icons provide the following functions.

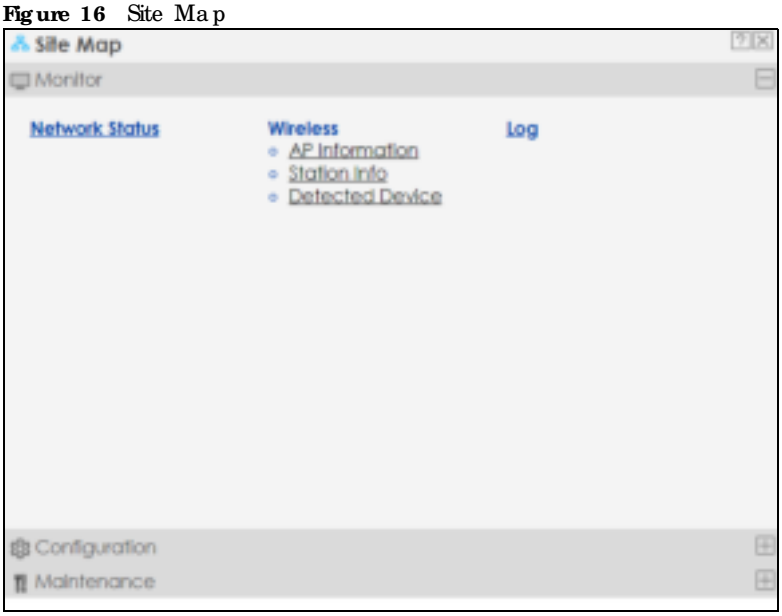
Table 7 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See Chapter 7 on page 49 for more information.
Help	Click this to open the help page for the current screen.
Forum	Click this to go to Zyxel Biz User Forum, where you can get the latest Zyxel Device information and have conversations with other people by posting your messages.
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.

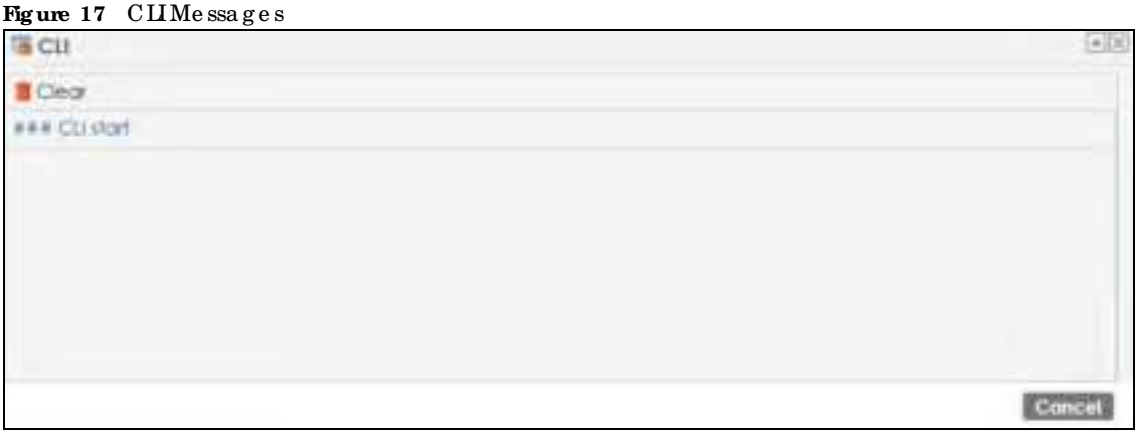
Figure 16 Site Map



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 17 CLI Messages



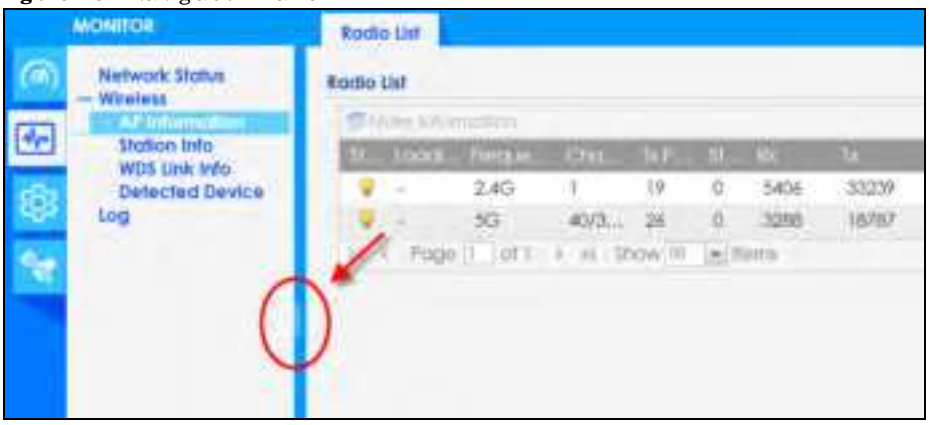
Click **Clear** to remove the currently displayed information.

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 18 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 1.4 on page 18 to see which features your Zyxel Device model supports.

Dashboard

The dashboard displays 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 44.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 8 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
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 9 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.
	NCC Discovery	Configure proxy server settings to access the NCC.
Wireless		
AP Management	WLAN Setting	Manage the Zyxel Device's general wireless settings.
Rogue AP	Rogue/Friendly AP List	Configure how the Zyxel Device monitors for rogue APs.
DCS	DCS	Configure dynamic wireless 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 wireless radio settings files that can be associated with different APs.
	SSID	Create and manage wireless SSID, security, MAC filtering, and layer-2 isolation files that can be associated with different APs.
MON Profile	MON Profile	Create and manage rogue AP monitoring files that can be associated with different APs.

Table 9 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
WDS Profile	WDS	Create and manage WDS profiles that can be used to connect to different APs in WDS.
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.
Power Mode	Power Mode	Configure the Zyxel Device's power settings.
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, e-mail logs, 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 10 Maintenance Menu Screens Summary

FOLDER 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.
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.
Antenna	Antenna Switch	Change antenna orientation for the radios.
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 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 23 on page 187.

Configuration Menu

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

Table 11 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.

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.

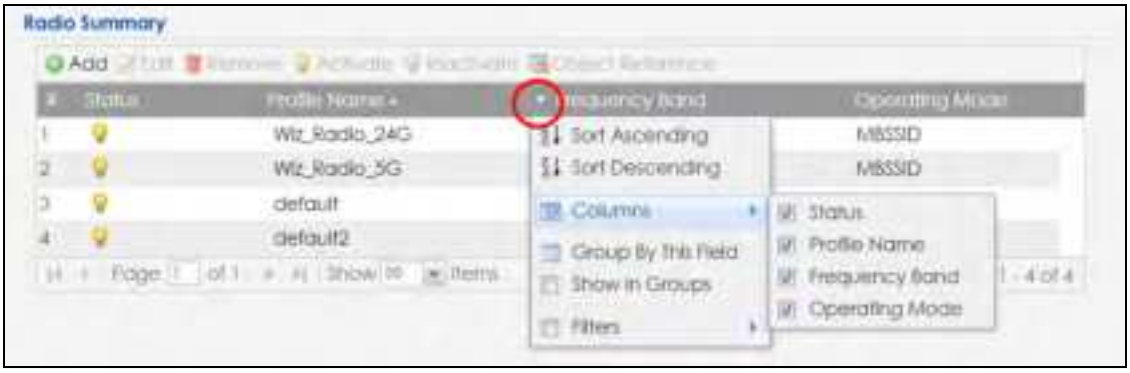
4.3.5.1 Manipulating Table Display

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

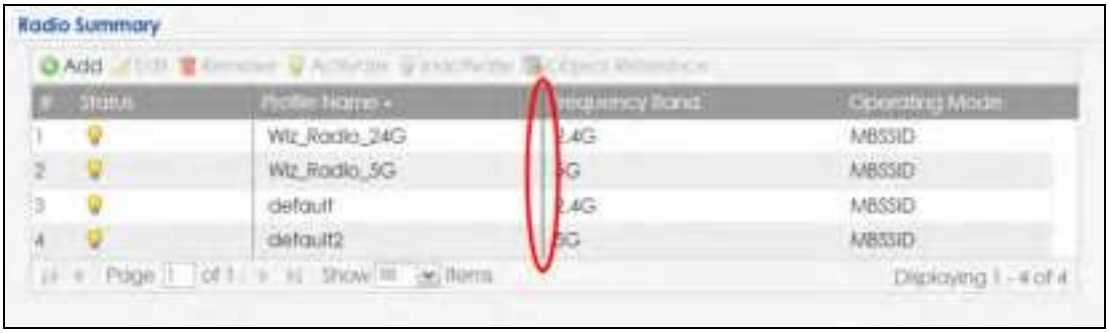
1 Click a column heading to sort the table's entries according to that column's criteria.

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.



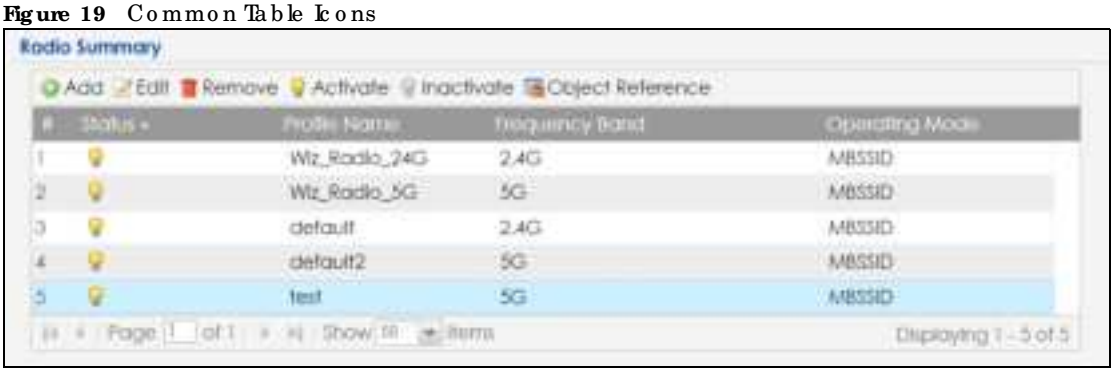
4 Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

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 19 Common Table Icons



Here are descriptions for the most common table icons.

Table 12 Common Table Icons

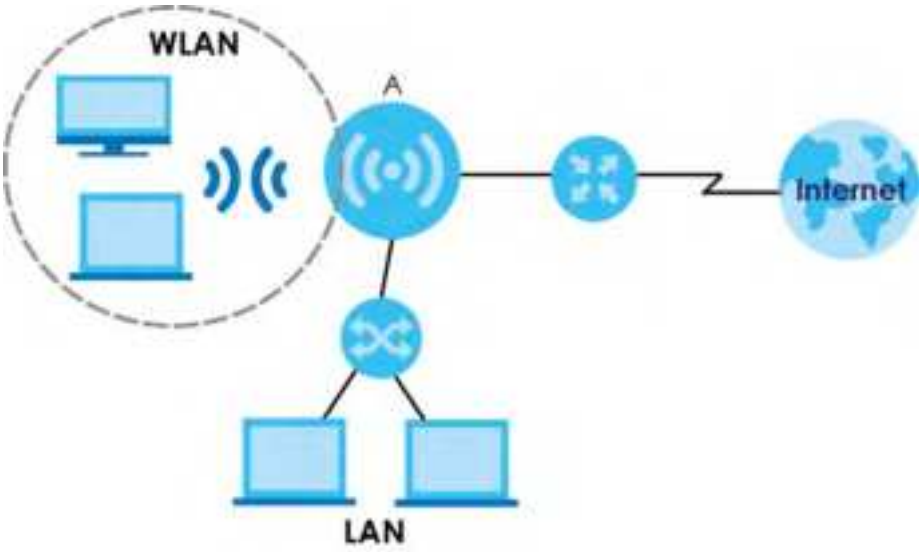
LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** 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 **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Select an entry and click **Object Reference** 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, wireless 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 13 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 **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The Zyxel Device writes all cached data to the local storage, stops the system processes, and then does a warm start.

Table 13 Starting and Stopping the Zyxel Device

METHOD	DESCRIPTION
Using the RESET button	If you press the **RESET** button on the back of the Zyxel Device, the Zyxel Device sets the configuration to its default values and then reboots. See Section 26.6 on page 205 for more information.
Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command	Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` 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.

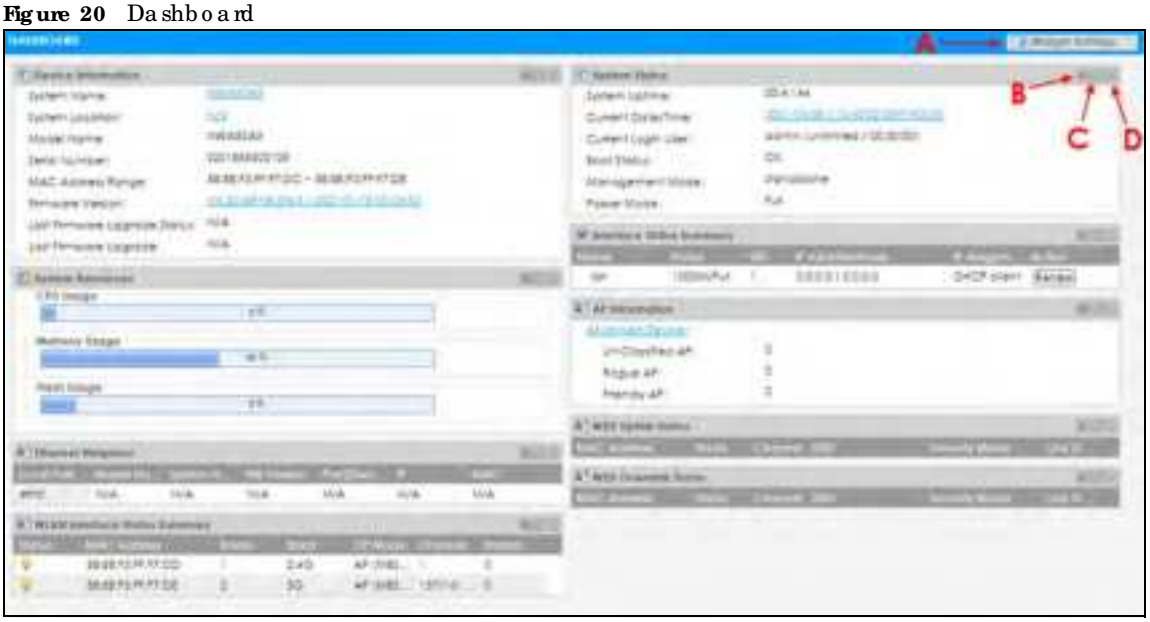
The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

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.

Figure 20 Dashboard



The following table describes the labels in this screen.

Table 14 Dashboard

LABEL	DESCRIPTION
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 **Widget Settings** 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 14 Dashboard (continued)

LABEL	DESCRIPTION
MAC Address Range	This field displays the MAC addresses used by the Zyxel Device. Each physical port or wireless 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 **Show CPU Usage** 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 **Show Memory Usage** 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 wireless 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 username used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Boot Status	This field displays details about the Zyxel Device's startup state. **OK** - The Zyxel Device started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - 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. **Fallback to lastgood configuration** - The Zyxel Device was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The Zyxel Device is still applying the system configuration.
Management Mode	This shows whether the Zyxel Device is set to work as a stand alone AP.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).
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	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Action	If the interface has a static IP address, this shows **n/a**. If the interface has a dynamic IP address, use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server.
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 wireless frequency band currently being used by the radio. This shows **-** when the radio is in monitor mode.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **MON** (monitor), **Root AP** or **Repeater**.

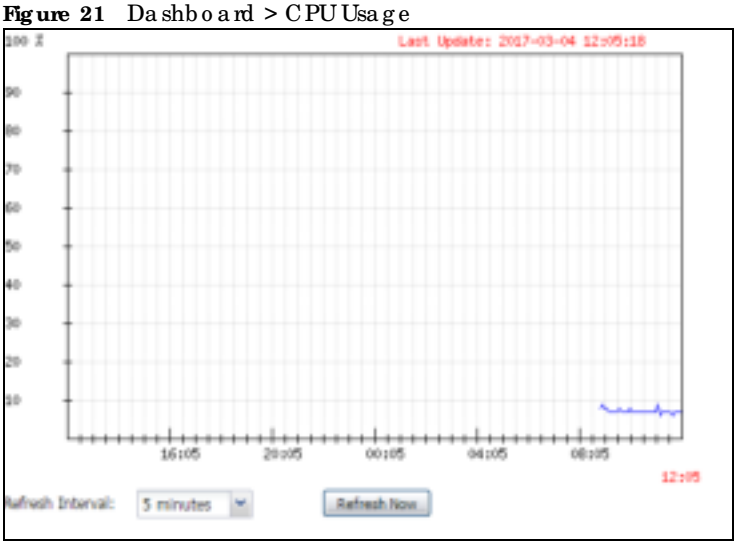
Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Channel	This indicates the channel number the radio is using.
Antenna	This indicates the antenna orientation for the radio (**Wall** or **Ceiling**). This field is not available if the Zyxel Device does not allow you to adjust antenna orientation for the Zyxel Device's radio(s) using the web configurator or a physical switch. Refer to Section 1.4 on page 18 to see if your Zyxel Device has an antenna switch.
Station	This displays the number of wireless 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 **Monitor > Wireless > Detected Device** 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 21 Dashboard > CPU Usage



The following table describes the labels in this screen.

Table 15 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 22 Dashboard > Memory Usage

The following table describes the labels in this screen.

Table 16 Dashboard > Memory Usage

LABEL	DESCRIPTION
%	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 ZyxelDevice 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 ZyxelDevice IP address, change time zone, daylight saving and radio settings, and edit an SSID profile to change general wireless and wireless security settings.

7.2.1 Step 1 Time Settings

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

- **Country Code**: Select the country where the ZyxelDevice is located.

Note: The country code field is not available and you cannot change the country code if the ZyxelDevice 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 23 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.

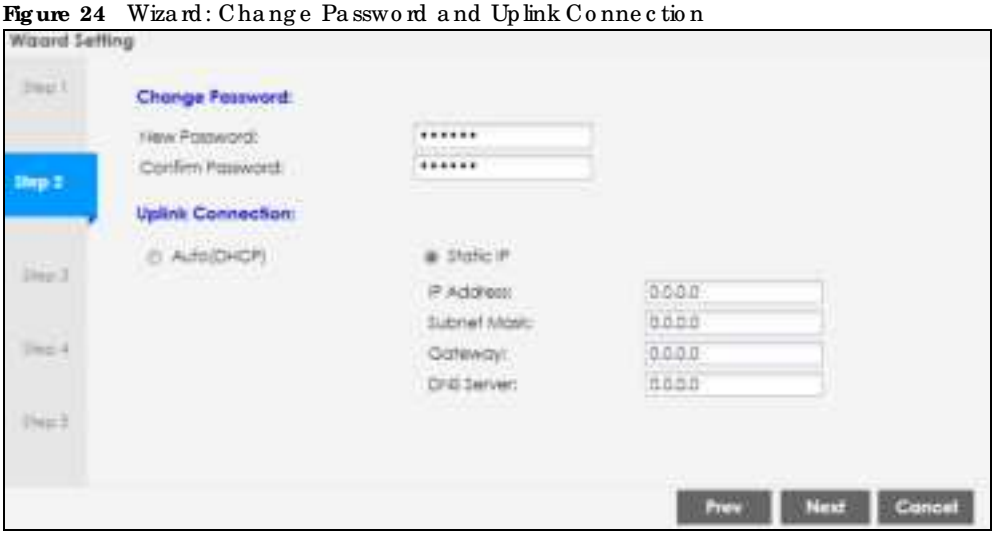
Uplink Connection: Select **Auto (DHCP)** if the Zyxel Device is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Zyxel Device in order to access the Zyxel Device's Web Configurator again.

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.

Figure 24 Wizard: Change Password and Uplink Connection



7.2.3 Step 3 Radio

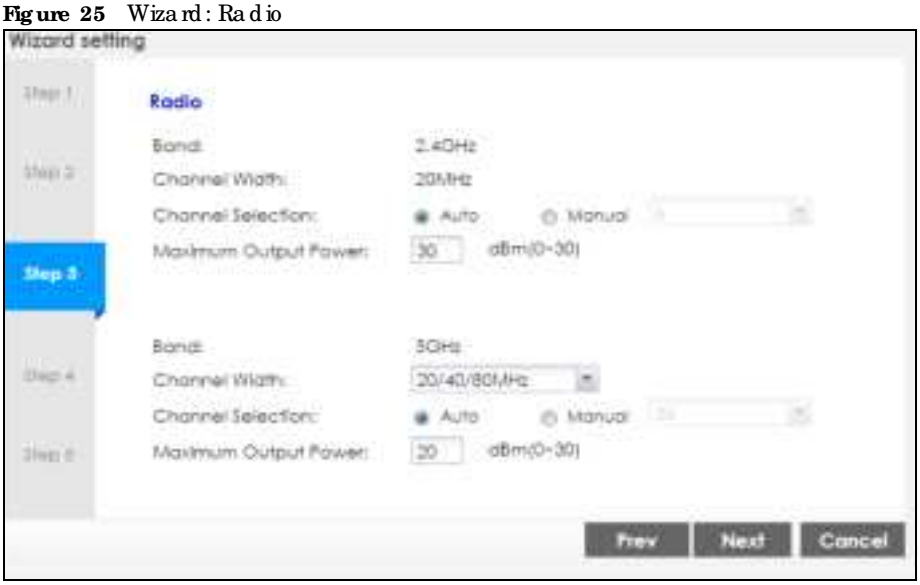
Use this screen to configure the Zyxel Device's radio transmitter(s).

- **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 25 Wizard: Radio



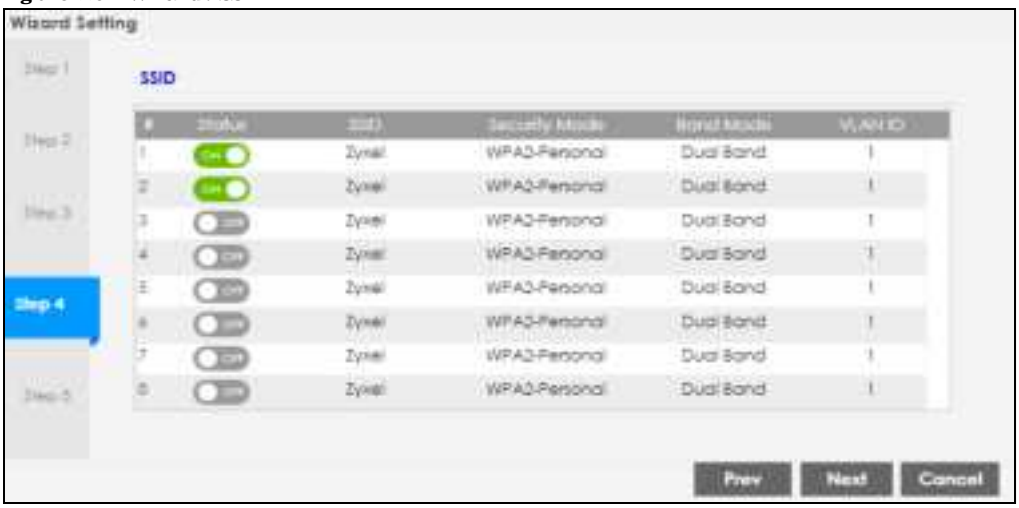
7.2.4 Step 4 SSID

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 52 for more information.

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

Figure 26 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 wireless band which this profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients. 5 GHz is the frequency used by IEEE 802.11ac/a/n wireless clients.
- **Security Type**: Select **WPA2** to add security on this wireless network. Otherwise, select **OPEN** to allow any wireless 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.

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

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 27 Wizard: Summary

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 55) displays general LAN interface information and packet statistics.
- The **AP Information > Radio List** screen (Section 8.4 on page 57) displays statistics about the wireless radio transmitters in the Zyxel Device.
- The **Station Info** screen (Section 8.5 on page 61) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen (Section 8.6 on page 62) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen (Section 8.7 on page 63) displays information about suspected rogue APs.
- The **View Log** screen (Section 8.8 on page 66) displays the Zyxel Device's current log messages. You can change the way the log is displayed, you can e-mail 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. See Chapter 13 on page 117 for details.

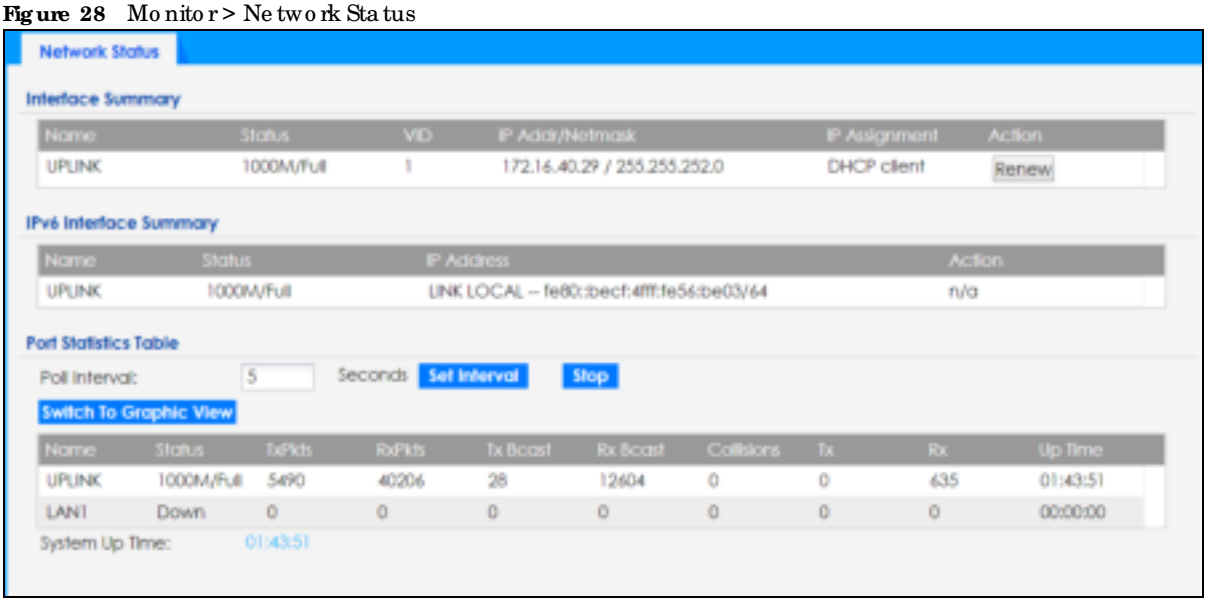
Friendly AP

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). See Chapter 13 on page 117 for details.

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 28 Monitor > Network Status



The following table describes the labels in this screen.

Table 17 Monitor > Network Status

LABEL	DESCRIPTION
Interface Summary IPv6 Interface Summary	Use the **Interface Summary** section for IPv4 network settings. Use the **IPv6 Interface Summary** 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. **Down** - The port is not connected. **Speed / Duplex** - The port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
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. **Static** - This interface has a static IPv4 address. **DHCP Client** - 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 **Renew** 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 **n/a**.
Port Statistics Table	
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.

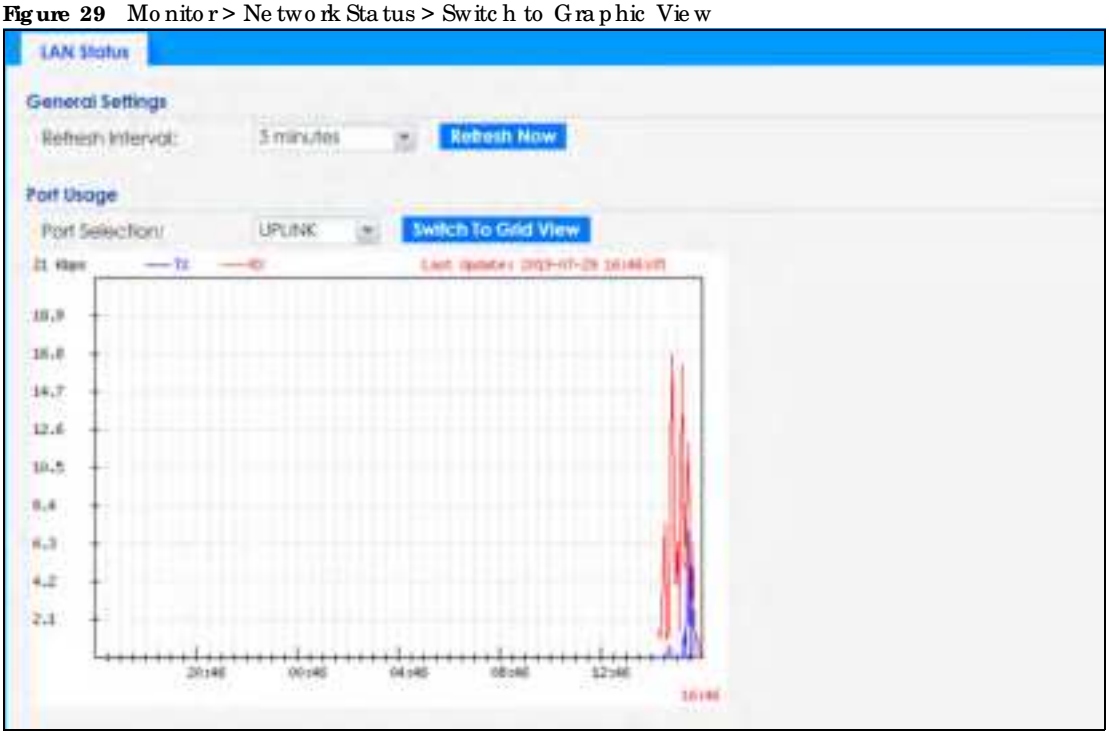
Table 17 Monitor > Network Status (continued)

LABEL	DESCRIPTION
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.
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. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the ZyxelDevice on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the ZyxelDevice on the physical port since it was last connected.
Tx Bcast	This field displays the number of broadcast packets transmitted from the ZyxelDevice on the physical port since it was last connected.
Rx Bcast	This field displays the number of broadcast packets received by the ZyxelDevice 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 ZyxelDevice 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 29 Monitor > Network Status > Switch to Graphic View



The following table describes the labels in this screen.

Table 18 Monitor > Network Status > Switch to Graphic View

LABEL	DESCRIPTION
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 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 wireless radio transmitters. To access this screen, click **Monitor > Wireless > AP Information > Radio List**.

Figure 30 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that supports WDS)

Figure 31 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that does not support WDS)

The following table describes the labels in this screen.

Table 19 Monitor > Wireless > AP Information > 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.
Loading	This indicates the AP's load balance status (**UnderLoad** or **OverLoad**) when load balancing is enabled on the Zyxel Device. Otherwise, it shows **-** when load balancing is disabled or the radio is in monitor mode.
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 **AP (MBSSID)**, **MONITOR**, **Root AP** or **Repeater**.
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. This shows **-** when the radio is in monitor mode.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of wireless clients connected to this radio on the Zyxel Device.

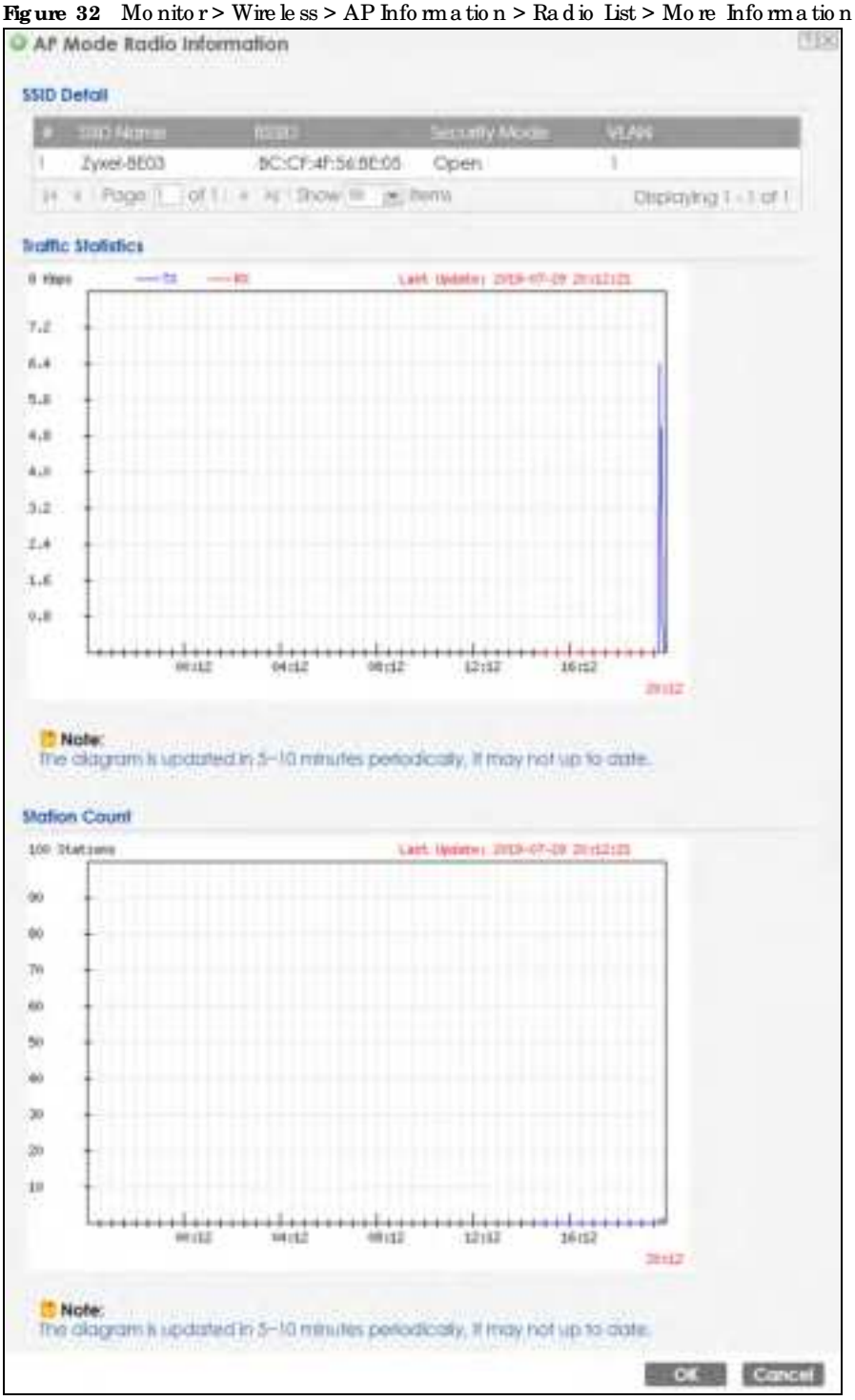
Table 19 Monitor > Wireless > AP Information > Radio List (continued)

LABEL	DESCRIPTION
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 32 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

Table 20 Monitor > Wireless > AP Information > Radio List > More Information

LABEL	DESCRIPTION
SSID Detail	This list shows information about all the wireless clients that have connected to the specified radio over the preceding 24 hours.
#	This is the item's sequential number in the list. It has no bearing on the actual data in this list.

Table 20 Monitor > Wireless > AP Information > Radio List > More Information (continued)

LABEL	DESCRIPTION
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 "wireless clients"). Click **Monitor > Wireless > Station Info** to access this screen.

Figure 33 Monitor > Wireless > Station Info

The following table describes the labels in this screen.

Table 21 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.
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 IEEE 802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (**N/A**).

Table 21 Monitor > Wireless > Station Info (continued)

LABEL	DESCRIPTION
SSID Name	This indicates the name of the wireless 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 wireless 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 wireless 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 1.2 on page 12 to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

Figure 34 Monitor > Wireless > WDS Link Info

The following table describes the labels in this screen.

Table 22 Monitor > Wireless > WDS Link Info

LABEL	DESCRIPTION
WDS Uplink Info WDS Downlink Info	**Uplink** refers to the WDS link from the repeaters to the root AP. **Downlink** refers to the WDS link from the root AP to the repeaters. When the Zyxel Device is in root AP mode and connected to a repeater, only the downlink information is displayed. When the Zyxel Device is in repeater mode and connected to a root AP directly or via another repeater, the uplink information is displayed. 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.
#	This is the index number of the root AP or repeater in this list.

Table 22 Monitor > Wireless > WDS Link Info (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC address of the root AP or repeater 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 wireless 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. Not all Zyxel Devices support monitor mode (see Section 1.4 on page 18). For more information about Rogue APs, see Section 10.3 on page 79.

Note: If the Zyxel Device supports monitor mode, the radio or at least one of the Zyxel Device's radio must be set to monitor mode (in the **Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

If the Zyxel Device does not support monitor mode, turn on rogue AP detection in the **Configuration > Wireless > Rogue AP** screen to detect other APs.

Figure 35 Monitor > Wireless > Detected Device (for Zyxel Device that supports Monitor mode)

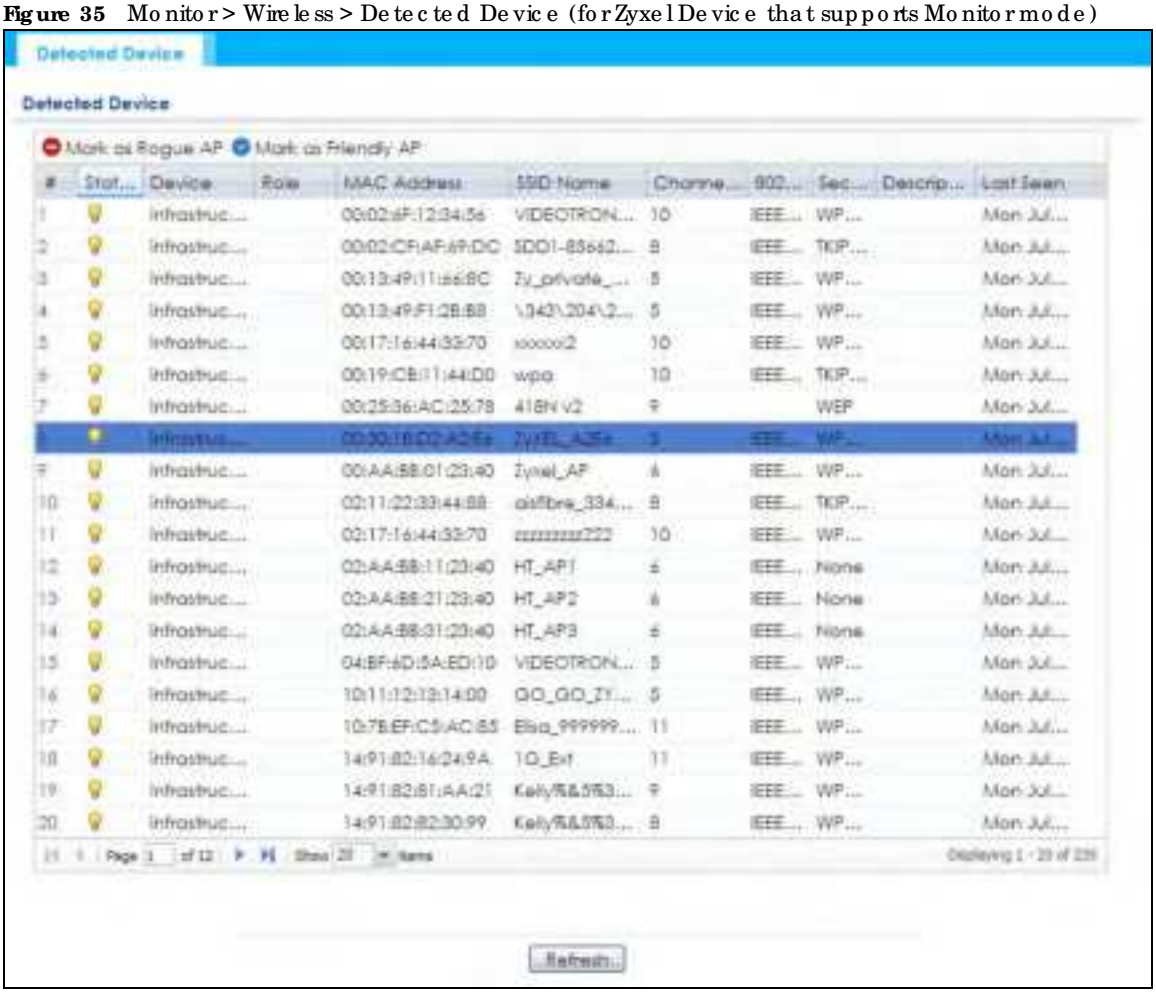
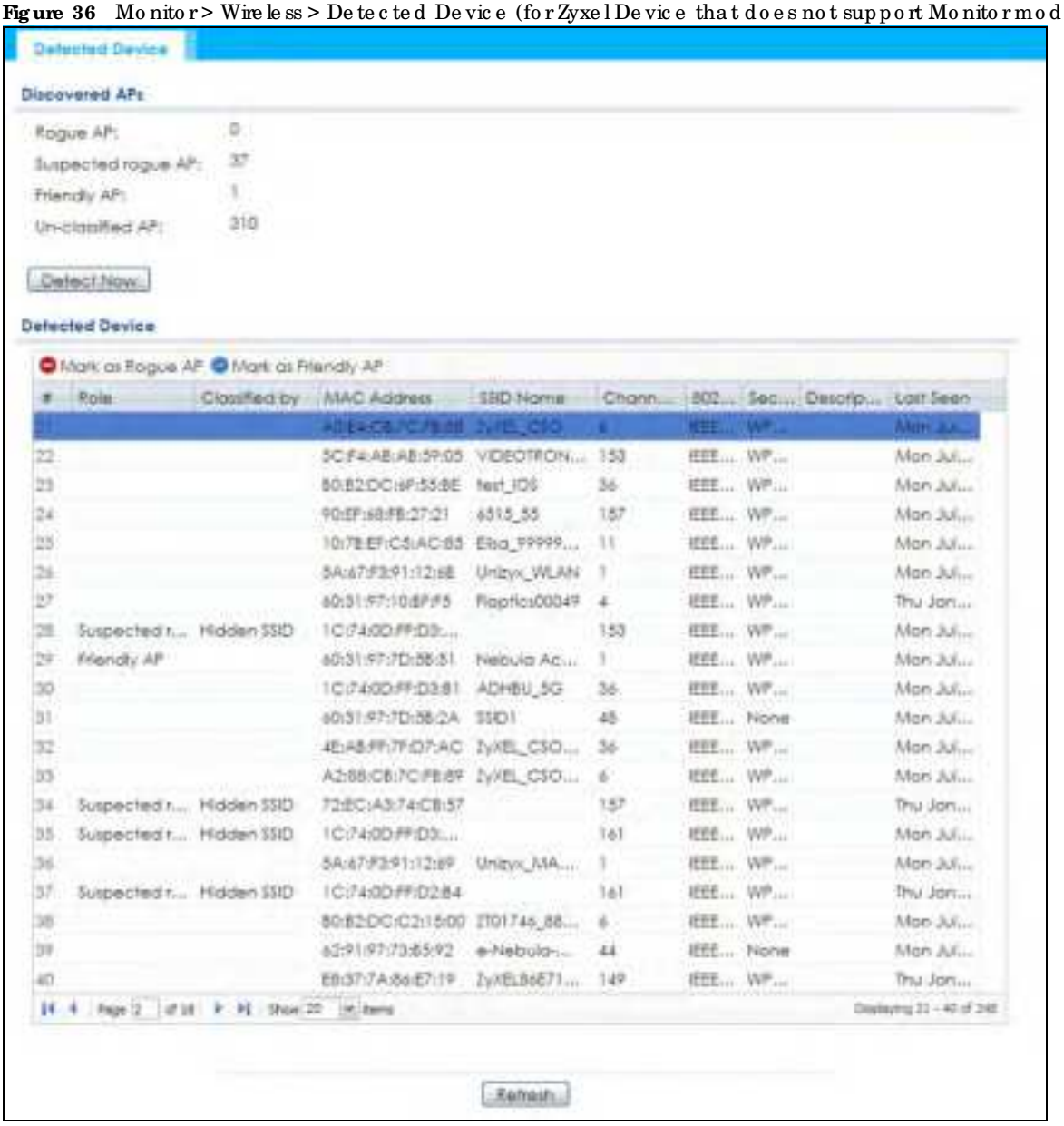


Figure 36 Monitor > Wireless > Detected Device (for Zyxel Device that does not support Monitor mode)



The following table describes the labels in this screen.

Table 23 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 Section 10.3 on page 79.
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	

Table 23 Monitor > Wireless > Detected Device (continued)

LABEL	DESCRIPTION
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. For more on managing rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 10.3 on page 79).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the **Configuration > Wireless > Rogue AP** screen (Section 10.3 on page 79).
#	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.
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.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 10.3 on page 79).
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.

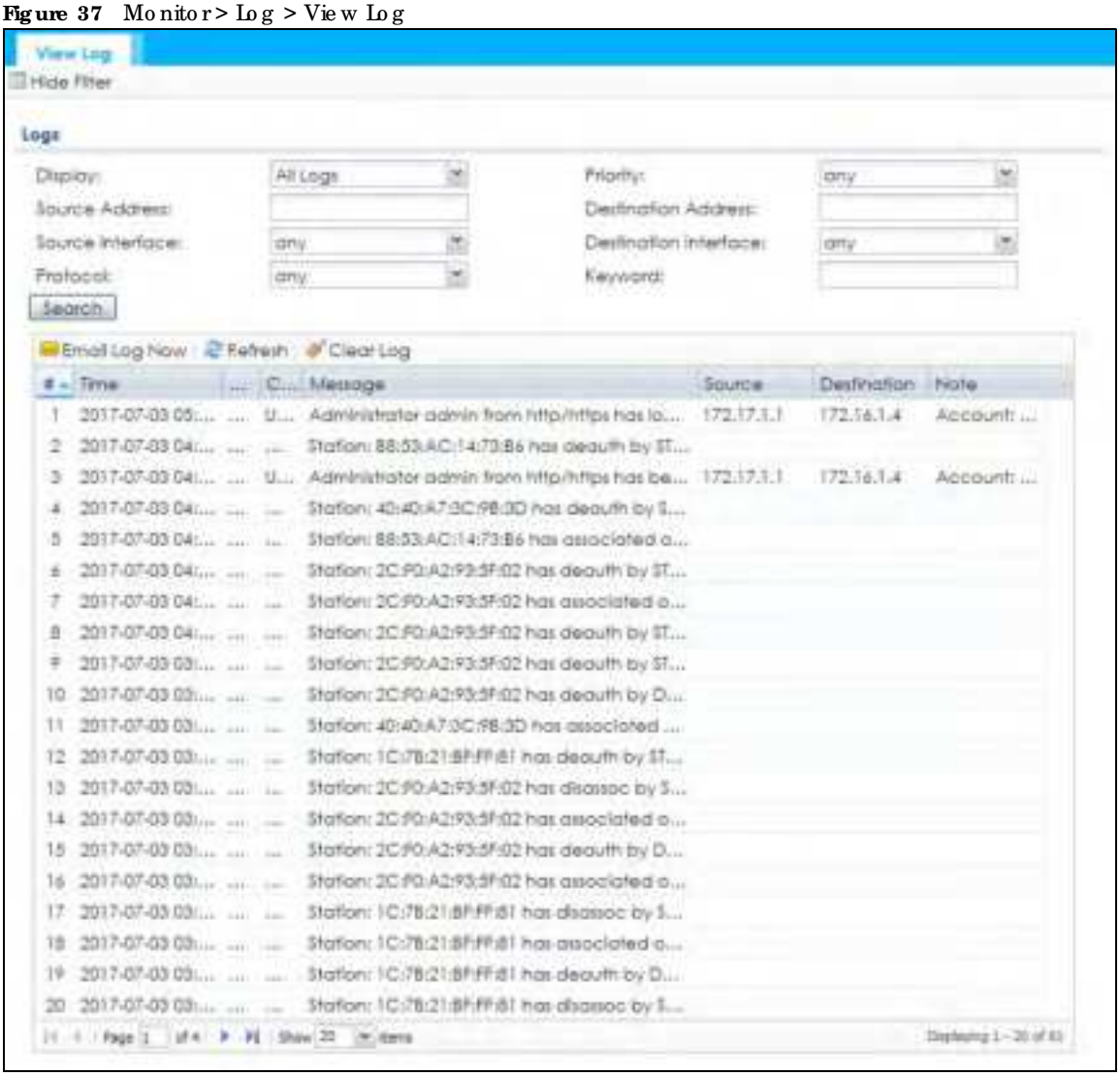
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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 37 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 24 Monitor > 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 **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
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: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
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.

Table 24 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
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 **Message**, **Source**, **Destination** and **Note** 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.
Email Log Now	Click this button to send log messages to the **Active** e-mail addresses specified in the **Send Log To** field on the **Configuration > Log & Report > Log Settings** screen.
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 **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** 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.

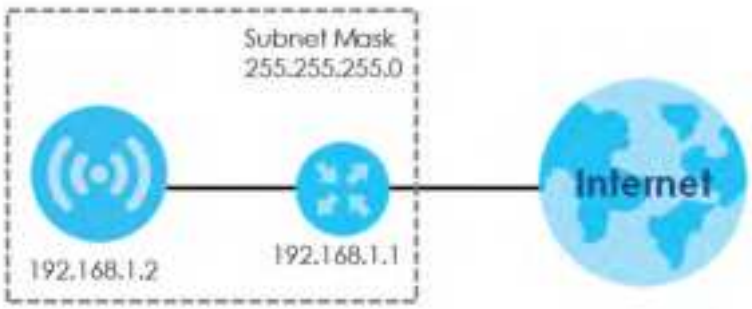
CHAPTER 9
Network

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 38 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.

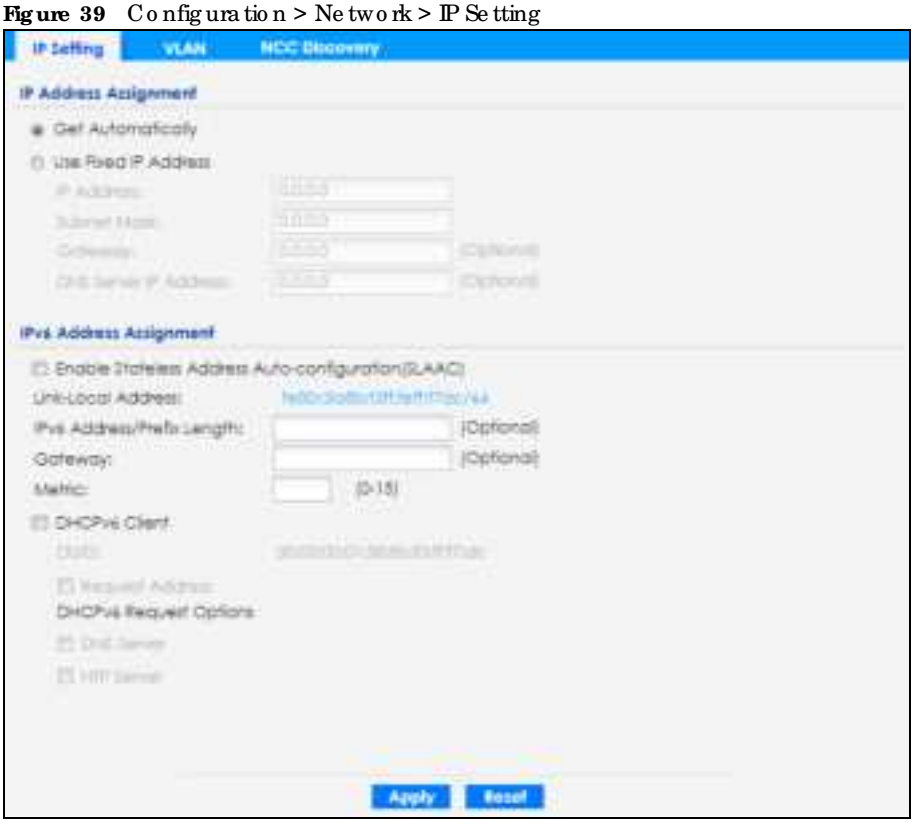
9.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 9.2 on page 69) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 9.3 on page 71) configures the Zyxel Device's VLAN settings.
- The **NCC Discovery** screen (Section 9.4 on page 73) 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 39 Configuration > Network > IP Setting



Each field is described in the following table.

Table 25 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 25 Configuration > Network > IP Setting (continued)

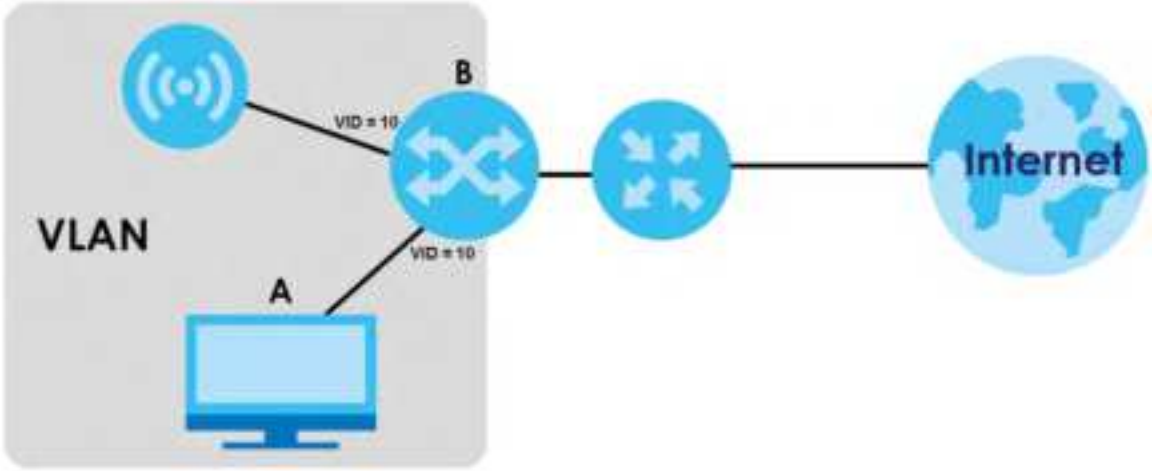
LABEL	DESCRIPTION
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, 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 Appendix B on page 230 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** 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 in your Zyxel Device can make it inaccessible. If this happens, you will have to reset the Zyxel Device.

Figure 40 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.

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**.

The screen varies depending on whether the Zyxel Device has an extra Ethernet port (except the uplink port).

Figure 41 Configuration > Network > VLAN (for Zyxel Device with one Ethernet port)

Each field is described in the following table.

Table 26 Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device.
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.
IAN Setting	
Port Setting	
Edit	Double-click an entry or select it and click **Edit** 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.
Activate/ Inactivate	To turn on an entry, select it and click **Activate**. To turn off an entry, select it and click **Inactivate**.
#	This is the index number of the port.

Table 26 Configuration > Network > VLAN (continued)

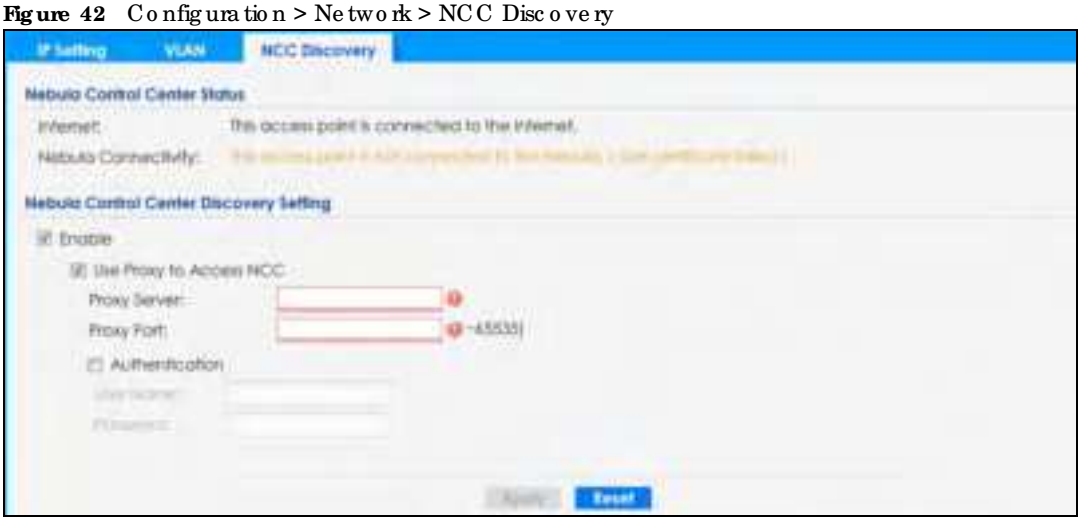
LABEL	DESCRIPTION
Status	This field indicates whether the port is enabled (a yellow bulb) or not (a gray bulb).
Port	This field displays the name of the port.
PVID	This field displays the port number of the VLAN ID.
VLAN Configuration	
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** 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 **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate / Inactivate	To turn on an entry, select it and click **Activate**. To turn off an entry, select it and click **Inactivate**.
#	This is the index number of the VLAN ID.
Status	This field indicates whether the VLAN is enabled (a yellow bulb) or not (a gray bulb).
Name	This field displays the name of each VLAN.
VID	This field displays the VLAN ID.
Member	This field displays the VLAN membership to which the port belongs.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** 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 42 Configuration > Network > NCC Discovery



Each field is described in the following table.

Table 27 Configuration > Network > 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	
Enable	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. If NCC discovery is disabled, the Zyxel Device will not discover the NCC and remain in standalone operation.
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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

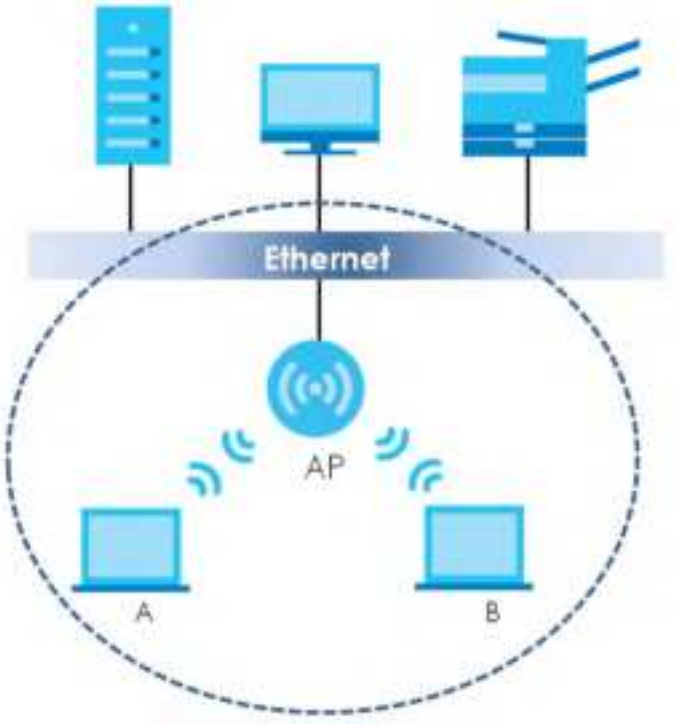
CHAPTER 10
Wireless

10.1 Overview

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

The following figure provides an example of a wireless network.

Figure 43 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless 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 76) allows you to manage the Zyxel Device's general wireless settings.
- The **Rogue AP** screen (Section 10.3 on page 79) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen (Section 10.4 on page 83) allows you to configure network traffic load balancing between the APs and the Zyxel Device.
- The **DCS** screen (Section 10.4 on page 83) 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 / Wireless Client

A station or wireless client is any wireless-capable device that can connect to an AP using a wireless 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 84.

10.2 AP Management

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

Figure 44 Configuration > Wireless > AP Management

Each field is described in the following table.

Table 28 Configuration > Wireless > AP Management

LABEL	DESCRIPTION
Radio 1 Setting	
Radio 1 Activate	Select the checkbox to enable the Zyxel Device's first (default) radio.

Table 28 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Radio 1 OP Mode	Select the operating mode for radio 1. **AP Mode** means the radio can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients (see Section 1.2.3 on page 14). **Root AP** 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. **Repeater** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.
Radio 1 Profile	Select the radio profile the radio uses. Note: You can only apply a 2.4G AP radio profile to radio 1. Otherwise, the first radio will not be working.
Radio 1 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the **Radio 1 Uplink MAC Address** field.
Max Output Power	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. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Edit	Click **Edit** 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	
Radio 2 Activate	This displays if the Zyxel Device has a second radio. Select the check box to enable the Zyxel Device's second radio.

Table 28 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Radio 2 OP Mode	This displays if the Zyxel Device has a second radio. Select the operating mode for radio 2. **AP Mode** means the radio can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients (see Section 1.2.3 on page 14). **Root AP** 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. **Repeater** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.
Radio 2 Profile	This displays if the Zyxel Device has a second radio. Select the radio profile the radio uses. Note: You can only apply a 5G AP radio profile to radio 2. Otherwise, the second radio will not be working.
Radio 2 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with tbe MAC address specified in the **Radio 2 Uplink MAC Address** field.
Max Output Power	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. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Edit	Click **Edit** ( ) 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.3 Rogue AP

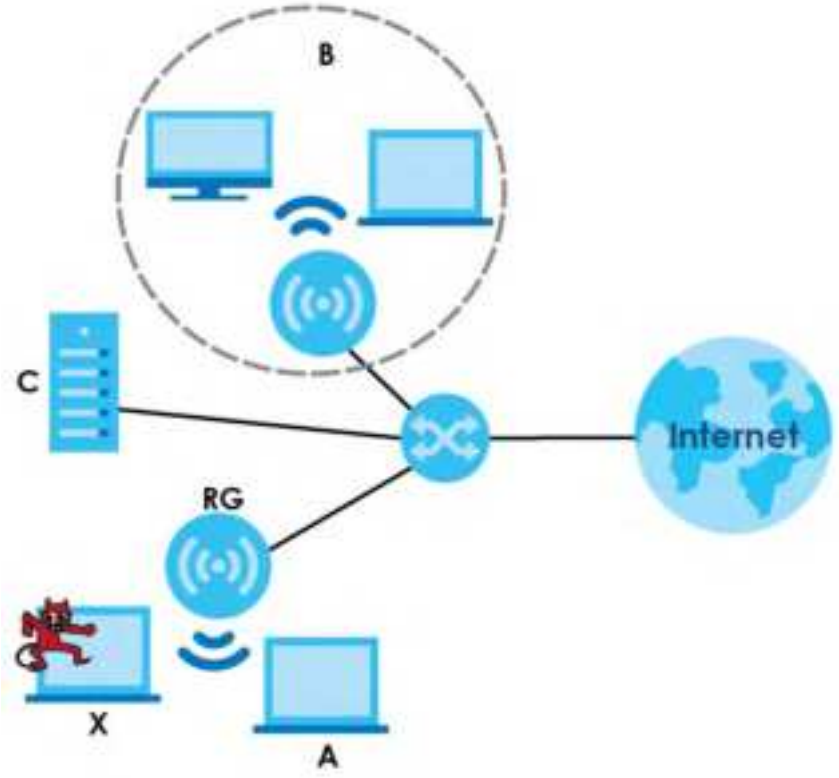
Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

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 wireless 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 45 Rogue AP Example



Friendly APs

If you have more than one AP in your wireless 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 1.2.3 on page 14). 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 1.4 on page 18 to

know which models support **Rogue AP Detection**.

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

Figure 46 Configuration > Wireless > Rogue AP (for Zyxel Devices that support Monitor mode)

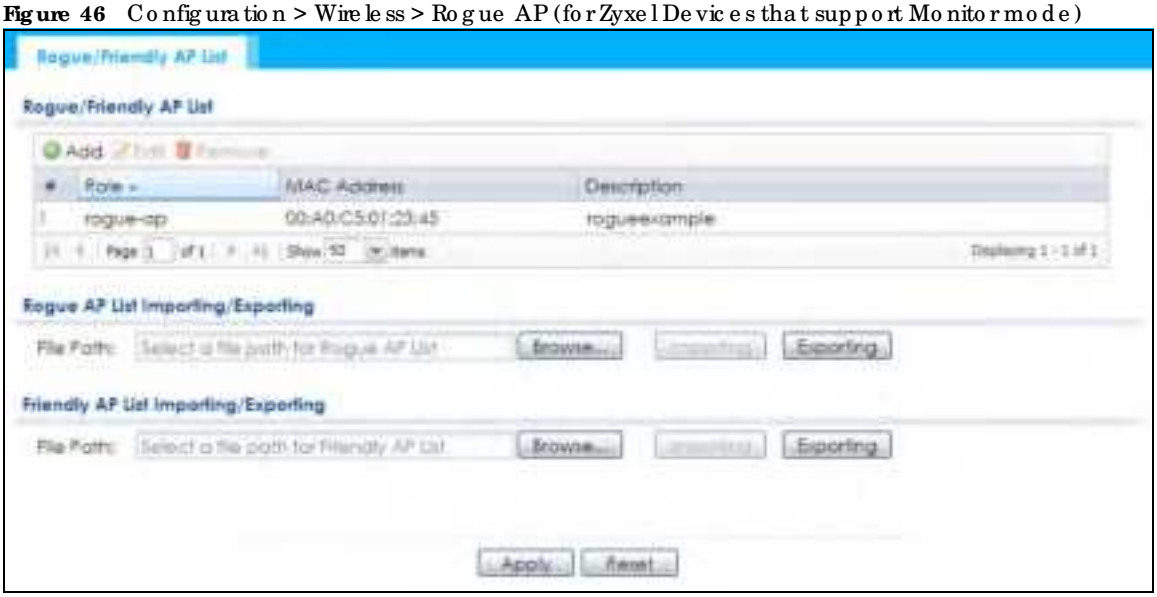
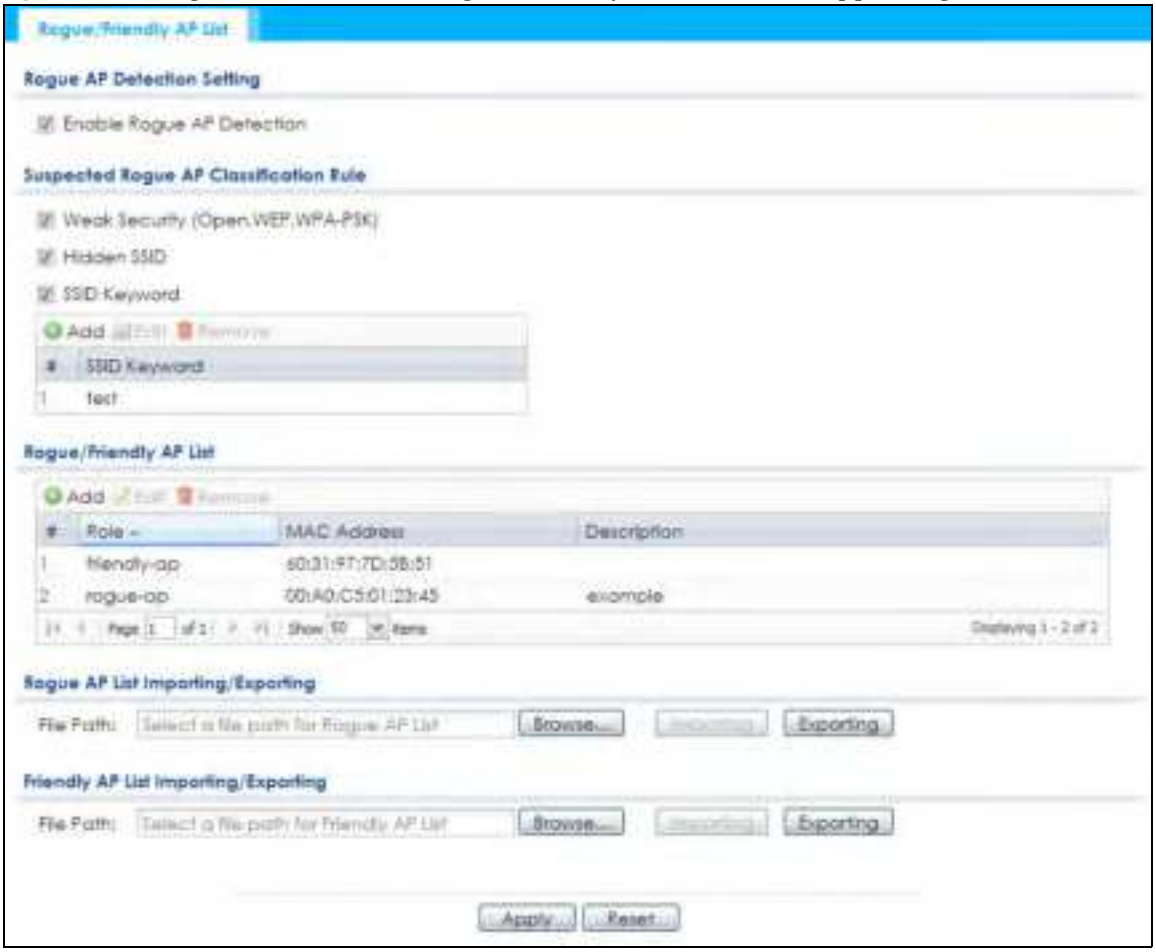


Figure 47 Configuration > Wireless > Rogue AP (for Zyxel Devices that support Rogue AP Detection)



Each field is described in the following table.

Table 29 Configuration > Wireless > Rogue AP

LABEL	DESCRIPTION
Rogue AP Detection Setting	
Enable Rogue AP Detection	Select this check box to detect Rogue APs in the network.
Suspected Rogue AP Classification Rule	Select the check boxes (**Weak Security (Open, WEP, WPA-PSK)**, **Hidden SSID**, **SSID Keyword**) 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.
Rogue/Friendly AP List	
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.
#	This field is a sequential value, and it is not associated with any interface.

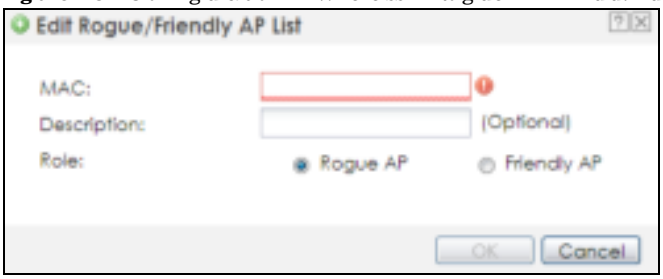
Table 29 Configuration > Wireless > Rogue AP (continued)

LABEL	DESCRIPTION
Role	This field indicates whether the selected AP is a **rogue-ap** or a **friendly-ap**. To change the AP's role, click the **Edit** 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 **Edit** 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 **Browse** button to locate it. Once the **File Path** field has been populated, click **Importing** 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** 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 48 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List



Each field is described in the following table.

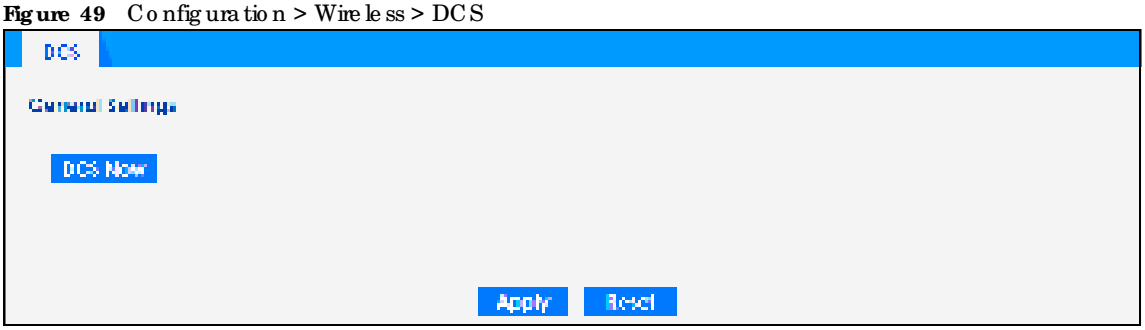
Table 30 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

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 **Rogue AP** or **Friendly AP** for the AP's role.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** 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 76). Click **Configuration > Wireless > DCS** to access this screen.

Figure 49 Configuration > Wireless > DCS



Each field is described in the following table.

Table 31 Configuration > Wireless > DCS

LABEL	DESCRIPTION
DCS Now	Click this to have the ZyxelDevice scan for and select an available channel immediately.
Apply	Click **Apply** to save your changes back to the ZyxelDevice.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.5 Technical Reference

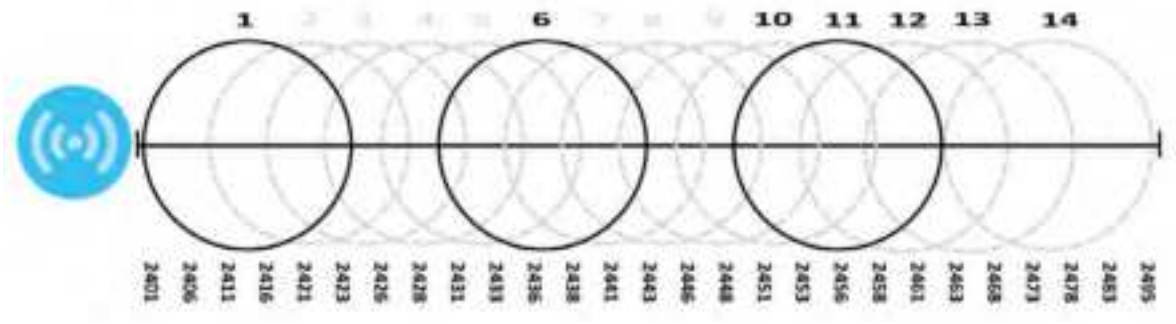
The following section contains additional technical information about the features described in this chapter.

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.

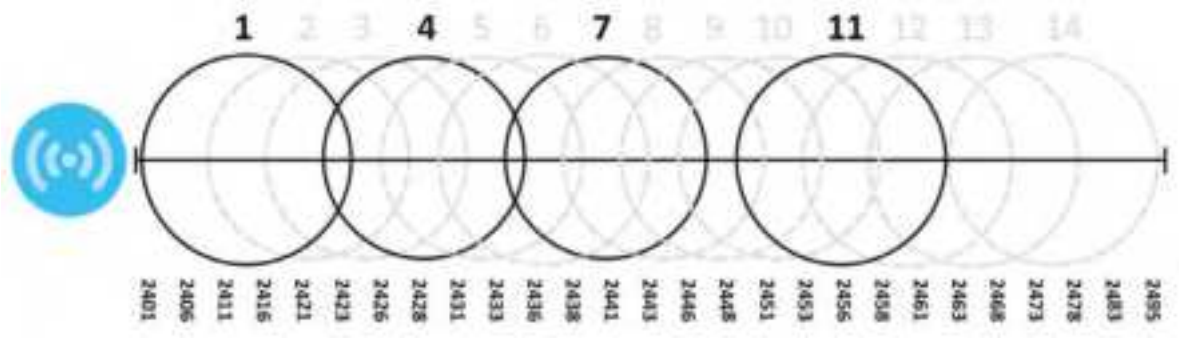
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 50 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.

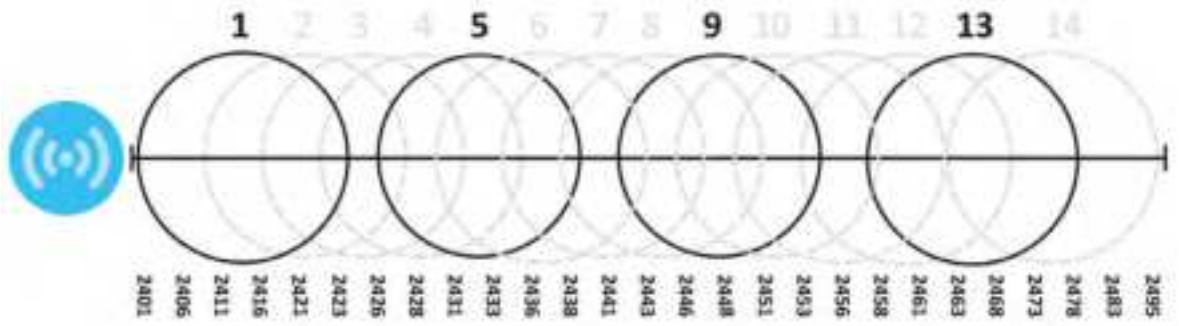
Figure 51 An Example Four-Channel Deployment



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 that the other one.

Figure 52 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 87) provides a summary of all user accounts.
- The **Setting** screen (see Section 11.3 on page 89) 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 32 Types of User Accounts

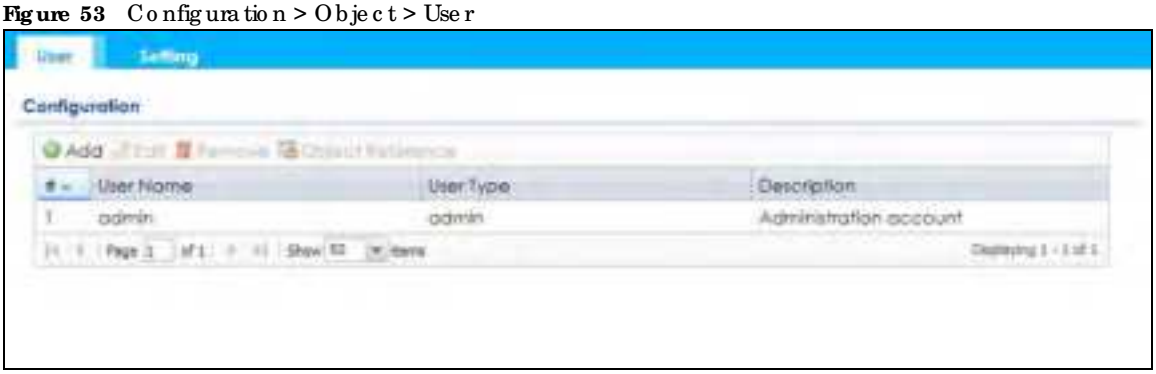
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, TELNET, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access 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 53 Configuration > Object > User



The following table describes the labels in this screen.

Table 33 Configuration > Object > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Object Reference	Select an entry and click **Object Reference** 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. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this user has access to the Zyxel Device's services but cannot look at the configuration
Description	This field displays the description for each user.

11.2.1 Add/Edit User

The **User Add/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 usernames are:

- Usernames 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'.
- Usernames have to be different than usergroup names.
- Here are the reserved usernames:

• 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 54 Configuration > Object > User > Add/Edit A User

The following table describes the labels in this screen.

Table 34 Configuration > User > User > Add/Edit A User

LABEL	DESCRIPTION
User Name	Type the username 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. Usernames have to be different than usergroup names, and some words are reserved.
User Type	Select what type of user this is. Choices are: • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
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 34 Configuration > User > User > Add/Edit A User (continued)

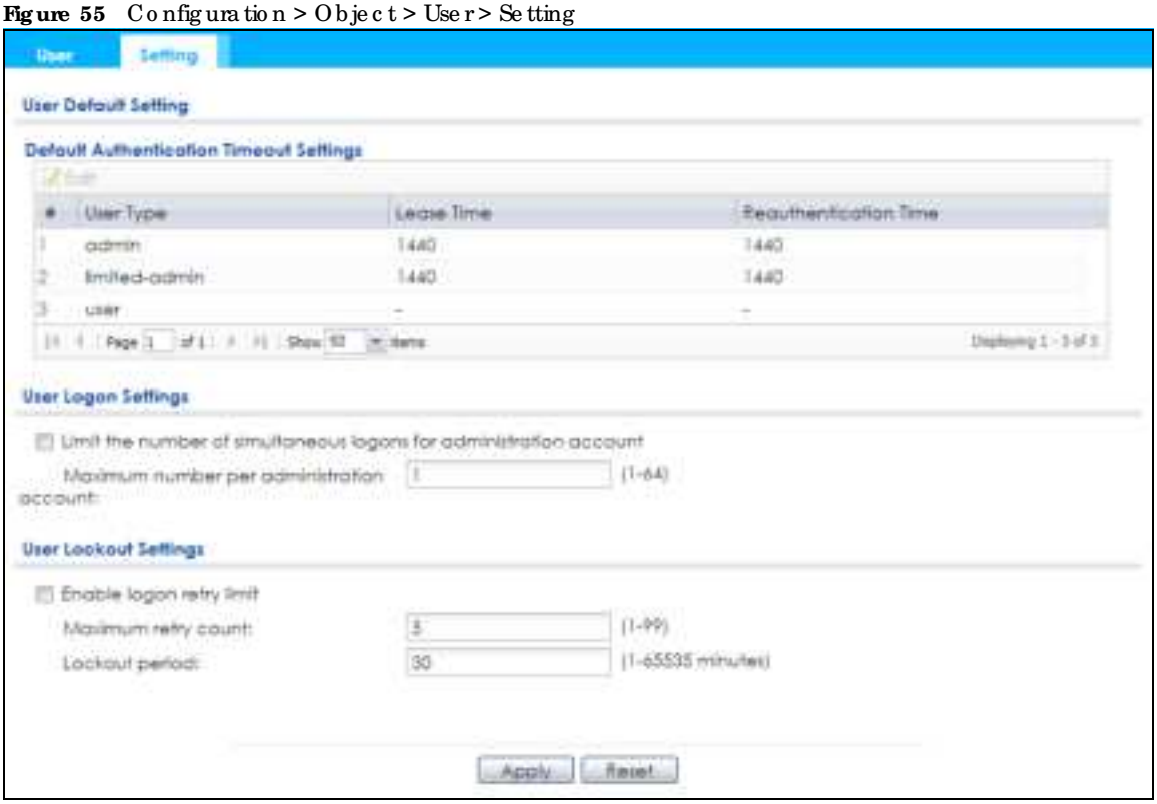
LABEL	DESCRIPTION
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.
Lease Time	This field is not available if the user type is **user**. 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 **user**. 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 **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** 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 55 Configuration > Object > User > Setting



The following table describes the labels in this screen.

Table 35 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 **Edit** 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. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
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 **Lease Time**, the user has no opportunity to renew the session without logging out.
User Logon Settings	

Table 35 Configuration > Object > User > Setting (continued)

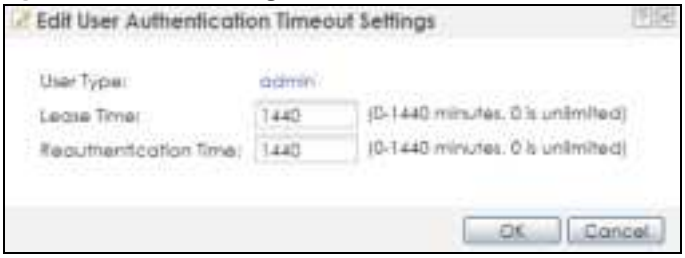
LABEL	DESCRIPTION
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** 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 **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** 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 56 User > Setting > Edit User Authentication Timeout Settings



The following table describes the labels in this screen.

Table 36 User > Setting > Edit User Authentication Timeout Settings

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the Zyxel Device. • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it.
Lease Time	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. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** 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.
Reauthentication Time	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 **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** 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 94) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 12.3 on page 100) 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 wireless 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 wireless 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 wireless 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.

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 wireless 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 wireless 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.

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).

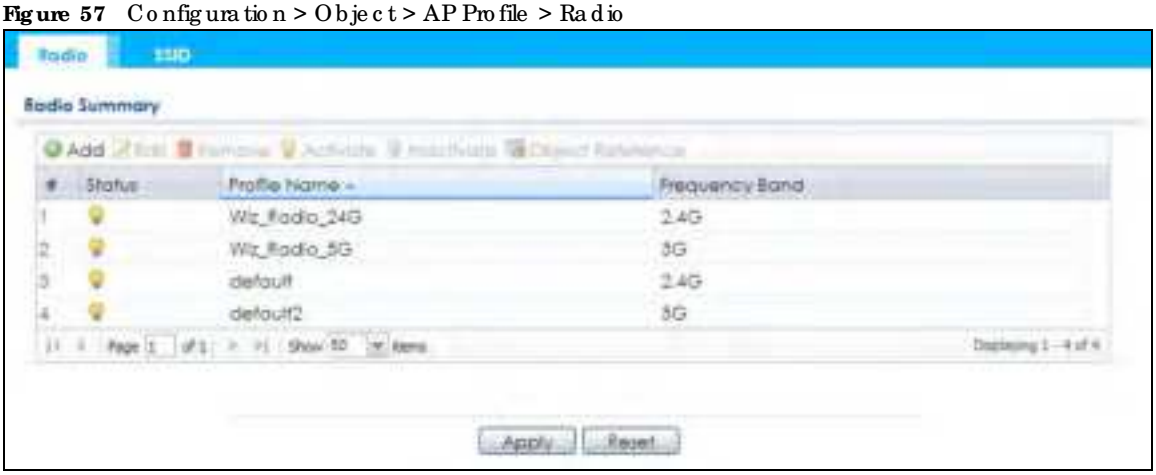
The IEEE 802.11v BSS Transition Management feature lets an AP automatically provide load information of the neighbor APs to clients. It helps the Zyxel Device steer clients to a suitable AP for better performance or load balancing.

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 57 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

Table 37 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 **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** 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 58 Configuration > Object > AP Profile > Radio > Add/Edit

The following table describes the labels in this screen.

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the **Advanced Settings** in this window.
General Settings	
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 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
802.11 Mode	Select how to let wireless clients connect to the AP. If **802.11 Band** is set to **2.4G**: • **11b/g**: 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. • **11n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. • **11ax**: 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. If **802.11 Band** is set to **5G**: • **11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • **11n**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the Zyxel Device. • **11ac**: 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. • **11ax**: 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.
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood. Select **20/40 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference. Select **20/40/80** 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 **11ac** or **11ax** in the **802.11 Mode** field. Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	This is the radio channel which the signal will use for broadcasting by this radio profile. • **DCS**: Choose Dynamic Channel Selection to have the Zyxel Device choose a radio channel that has least interference. • **Manual**: Choose from the available radio channels in the list. If your Zyxel Device is outdoor type, be sure to choose non-indoors channels.
Enable DCS Client Aware	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. 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 when it switches channels are dropped.
Enable DCS Client Aware	This field is available when you set **Channel Selection** to **DCS**. 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. 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 when it switches channels are dropped.

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Selection Method	This field is available when you set **Channel Selection** to **DCS**. Select how you want to specify the channels the Zyxel Device switches between for 2.4 GHz operation. Select **auto** to have the Zyxel Device display a **2.4 GHz Channel Deployment** field you can use to limit channel switching to 3 or 4 channels. Select **manual** to select the individual channels the Zyxel Device switches between. Note: The method is automatically set to **auto** when no channel is selected or any one of the previously selected channels is not supported.
Channel ID	This field is available only when you set **Channel Selection** to **DCS** and set **2.4 GHz Channel Selection Method** to **manual**. Select the channels that you want the Zyxel Device to use.
2.4 GHz Channel Deployment	This is available when you set **Channel Selection** to **DCS** and the **2.4 GHz Channel Selection Method** is set to **auto**. Select **Three-Channel Deployment** 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. Select **Four-Channel Deployment** 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.
Enable 5 GHz DFS Aware	This field is available only when you select **5G** in the **802.11 Band** field, set **Channel Selection** to **DCS** and set **5 GHz Channel Selection Method** to **auto**. Select this if your APs are operating in an area known to have RADAR devices. This allows the Zyxel Device to downgrade its frequency to below 5 GHz in the event RADAR signal is detected, thus preventing it from interfering with that signal. Enabling this forces the AP to select a non-DFS channel.
5 GHz Channel Selection Method	Select how you want to specify the channels the Zyxel Device switches between for 5 GHz operation. Select **Auto** to have the Zyxel Device automatically select the best channel. Select **manual** to select the individual channels the Zyxel Device switches between. Note: The method is automatically set to **auto** when no channel is selected or any one of the previously selected channels is not supported.
Channel ID	This field is available only when you set **Channel Selection** to **DCS** and set **5 GHz Channel Selection Method** to **manual**. Select the channels that you want the Zyxel Device to use.
Time Interval	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.
DCS Time Interval	This field is available when you set **Channel Selection** to **DCS** and select the **Time Interval** option. 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.

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
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	This field is available only when the channel width is **20/40MHz** or **20/40/80MHz** and the **802.11 Mode** is either **11n** or **11ac**. Set the guard interval for this radio profile to either **short** or **long**. 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.
Enable A-MPDU Aggregation	This field is not available when you set **802.11 Mode** to **11a** or **11b/g**. Select this to enable A-MPDU aggregation. 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.
Enable A-MSDU Aggregation	This field is not available when you set **802.11 Mode** to **11a** or **11b/g**. Select this to enable A-MSDU aggregation. 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.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless 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 fragmentation threshold to turn RTS/CTS off.
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	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -105 is the weakest.

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the Zyxel Device disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -105 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP
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	This field is available if **802.11 Band** is set to **5G** and **Channel Selection** is set to **DCS**. 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.
Enable 802.11d	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. 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.
Multicast Settings	
Transmission Mode	Specify how the Zyxel Device handles wireless multicast traffic. Select **Multicast to Unicast** to broadcast wireless multicast traffic to all of the wireless 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. Select **Fixed Multicast Rate** to send multicast traffic to all wireless clients at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate (Mbps)	If you set **Transmission Mode** to **Fixed Multicast Rate**, select a data rate at which the Zyxel Device transmits multicast packets to wireless clients. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.
WLAN Rate Control Setting	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. 5, 6, 9, 11, 12, 18, 24, 36, 48, 54. 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. 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.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** 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 wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

12.3.1 SSID List

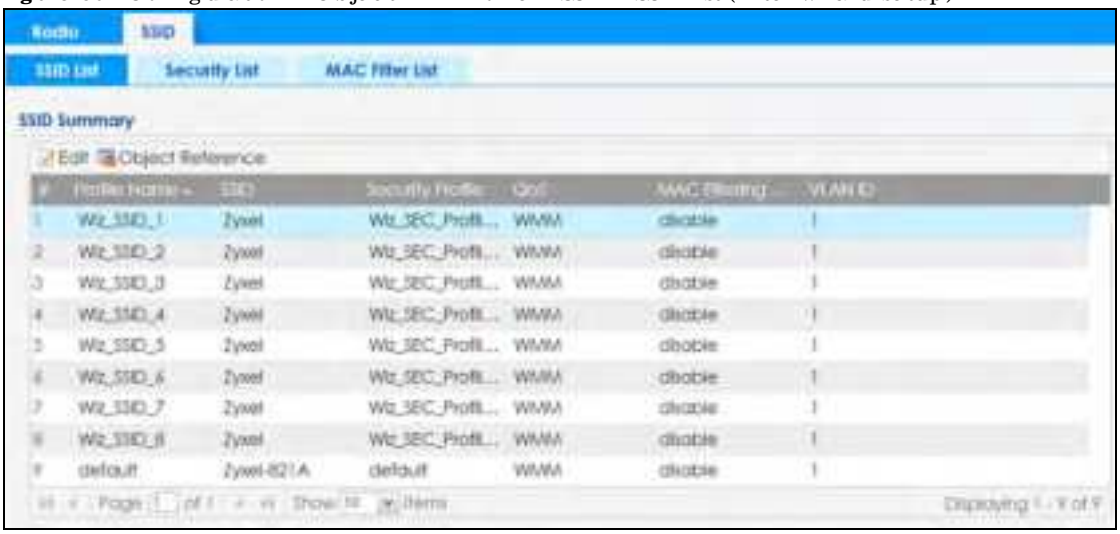
This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless 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 59 Configuration > Object > AP Profile > SSID > SSID List (Default)

Figure 60 Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)



The following table describes the labels in this screen.

Table 39 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.

Table 39 Configuration > Object > AP Profile > SSID > SSID List (continued)

LABEL	DESCRIPTION
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 wireless 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.
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 61 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (NWA50AX)

The following table describes the labels in this screen.

Table 40 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 wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.

Table 40 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The **disable** setting means no MAC filtering is used.
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: **disable**: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. **WMM**: 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. **WMM_VOICE**: 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. **WMM_VIDEO**: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. **WMM_BEST_EFFORT**: 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. **WMM_BACKGROUND**: 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.
Rate Limiting	
Downlink	Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
Uplink	Define the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When a SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID 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 wireless clients connected to the Zyxel Device using this SSID profile.
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.

Table 40 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

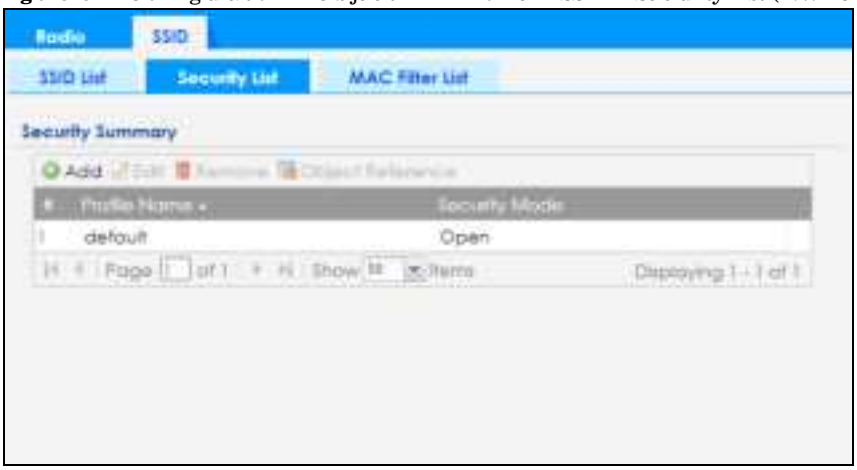
12.4 Security List

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 62 Configuration > Object > AP Profile > SSID > Security List (NWA50AX)



The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
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.

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

Figure 63 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none (NWA50AX)

The following table describes the labels in this screen.

Table 42 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: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Advance Note: Click on the **Show Advanced Settings** 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.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 64 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open

The following table describes the labels in this screen.

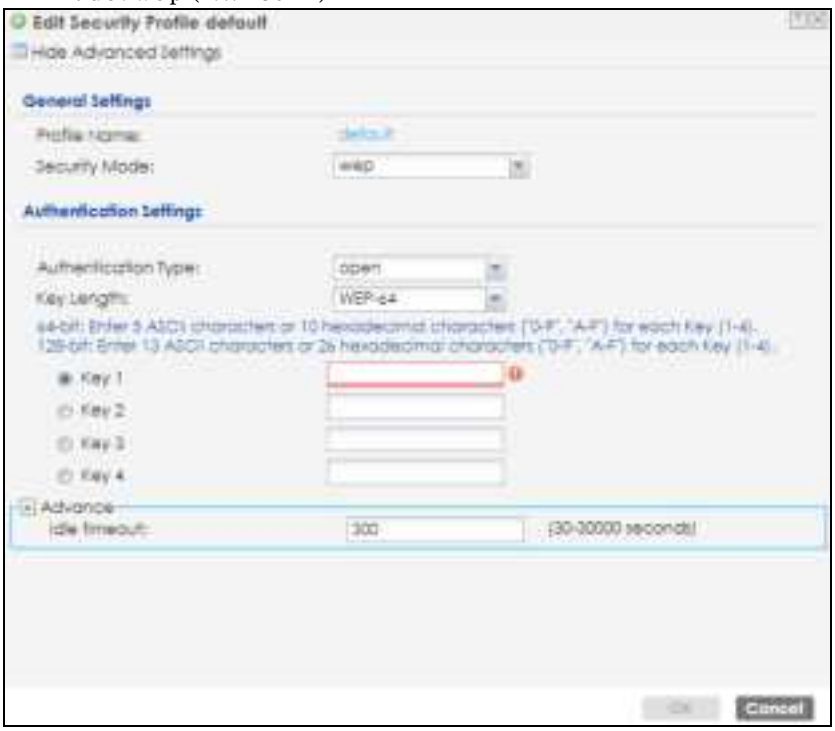
Table 43 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open

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: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Transition Mode	Enable this for backwards compatibility. This option is only available if the **Security Mode** is **wpa3** or **enhanced-open**. This creates two virtual APs (VAPs) with a primary (**wpa3** or **enhanced-open**) and fallback (**wpa2** or **none**) security method. If the **Security Mode** is **wpa3**, enabling this will force **Management Frame Protection** to be set to **Optional**. If this is disabled or if the **Security Mode** is **enhanced-open**, **Management Frame Protection** will be set to **Required**.
Advance Note: Click on the **Show Advanced Settings** 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.

Table 43 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open (continued)

LABEL	DESCRIPTION
Management Frame Protection	This field is available only when you select **wpa2** in the **Security Mode** field and set **Cipher Type** to **aes**. 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 checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. Select **Optional** if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select **Required** and wireless clients must support MFP in order to join the Zyxel Device's wireless network.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 65 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wep (NWA50AX)

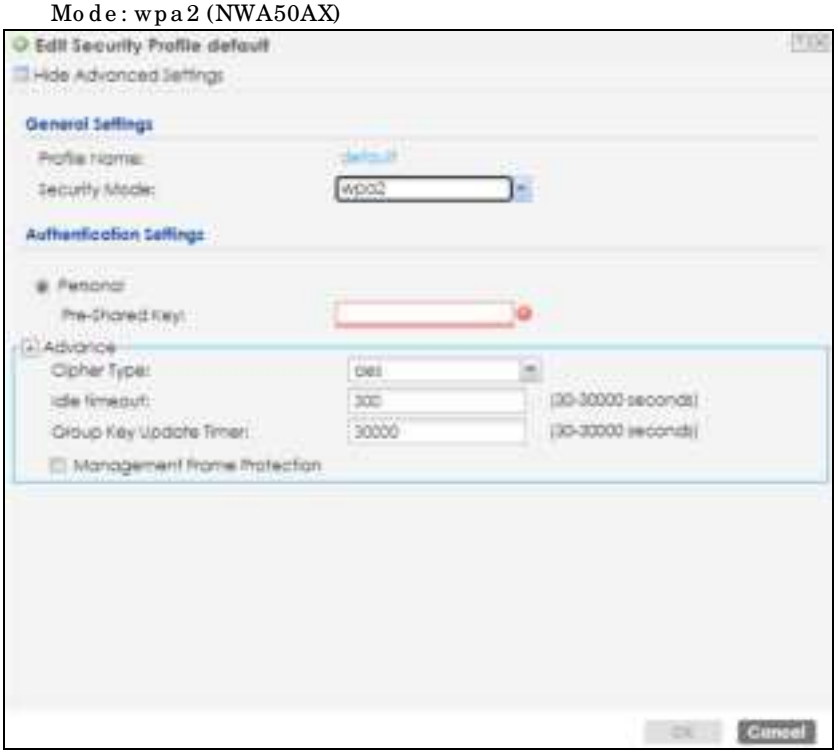


The following table describes the labels in this screen.

Table 44 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: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Authentication Type	Select a WEP authentication method. Choices are **Open** or **Share** key.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select **WEP-64**: • Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each **Key** used. or • Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each **Key** used. If you select **WEP-128**: • Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each **Key** used. or • Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each **Key** used.
Key 1~4	Based on your **Key Length** selection, enter the appropriate length hexadecimal or ASCII key.
Advance Note: Click on the **Show Advanced Settings** 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.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 66 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wpa2 (NWA50AX)



The following table describes the labels in this screen.

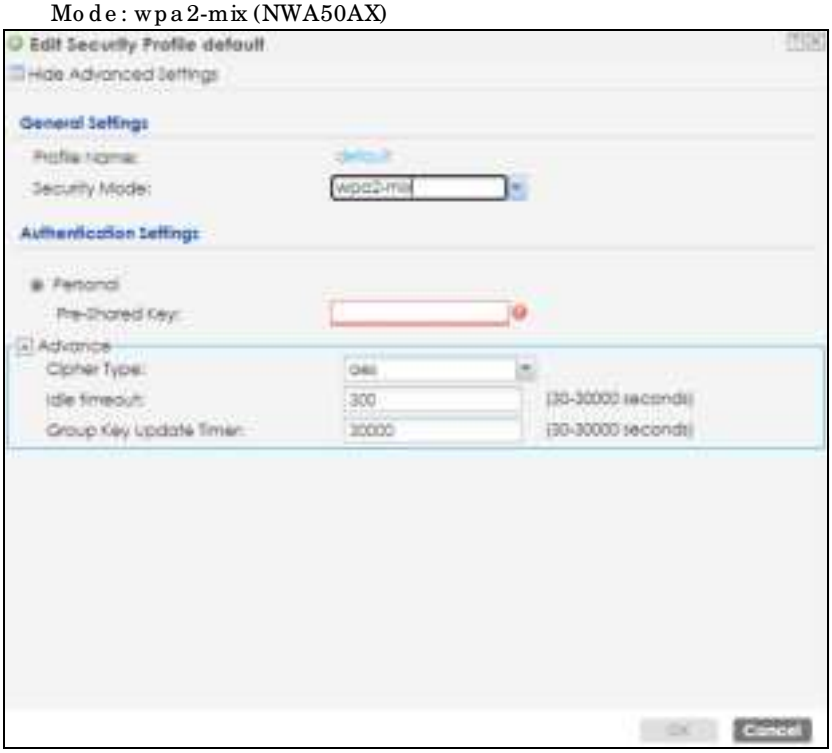
Table 45 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa2

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: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** 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 **Show Advanced Settings** button to show the fields describe below.	

Table 45 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa2 (continued)

LABEL	DESCRIPTION
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
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.
Pre-Authentication	Select **Enable** to allow pre-authentication. Otherwise, select **Disable**.
Management Frame Protection	This field is available only when you select **wpa2** in the **Security Mode** field and set **Cipher Type** to **aes**. 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 checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. Select **Optional** if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select **Required** and wireless clients must support MFP in order to join the Zyxel Device's wireless network.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 67 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wpa2-mix (NWA50AX)



The following table describes the labels in this screen.

Table 46 Configuration > Object > AP Profile > SSID > Security List > AAdd/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: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** 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 **Show Advanced Settings** button to show the fields describe below.	

Table 46 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa2-mix (continued)

LABEL	DESCRIPTION
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
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.
Pre-Authentication	Select **Enable** to allow pre-authentication. Otherwise, select **Disable**.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 68 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wpa3 (NWA50AX)

The following table describes the labels in this screen.

Table 47 Configuration > Object > AP Profile > SSID > Security List > AAdd/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.

Table 47 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa3 (continued)

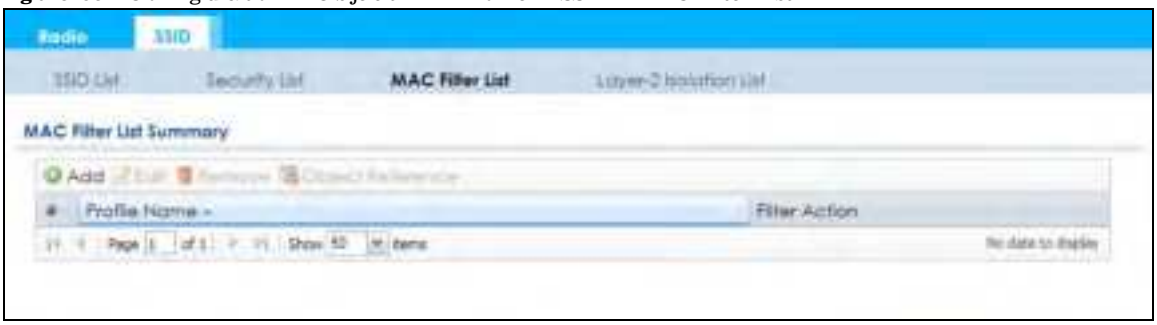
LABEL	DESCRIPTION
Security Mode	Select a security mode from the list: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** 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	Enable this for backwards compatibility. This option is only available if the **Security Mode** is **wpa3** or **enhanced-open**. This creates two virtual APs (VAPs) with a primary (**wpa3** or **enhanced-open**) and fallback (**wpa2** or **none**) security method. If the **Security Mode** is **wpa3**, enabling this will force **Management Frame Protection** to be set to **Optional**. If this is disabled or if the **Security Mode** is **enhanced-open**, **Management Frame Protection** will be set to **Required**.
Advance Note: Click on the **Show Advanced Settings** 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.
Pre-Authentication	Select **Enable** to allow pre-authentication. Otherwise, select **Disable**.
Management Frame Protection	This field is available only when you select **wpa2** in the **Security Mode** field and set **Cipher Type** to **aes**. 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 checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. Select **Optional** if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select **Required** and wireless clients must support MFP in order to join the Zyxel Device's wireless network.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** 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 69 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 48 Configuration > Object > AP Profile > SSID > MAC Filter List

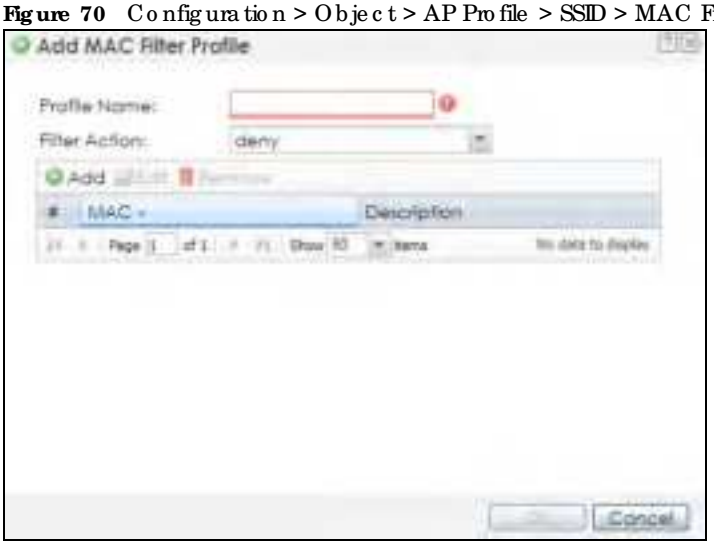
LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for 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 70 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 49 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 **allow** to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select **deny** to block the wireless 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 **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 13
MON Profile

13.1 Overview

This screen allows you to set up monitor mode configurations that allow your Zyxel Device to scan for other wireless devices in the vicinity. Once detected, you can use the **Wireless > MON Mode** screen (Section 10.3 on page 79) to classify them as either rogue or friendly.

Not all Zyxel Devices support monitor mode and rogue APs detection.

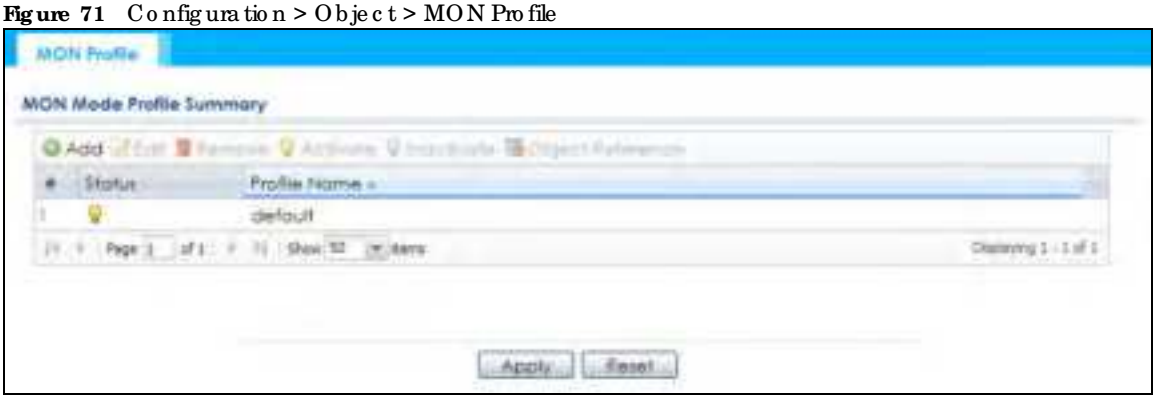
13.1.1 What You Can Do in this Chapter

The **MON Profile** screen (Section 13.2 on page 117) creates preset monitor mode configurations that can be used by the Zyxel Device.

13.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, log into the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 71 Configuration > Object > MON Profile



The following table describes the labels in this screen.

Table 50 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.

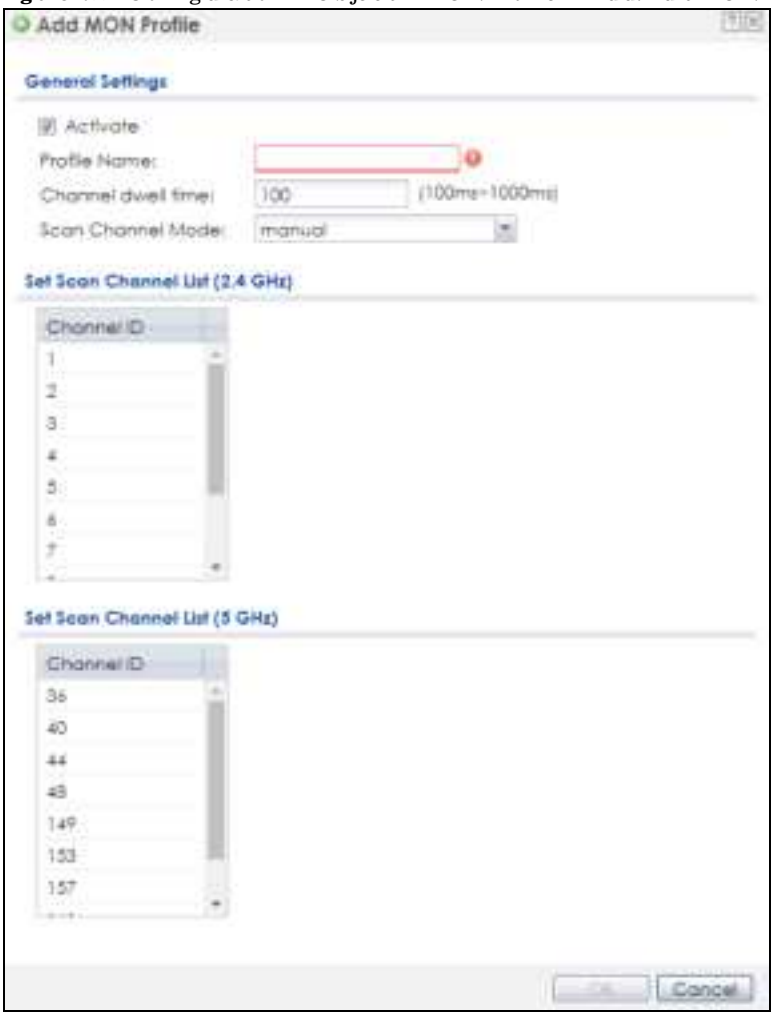
Table 50 Configuration > Object > MON Profile (continued)

LABEL	DESCRIPTION
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This field shows whether or not the entry is activated.
Profile Name	This field indicates the name assigned to the monitor profile.

13.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select and existing monitor mode profile and click the **Edit** button. See Section 1.2.3 on page 14 for more information about MON Mode.

Figure 72 Configuration > Object > MON Profile > Add/Edit MON Profile



The following table describes the labels in this screen.

Table 51 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the Zyxel Device switches to another channel for monitoring.
Scan Channel Mode	Select **auto** to have the Zyxel Device switch to the next sequential channel once the **Channel dwell time** expires. Select **manual** to set specific channels through which to cycle sequentially when the **Channel dwell time** expires. Selecting this options makes the **Scan Channel List** options available.
Set Scan Channel List (2.4 GHz)	Select one or more than one channel to have the Zyxel Device using this profile scan the channel(s) when **Scan Channel Mode** is set to **manual**. These channels are limited to the 2.4 GHz range (802.11 b/g/n/ax).
Set Scan Channel List (5 GHz)	Select one or more than one channel to have the Zyxel Device using this profile scan the channel(s) when **Scan Channel Mode** is set to **manual**. These channels are limited to the 5 GHz range (802.11 a/n/ac/ax). Not all Zyxel Devices support both 2.4 GHz and 5 GHz frequency bands.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 14
WDS Profile

14.1 Overview

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

14.1.1 What You Can Do in this Chapter

The **WDS Profile** screen (Section 14.2 on page 120) creates preset WDS configurations that can be used by the Zyxel Device.

14.2 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 73 Configuration > Object > WDS Profile

The following table describes the labels in this screen.

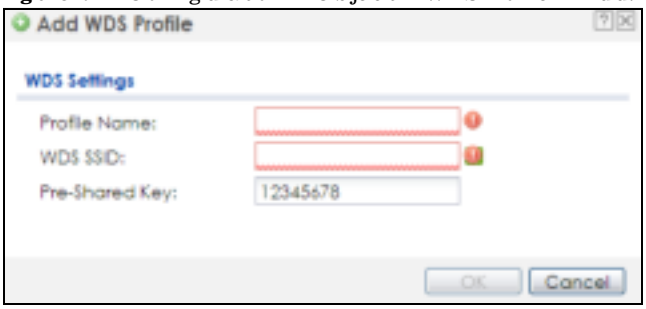
Table 52 Configuration > Object > WDS Profile

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.

14.2.1 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 and existing profile and click the **Edit** button.

Figure 74 Configuration > Object > WDS Profile > Add/Edit WDS Profile



The following table describes the labels in this screen.

Table 53 Configuration > Object > WDS Profile > Add/Edit WDS Profile

LABEL	DESCRIPTION
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 **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 15
Certificates

15.1 Overview

The ZyxelDevice 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.

15.1.1 What You Can Do in this Chapter

- The **My Certificates** screens (Section 15.2 on page 125) generate and export self-signed certificates or certification requests and import the ZyxelDevice's CA-signed certificates.
- The **Trusted Certificates** screens (Section 15.3 on page 132) save CA certificates and trusted remote host certificates to the ZyxelDevice. The ZyxelDevice 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.

15.1.2 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.

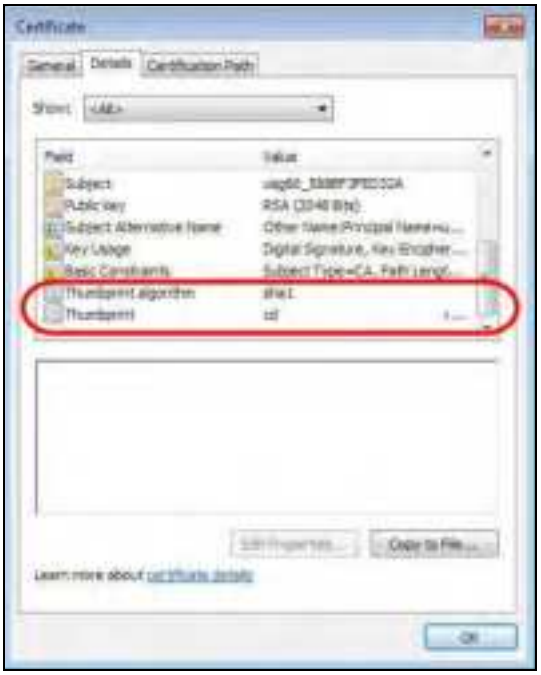
15.1.3 Verifying a Certificate

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.

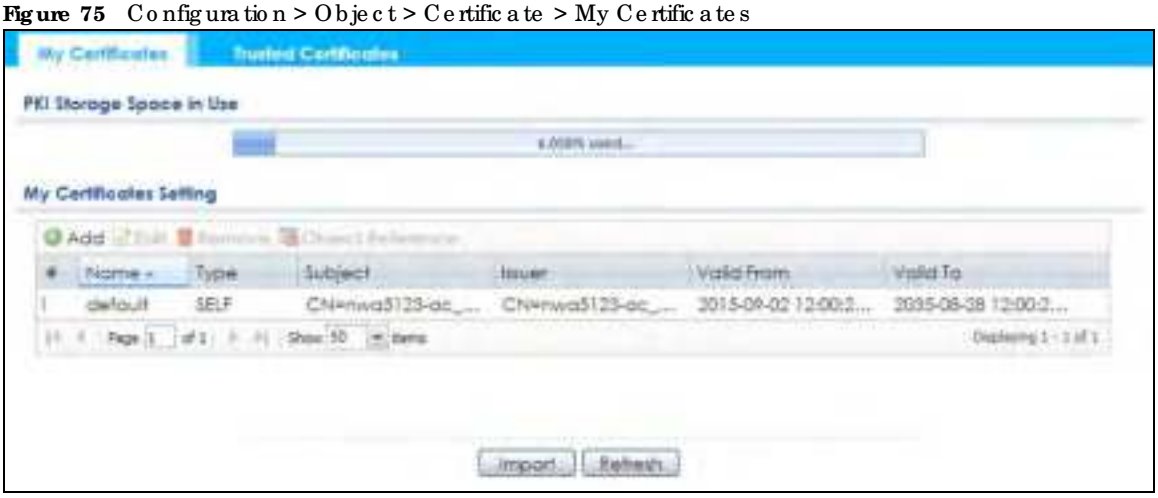


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

15.2 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 75 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 54 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 **Edit** 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 **Remove**. 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 **Object Reference** 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. **REQ** 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 **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** 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.

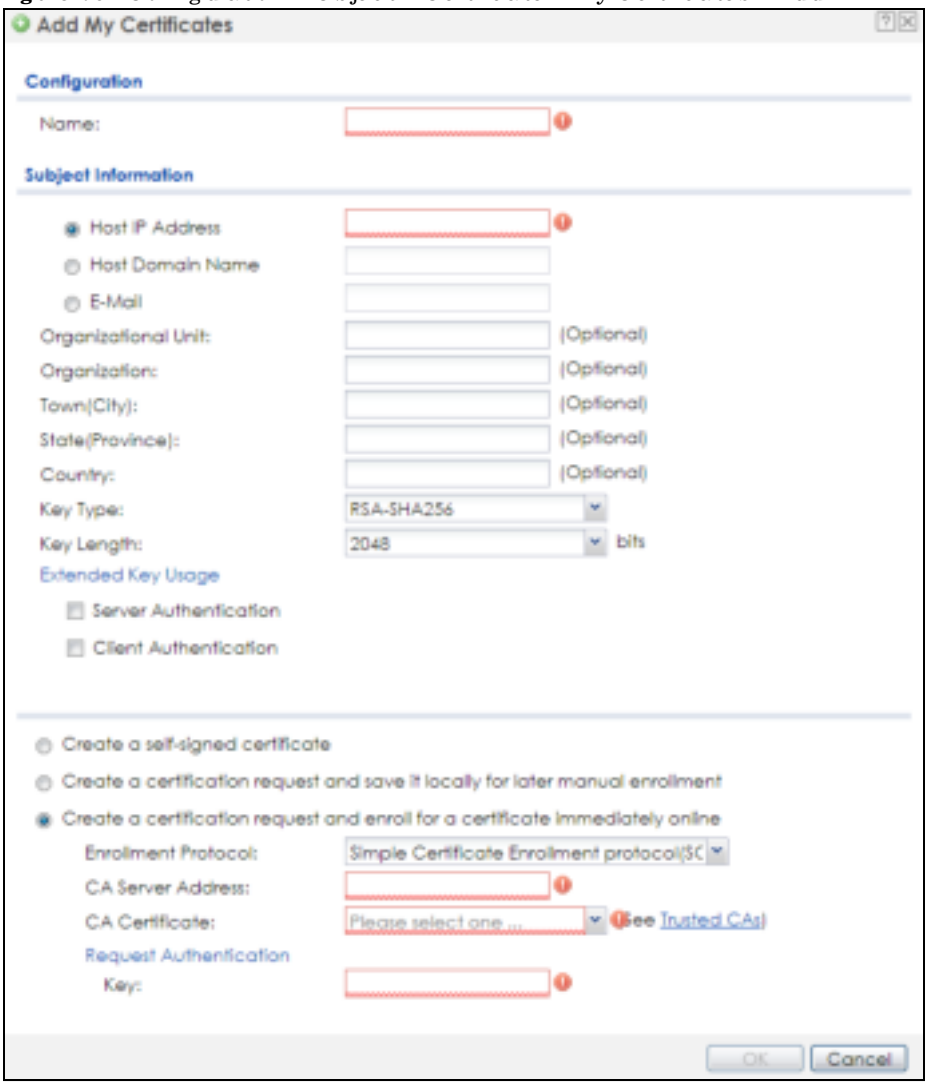
Table 54 Configuration > Object > Certificate > My Certificates (continued)

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 **Subject** 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 **Import** to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click **Refresh** to display the current validity status of the certificates.

15.2.1 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 76 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 55 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	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 **Host IP Address**, **Host Domain Name**, or **E-Mail**. 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. Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
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	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. Select a key type from **RSA-SHA256** and **RSA-SHA512**.
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	Select **Server Authentication** to allow a web server to send clients the certificate to authenticate itself. Select **Client Authentication** to use the certificate's key to authenticate clients to the secure gateway.
	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	Select this to have the Zyxel Device generate and store a request for a certificate. Use the **My Certificate Edit** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Edit** screen and then send it to the certification authority.

Table 55 Configuration > Object > Certificate > My Certificates > Add (continued)

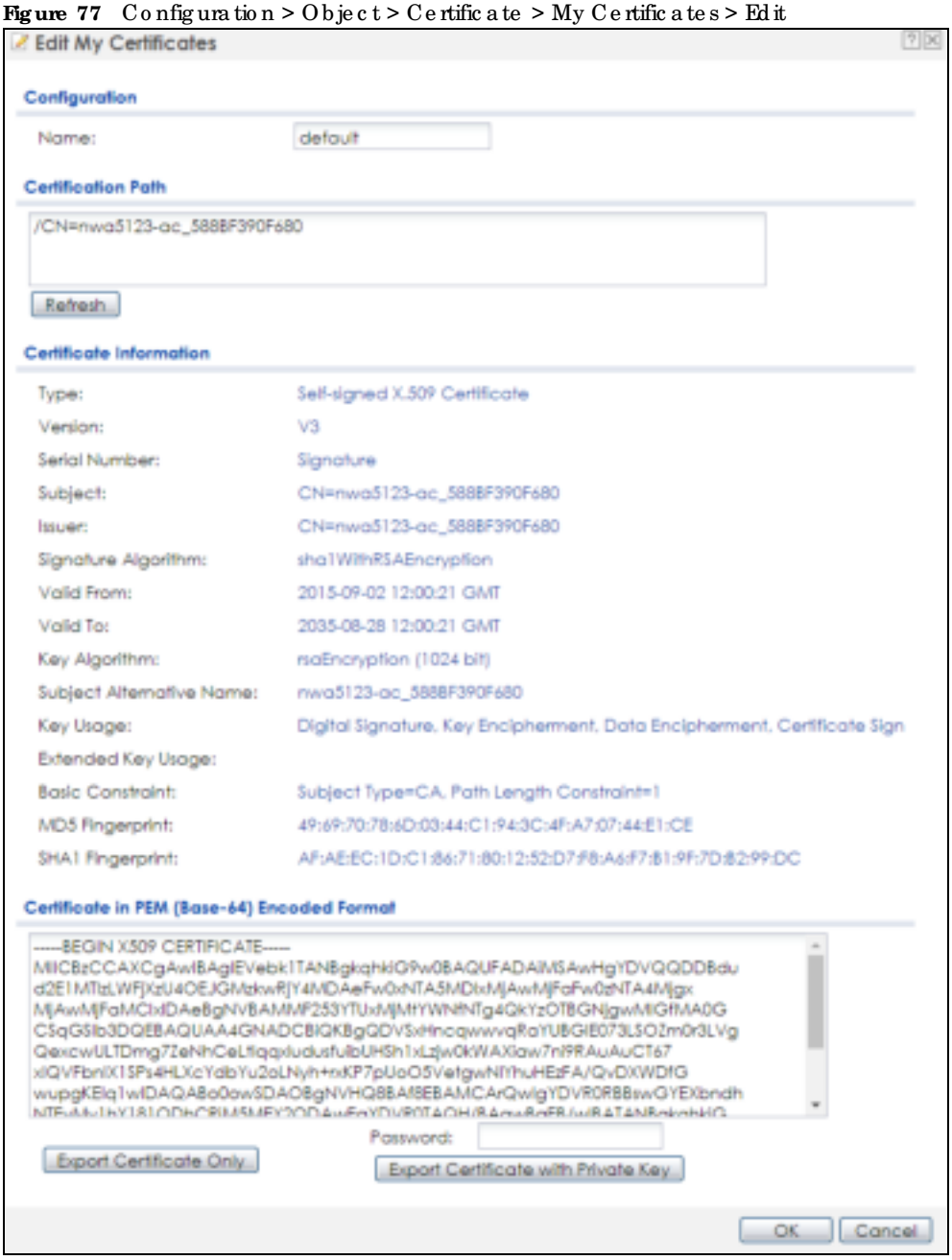
LABEL	DESCRIPTION
Create a certification request and enroll for a certificate immediately online	Select this to have the Zyxel Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server. For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-
CA Certificate	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the Zyxel Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses the CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol. For the reference number, use 0 to 99999999. For the key, use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** 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.

15.2.2 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 77 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 56 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 **Refresh** 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 **Refresh** 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-TX.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 **Subject Name** 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 e-mail 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.
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.

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

LABEL	DESCRIPTION
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	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 a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail 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).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
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 **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

15.2.3 Import Certificates

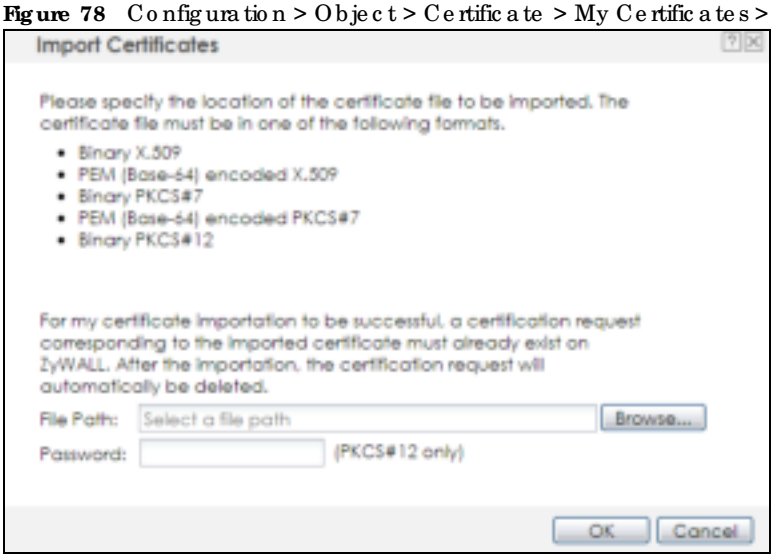
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

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 78 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

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

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

15.3 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 79 Configuration > Object > Certificate > Trusted Certificates

The following table describes the labels in this screen.

Table 58 Configuration > Object > Certificate > Trusted Certificates

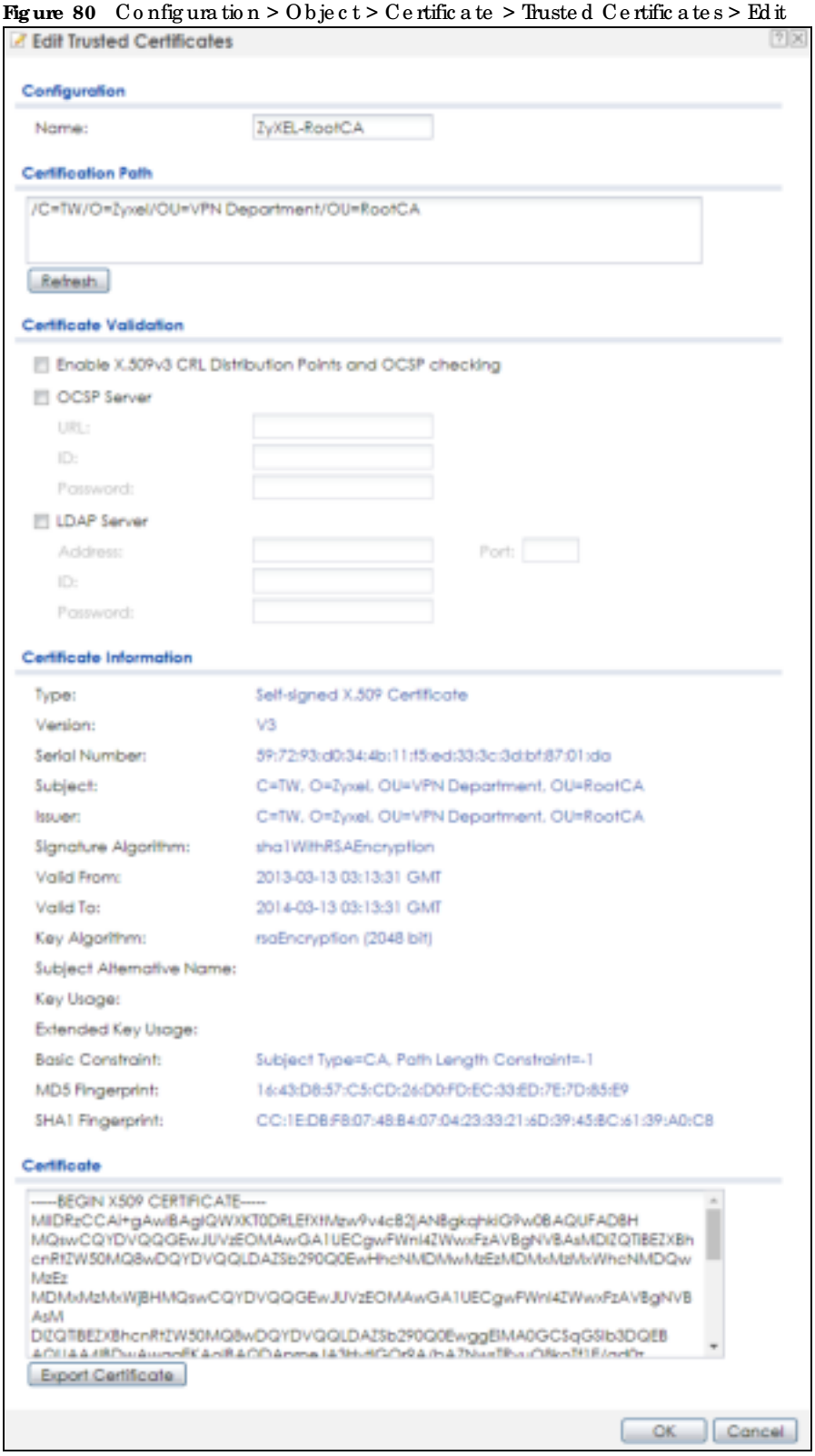
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** 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 **Remove**. 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 **Object Reference** 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 **Subject** 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 **Import** 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.

15.3.1 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

authority.

Figure 80 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 59 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
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 **Refresh** 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 **Refresh** to display the certification path.
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-TX.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 **Subject Name** field.
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).

Table 59 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

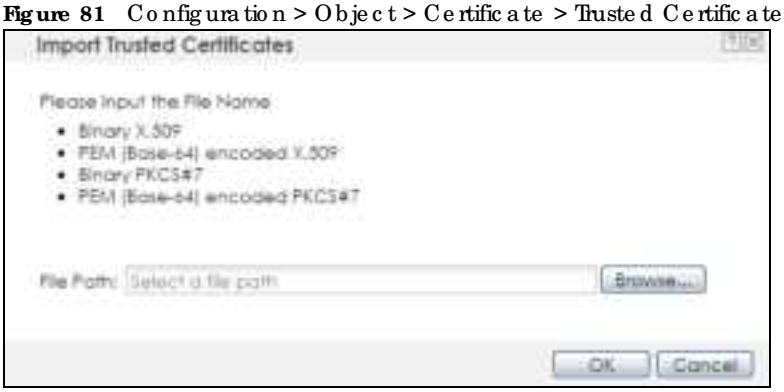
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in 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 e-mail 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 e-mail 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 **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

15.3.2 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 81 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

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

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

15.4 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 16
System

16.1 Overview

Use the system screens to configure general Zyxel Device settings.

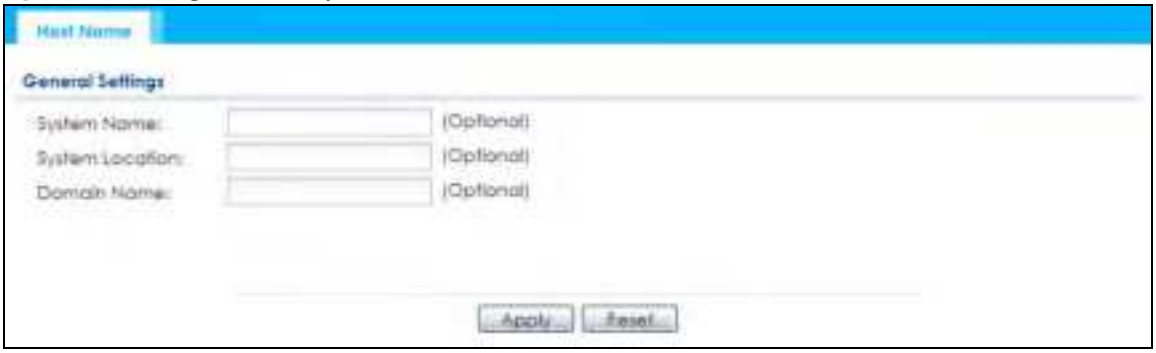
16.1.1 What You Can Do in this Chapter

- The **Host Name** screen (Section 16.2 on page 138) configures a unique name for the Zyxel Device in your network.
- The **Date/Time** screen (Section 16.3 on page 139) configures the date and time for the Zyxel Device.
- The **WWW** screens (Section 16.4 on page 143) configure settings for HTTP or HTTPS access to the Zyxel Device.
- The **SSH** screen (Section 16.5 on page 151) configures SSH (Secure SHell) for securely accessing the Zyxel Device's command line interface.
- The **Telnet** screen (Section 16.6 on page 155) configures Telnet for accessing the Zyxel Device's command line interface.
- The **FTP** screen (Section 16.6 on page 155) specifies FTP server settings. You can upload and download the Zyxel Device's firmware and configuration files using FTP. Please also see Chapter 18 on page 167 for more information about firmware and configuration files.

16.2 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 82 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 61 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.3 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 83 Configuration > System > Date/Time

The following table describes the labels in this screen.

Table 62 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 **Apply**.
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 **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
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 **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
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. • When the Zyxel Device starts up. • When you click **Apply** or **Sync. Now** in this screen. • 24-hour intervals after starting up.

Table 62 Configuration > System > 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 **Time Server Address** 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 **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** 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 **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.3.1 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 63 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.

16.3.2 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 84 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** checkbox 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.

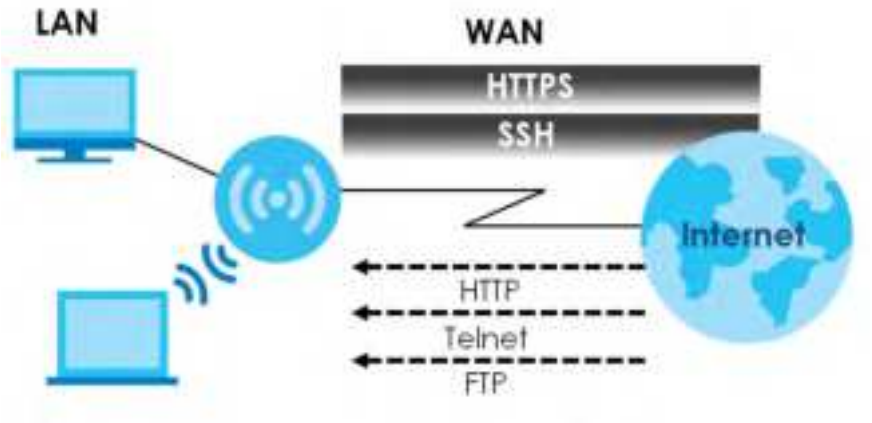
4 Under **Time and Date Setup**, enter a **Time Server Address**.

5 Click **Apply**.

16.4 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, Telnet, and FTP management access are not secure.

Figure 85 Secure and Insecure Service Access From the WAN



16.4.1 Service Access Limitations

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

16.4.2 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.

16.4.3 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 15 on page 122 for more information).

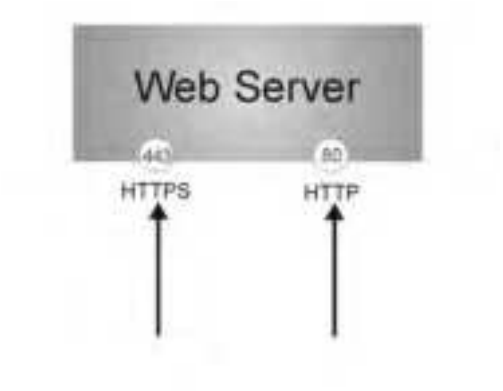
HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), 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 86 HTTP/HTTPS Implementation



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

16.4.4 Configuring WWW Service Control

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

Figure 87 Configuration > System > WWW > Service Control

The following table describes the labels in this screen.

Table 64 Configuration > System > WWW > 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 **Service Control** table to access the ZyxelDevice 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 ZyxelDevice, for example 8443, then you must notify people who need to access the ZyxelDevice Web Configurator to use "https://ZyxelDevice IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyxelDevice by sending the ZyxelDevice 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 ZyxelDevice.
Server Certificate	Select a certificate the HTTPS server (the ZyxelDevice) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** 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 **Service Control** table to access the ZyxelDevice 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 ZyxelDevice.
Apply	Click **Apply** to save your changes back to the ZyxelDevice.
Reset	Click **Reset** to return the screen to its last-saved settings.

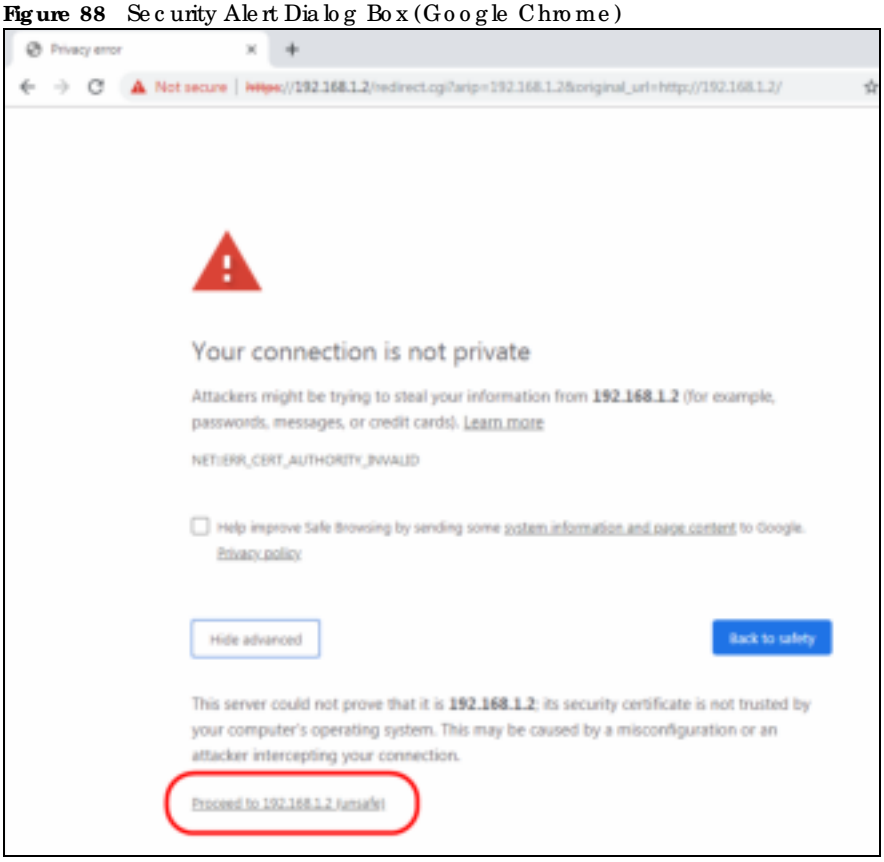
16.4.5 HTTPS Example

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

16.4.5.1 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 88 Security Alert Dialog Box (Google Chrome)



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

16.4.5.2 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 89 Security Certificate 1 (Firefox)

16.4.5.3 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 206 for details.

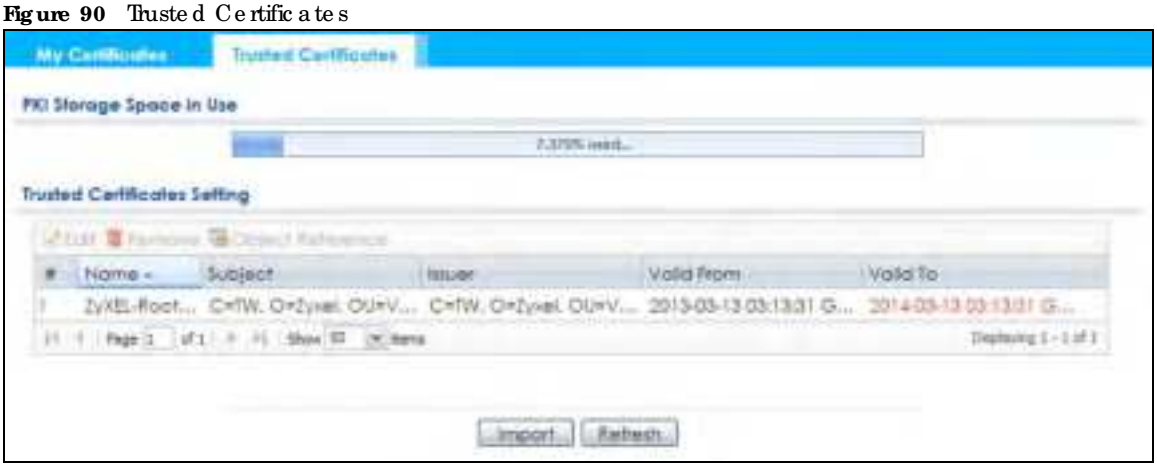
16.4.5.4 Enrolling and Importing SSL Client Certificates

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 90 Trusted Certificates



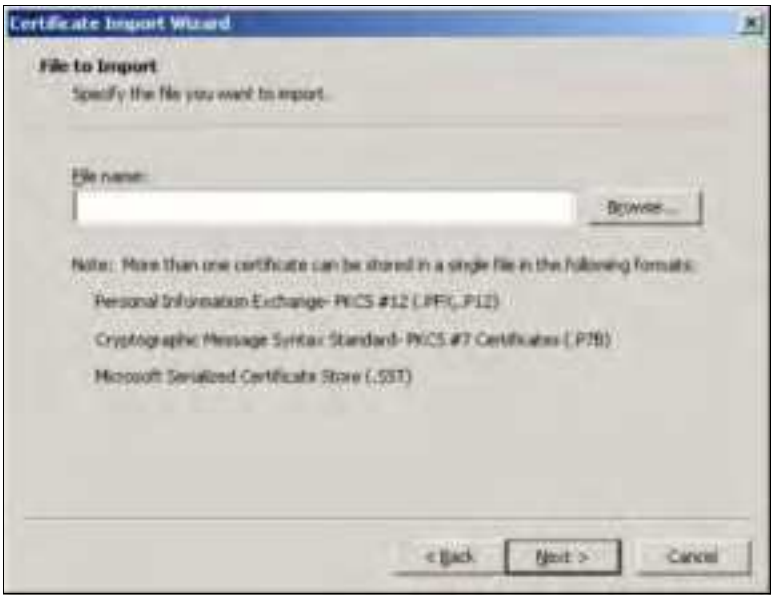
The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

16.4.5.5 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.

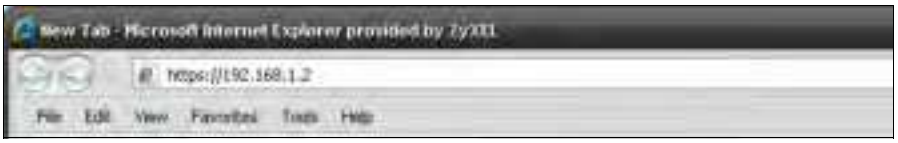
5 Click **Finish** to complete the wizard and begin the import process.

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

16.4.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device via HTTPS:

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



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

3 You next see the Web Configurator login screen.

16.5 SSH

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

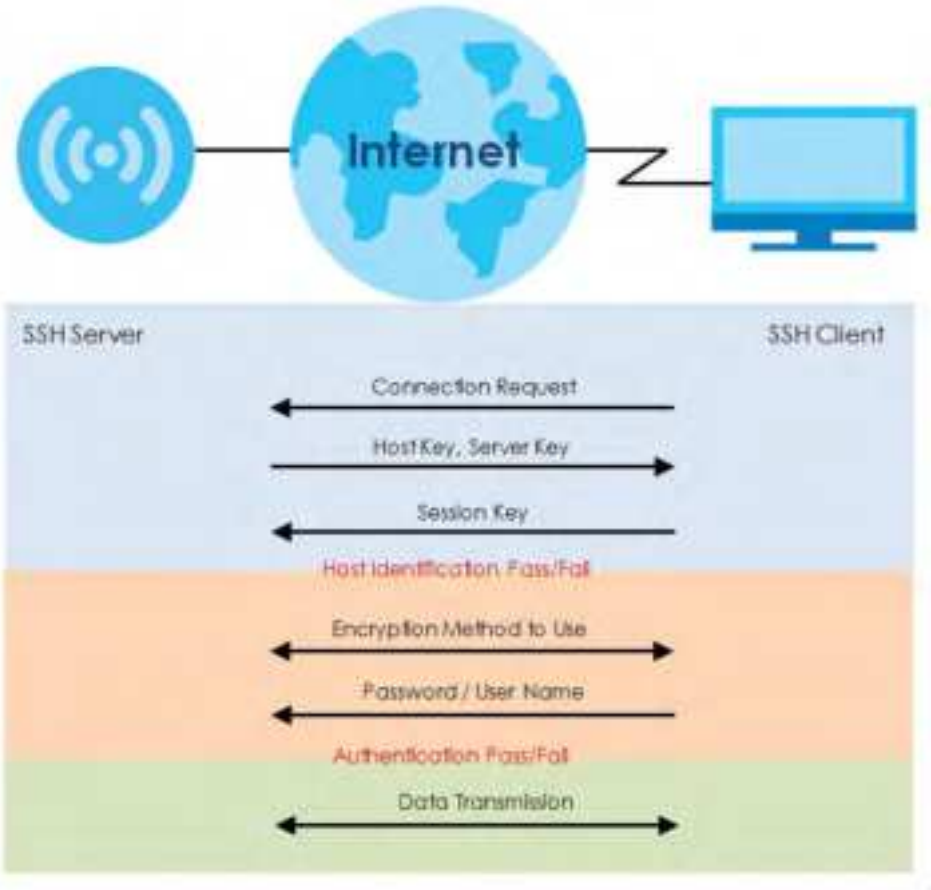
SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer B on the Internet uses SSH to securely connect to the ZyxelDevice (A) for a management session.

Figure 91 SSH Communication Over the WAN Example

16.5.1 How SSH Works

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

Figure 92 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.

16.5.2 SSH Implementation on the Zyxel Device

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

16.5.3 Requirements for Using SSH

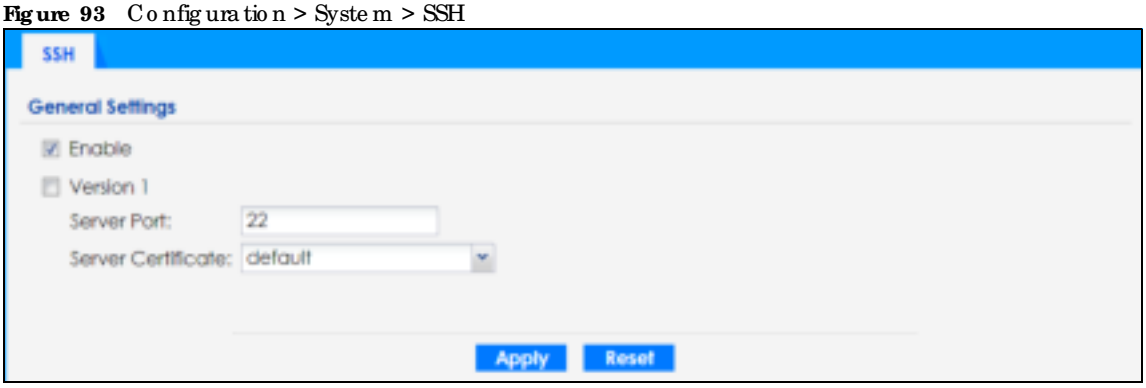
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

16.5.4 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 Telnet and FTP when you configure SSH for secure connections.

Figure 93 Configuration > System > SSH



The following table describes the labels in this screen.

Table 65 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service. Note: The Zyxel Device uses only SSH version 2 protocol.
Version 1	Select the checkbox to have the Zyxel Device use both SSH version 1 and version 2 protocols. If you clear the checkbox, 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 **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.5.5 Examples of Secure Telnet Using SSH

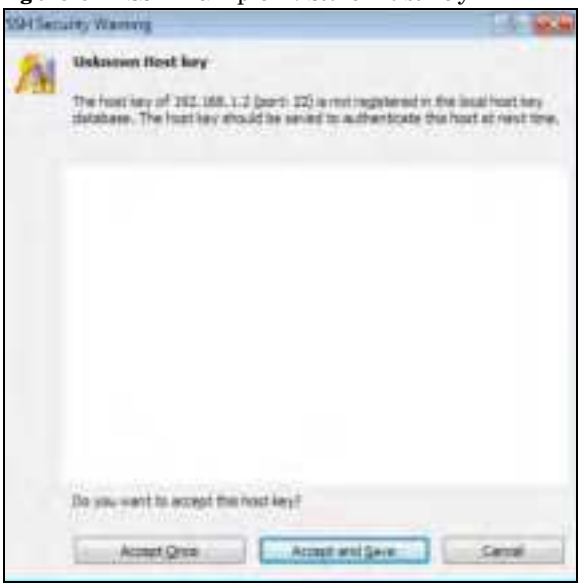
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Zyxel Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

16.5.5.1 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 94 SSH Example 1: Store Host Key



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

16.5.5.2 Example 2: Linux

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

1. Test whether the SSH service is available on the Zyxel Device.

   Enter "`telnet 192.168.1.2 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the Zyxel Device (using the default IP address of 192.168.1.2).

   A message displays indicating the SSH protocol version supported by the Zyxel Device.

Figure 95 SSH Example 2: Test

```
$ telnet 192.168.1.2 22
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "ssh -2 192.168.1.2". 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 96 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:
```

3 The CLI screen displays next.

16.6 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 18 on page 167 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 97 Configuration > System > FTP

The following table describes the labels in this screen.

Table 66 Configuration > System > 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 **Service Control** 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 **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 17
Log and Report

17.1 Overview

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

17.1.1 What You Can Do In this Chapter

- The **Log Setting** screens (Section 17.2 on page 157) specify which logs are e-mailed, where they are e-mailed, and how often they are e-mailed.

17.2 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) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The Zyxel Device provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** screen, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Setting** tab also controls what information is saved in each log. For the system log, you can also specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

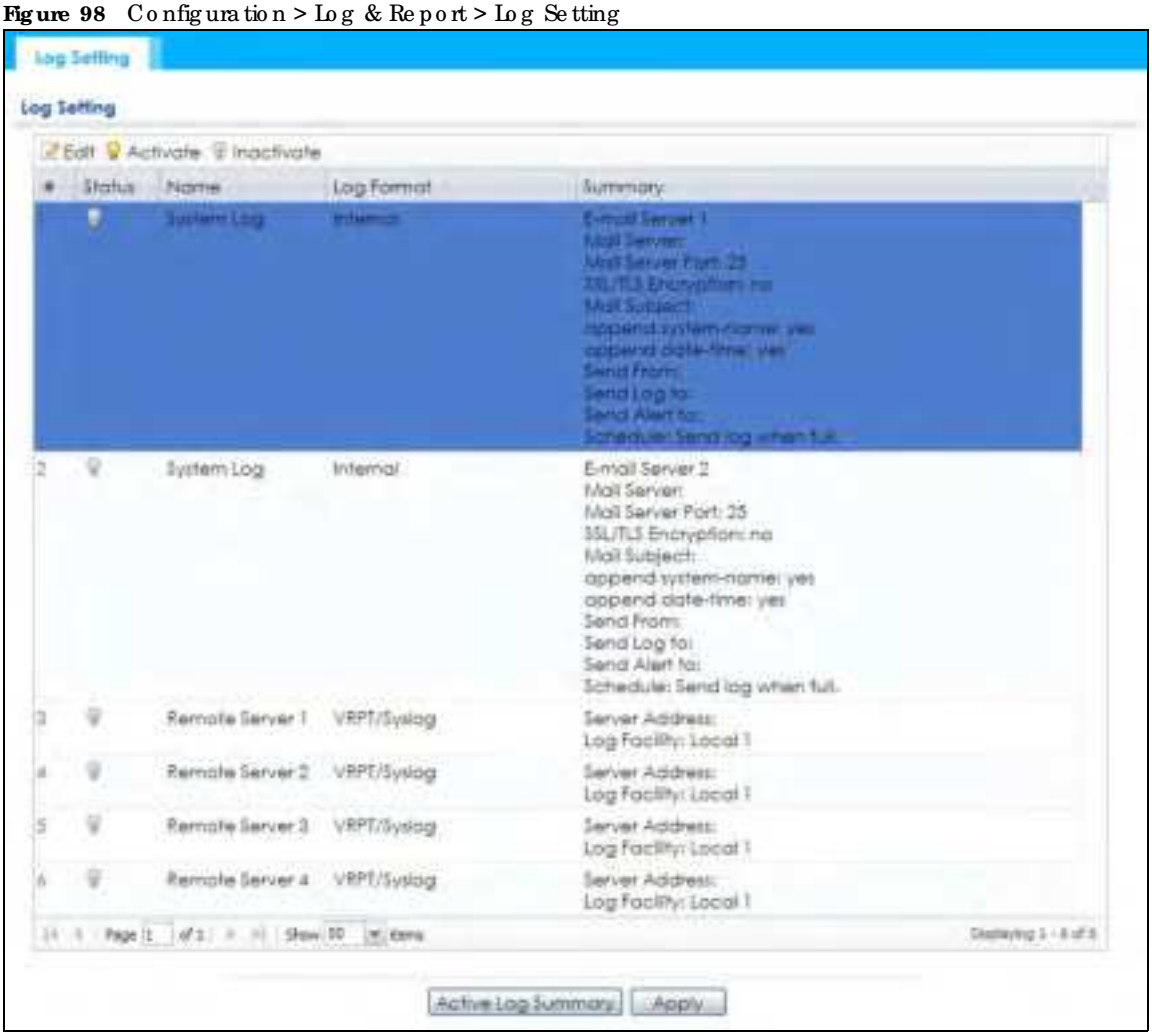
For alerts, the **Log Setting** screen controls which events generate alerts and where alerts are e-mailed.

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, e-mail addresses, 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.

17.2.1 Log Setting Screen

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

Figure 98 Configuration > Log & Report > Log Setting



The following table describes the labels in this screen.

Table 67 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	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. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.

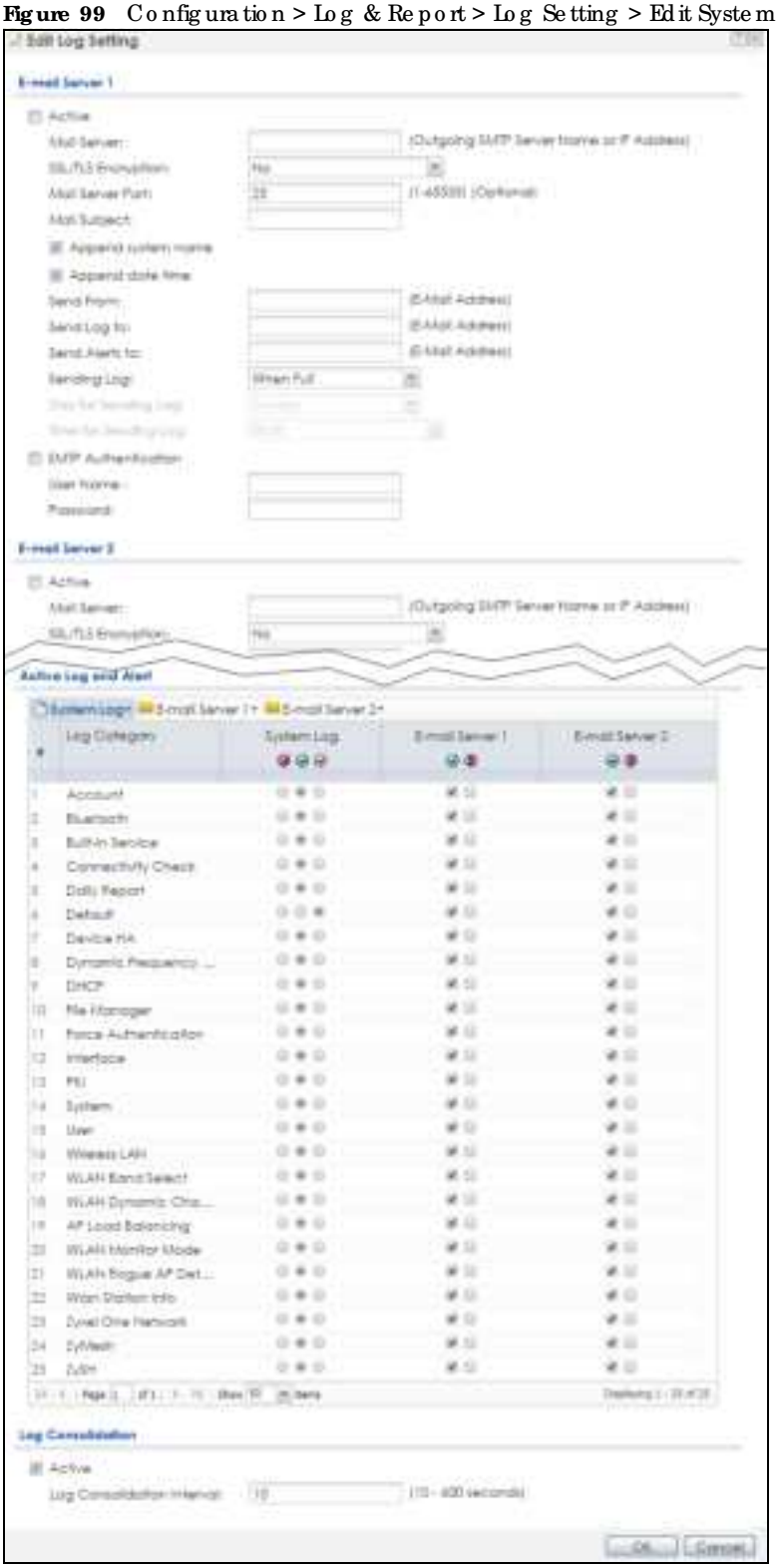
Table 67 Configuration > Log & Report > Log Setting (continued)

LABEL	DESCRIPTION
Active Log Summary	Click this button to open the **Active Log Summary** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

17.2.2 Edit System Log Settings

This screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Select a system log entry in the **Log Setting** screen and click the **Edit** icon.

Figure 99 Configuration > Log & Report > Log Setting > Edit System Log Setting



The following table describes the labels in this screen.

Table 68 Configuration > Log & Report > Log Setting > Edit System Log Setting

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
SSL/TLS Encryption	Select **SSL/TLS** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **No** to not encrypt the communications.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the Zyxel Device's system name to the subject. Select **Append date time** to add the Zyxel Device's system date and time to the subject.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the Zyxel Device will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not e-mail debugging information, even if this setting is selected.

Table 68 Configuration > Log & Report > Log Setting > Edit System Log Setting (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	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 **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
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.

17.2.3 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 100 Configuration > Log & Report > Log Setting > Edit Remote Server

The following table describes the labels in this screen.

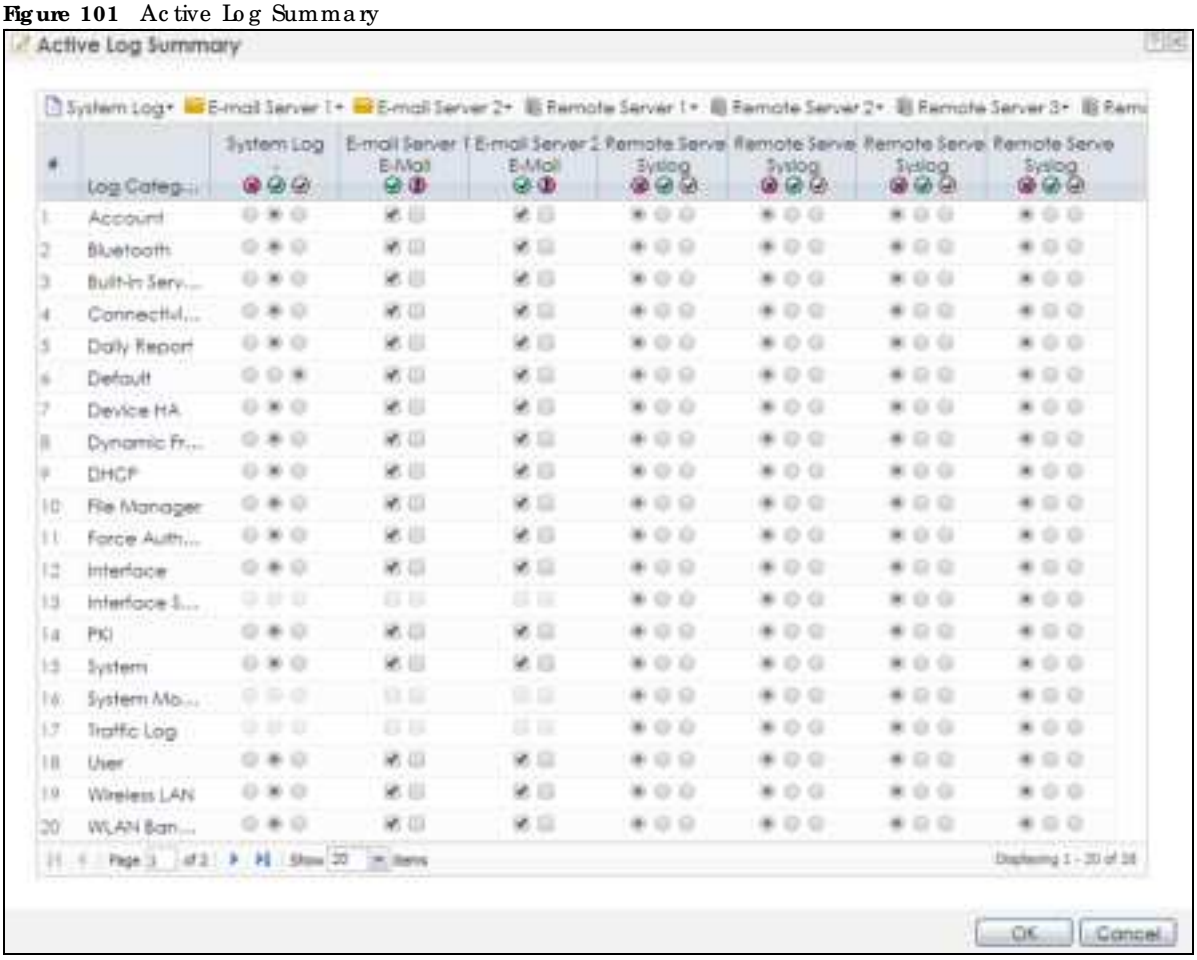
Table 69 Configuration > Log & Report > Log Setting > Edit Remote Server

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 **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - 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	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	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 **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
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.

17.2.4 Active Log Summary

This screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Setting** screen, and click the **Active Log Summary** button.

Figure 101 Active Log Summary



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 70 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	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the Zyxel Device will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not e-mail debugging information, even if this setting is selected.

Table 70 Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	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 **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
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 18
File Manager

18.1 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.

18.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 18.2 on page 168) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen (Section 18.3 on page 173) checks your current firmware version and uploads firmware to the Zyxel Device.
- The **Shell Script** screen (Section 18.4 on page 175) stores, names, downloads, uploads and runs shell script files.

18.1.2 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 102 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 71 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the aforementioned example as a shell script because the first command is run in **Privilege** 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 **Configuration** 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.

18.2 Configuration File

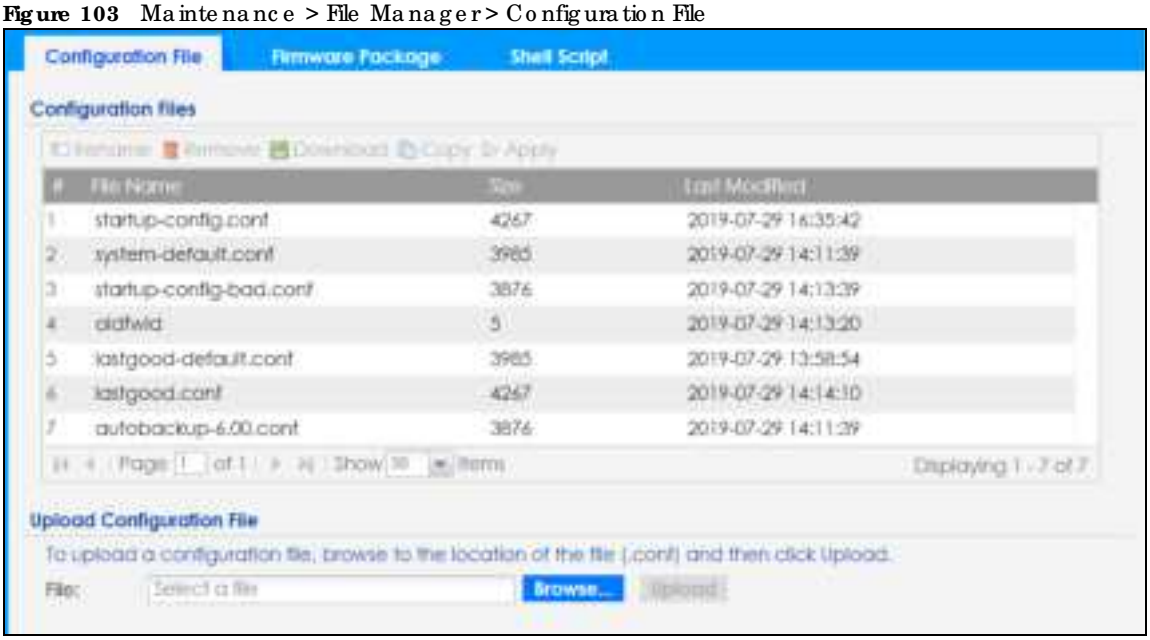
Click **Maintenance > File Manager > Configuration File** to open this screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel 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 backup 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 103 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 72 Maintenance > File Manager > Configuration File

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

Table 72 Maintenance > File Manager > Configuration File (continued)

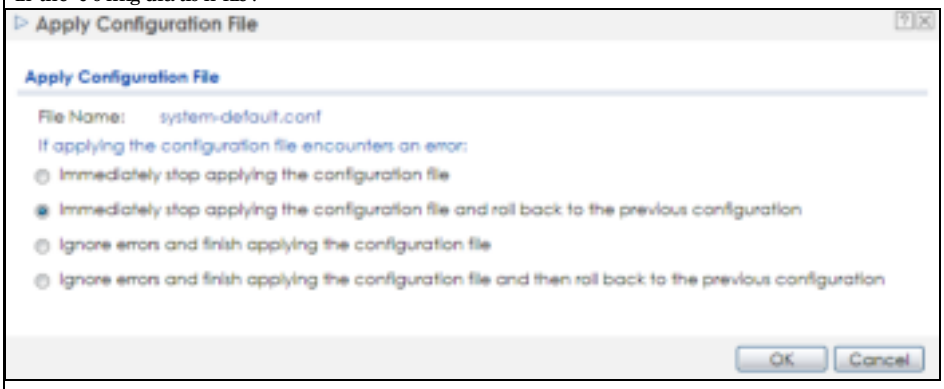
LABEL	DESCRIPTION
Apply	Use this button to have the Zyxel Device use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file.  **Immediately stop applying the configuration file** - 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. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - 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. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - 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. Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen.
#	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.
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the Zyxel Device's default settings. Select this file and click **Apply** to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** 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 **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** 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 lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.

Table 72 Maintenance > File Manager > 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 **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** 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 fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

18.2.1 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 example 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.

18.3 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 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 104 Maintenance > File Manager > Firmware Package

The following table describes the labels in this screen.

Table 73 Maintenance > File Manager > Firmware Package

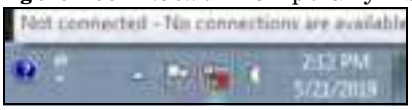
LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the Zyxel Device.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** 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 105 Network Temporarily Disconnected



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

18.3.1 Example of Firmware Upload Using FIP

This procedure requires the Zyxel Device's firmware. Download the firmware package from 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 FIP 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
```

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

18.4 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" file name 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 106 Maintenance > File Manager > Shell Script

Each field is described in the following table.

Table 74 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click **Apply** 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.
#	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 Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.

Table 74 Maintenance > File Manager > Shell Script (continued)

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

CHAPTER 19
Diagnostics

19.1 Overview

Use the diagnostics screen for troubleshooting.

19.1.1 What You Can Do in this Chapter

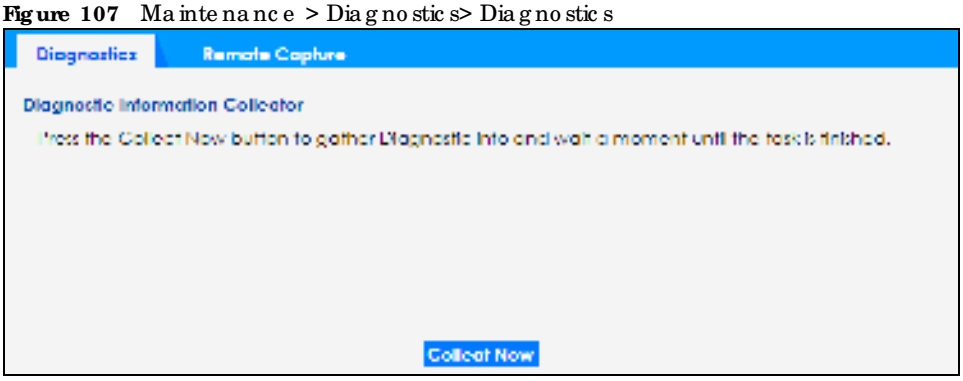
The **Diagnostics** screen (Section 19.2 on page 178) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.

19.2 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.

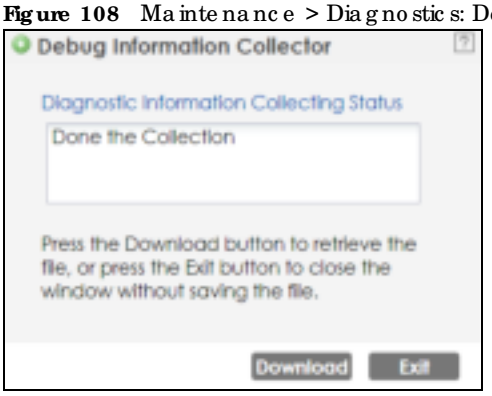
Click **Maintenance > Diagnostics> Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 107 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 108 Maintenance > Diagnostics: Debug Information Collector

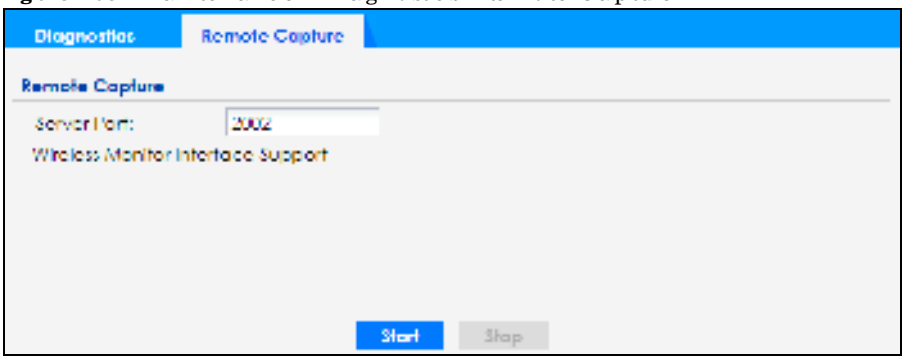


19.3 Remote Capture

Use this screen to capture network traffic going through the Zyxel Device connected to the Zyxel gateway or ZyWALL, and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark.

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

Figure 109 Maintenance > Diagnostics > Remote Capture



The following table describes the labels in this screen.

Table 75 Maintenance > Diagnostics > 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 20
LEDs

20.1 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 1.4 on page 18).

20.1.1 What You Can Do in this Chapter

- The **Suppression** screen (Section 20.2 on page 180) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The **Locator** screen (Section 20.3 on page 181) allows users to see the actual location of the Zyxel Device between several devices in the network.

20.2 Suppression Screen

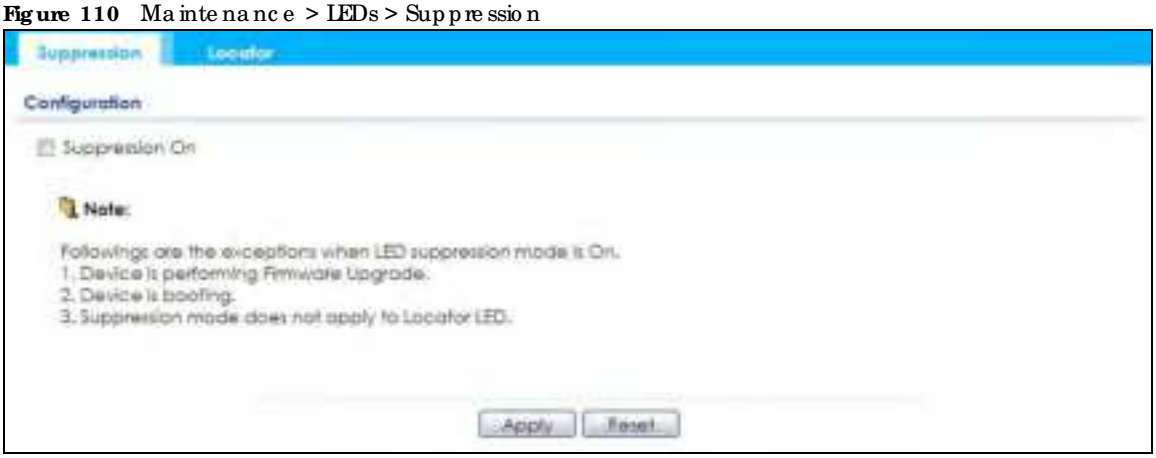
The LED Suppression feature allows you to control how the LEDs of your Zyxel Device behave after it's ready. The default LED suppression setting of your AP is different depending on your Zyxel Device model.

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 28) 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 110 Maintenance > LEDs > Suppression



The following table describes fields in the above screen.

Table 76 Maintenance > LED > Suppression

LABEL	DESCRIPTION
Suppression On	If the **Suppression On** 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.3 Locator Screen

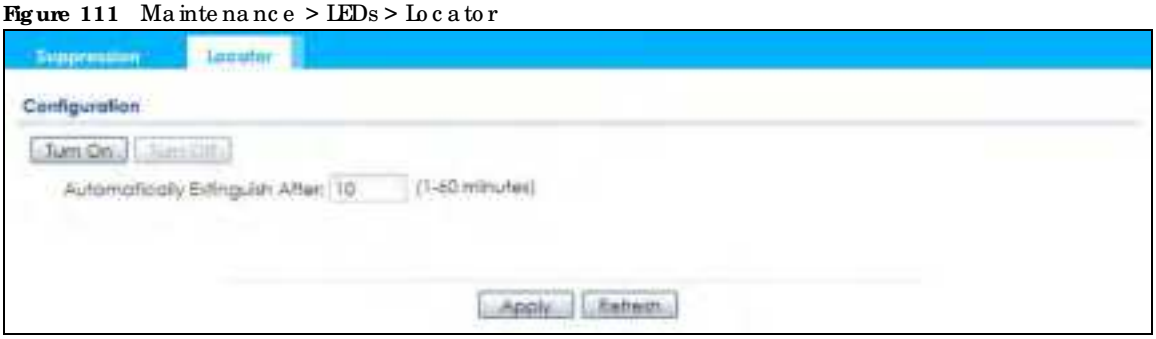
The Locator feature identifies the location of your Zyxel Device among several devices in the network. You can run this feature and set a timer in this screen.

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 111 Maintenance > LEDs > Locator



The following table describes fields in the above screen.

Table 77 Maintenance > LED > Locator

LABEL	DESCRIPTION
Turn On Turn Off	Click **Turn On** 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 **Turn Off** 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 **Apply** to save changes in this screen.
Refresh	Click **Refresh** to update the information in this screen.

CHAPTER 21
Reboot

21.1 Overview

Use this screen to restart the Zyxel Device.

21.1.1 What You Need To Know

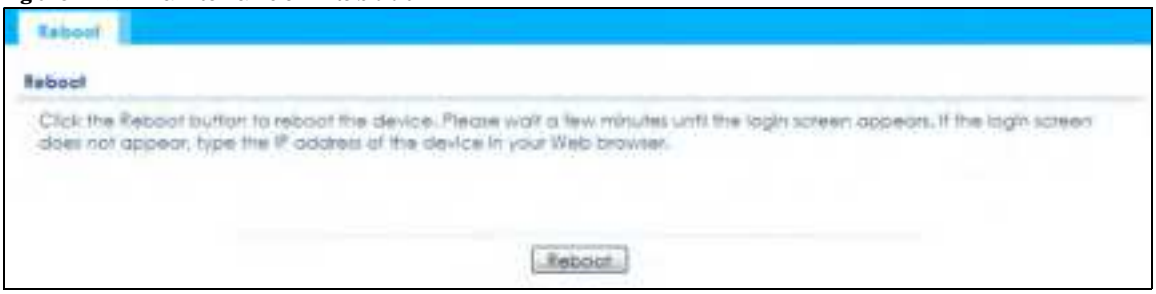
If you applied changes in the Web Configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

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

21.2 Reboot

This screen allows remote users can restart the Zyxel Device. To access this screen, click **Maintenance** > **Reboot**.

Figure 112 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 22
Shutdown

22.1 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.

22.1.1 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.

22.2 Shutdown

To access this screen, click **Maintenance** > **Shutdown**.

Figure 113 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.

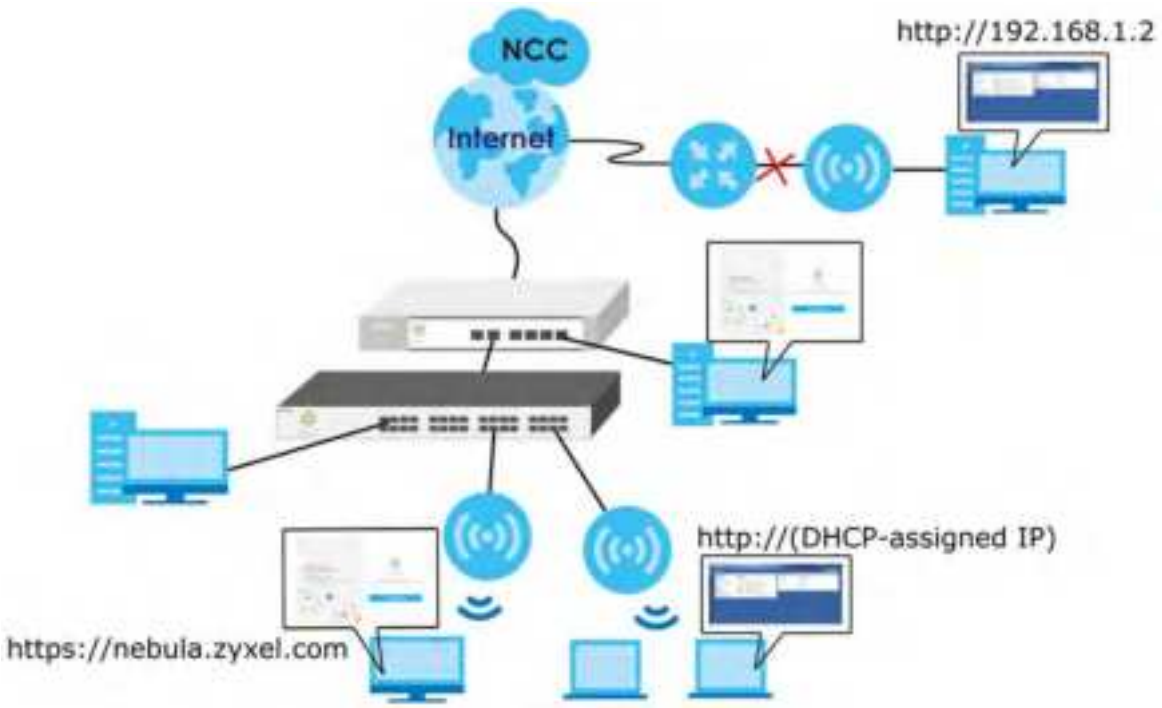
PART II
Local Configuration in Cloud Mode

CHAPTER 23
Cloud Mode

23.1 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 (see Chapter 4 on page 30). 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 114 Cloud Mode Application



23.2 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**
- **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.

23.3 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 115 Dashboard

The following table describes the labels in this screen.

Table 78 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 **Not activated** 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 **Not activated** if the wireless LAN is disabled.
Ethernet	This field displays whether the Zyxel Device's Ethernet port is connected and the IP address of the gateway to which the Zyxel Device is connected.
Internet	This field displays whether the Zyxel Device is connecting to the Internet.
Nebula Connectivity Status	This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC).

Table 78 Dashboard (continued)

LABEL	DESCRIPTION
Nebula Control Center Activation Status	This field displays whether the Zyxel Device has been registered and can be managed by the NCC.
Use Proxy to Access NCC	This displays whether the NAP uses a proxy server to access the NCC (Nebula Control Center).

If the Zyxel Device cannot connect to the Internet or to NCC, an error message is shown on this screen, as in the following.

CHAPTER 24
Network

24.1 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 69 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.

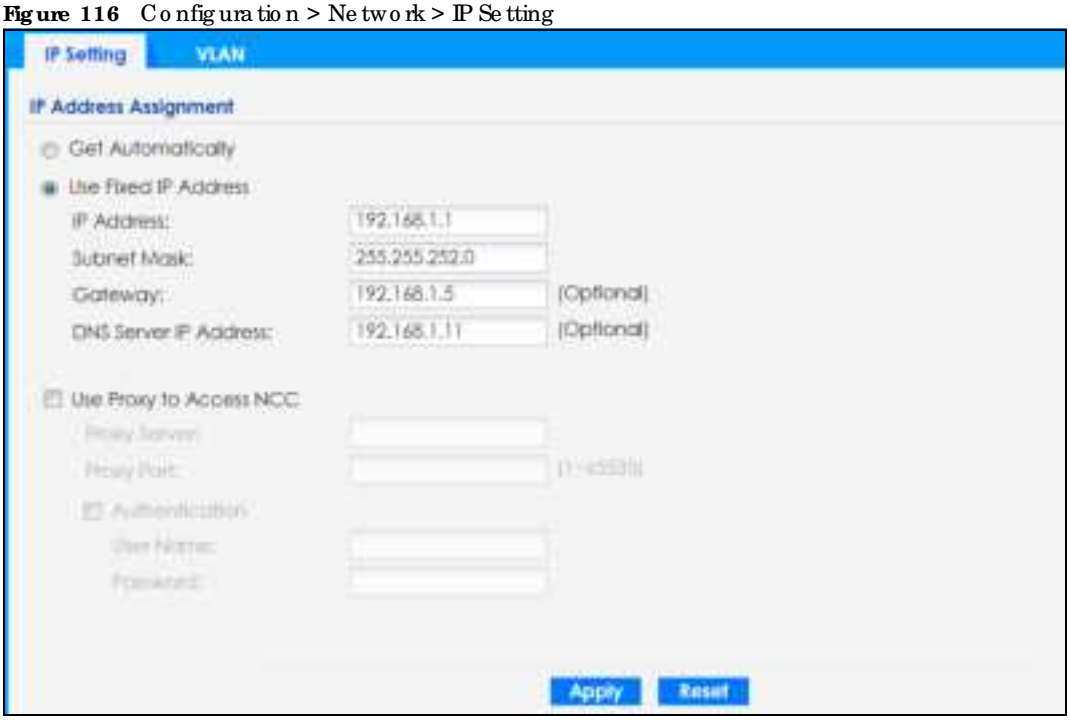
24.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 24.2 on page 189) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 24.3 on page 191) configures the Zyxel Device's VLAN settings.

24.2 IP Setting

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

Figure 116 Configuration > Network > IP Setting



Each field is described in the following table.

Table 79 Configuration > Network > IP Setting

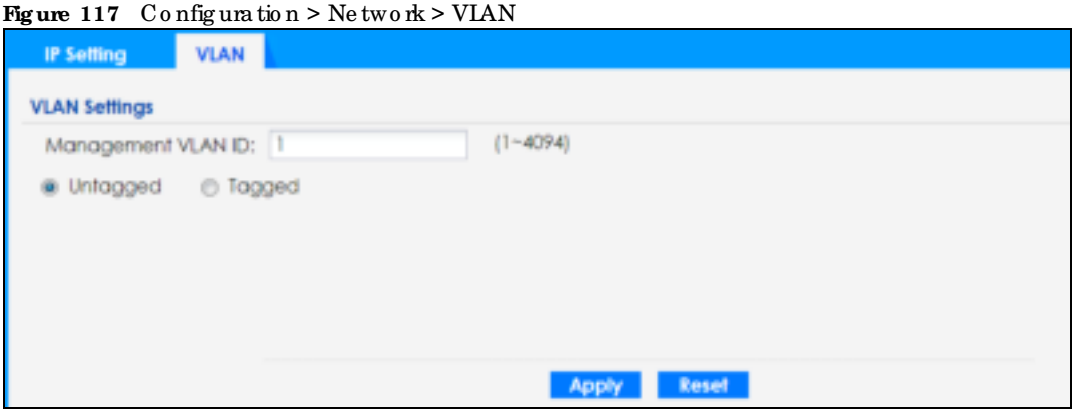
LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
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.
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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

24.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings. See Section 9.3 on page 71 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 117 Configuration > Network > VLAN



Each field is described in the following table.

Table 80 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 **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 25
Maintenance

25.1 Overview

When the Zyxel Device is set to work in cloud mode, the **Maintenance** screens let you mange shell script files on the Zyxel Device, generate a diagnostic file, or view log messages.

See Chapter 18 on page 167 for information about shell scripts.

25.1.1 What You Can Do in this Chapter

- The **Shell Script** screen (Section 25.2 on page 192) stores, names, downloads, and uploads shell script files.
- The **Diagnostics** screen (Section 25.3 on page 193) 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 25.4 on page 194) displays the Zyxel Device's current log messages when it is disconnected from the NCC.

25.2 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 118 Maintenance > Shell Script

Each field is described in the following table.

Table 81 Maintenance > Shell Script

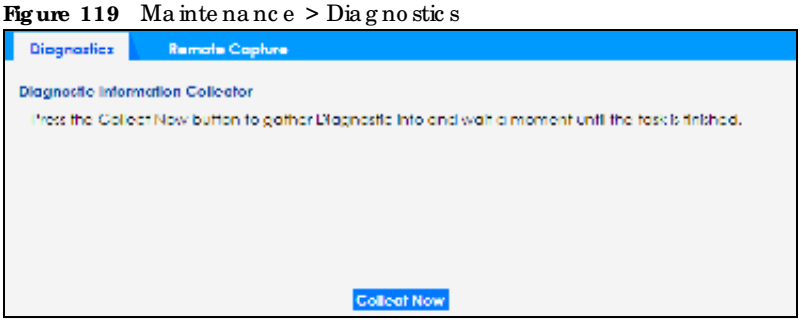
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
#	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 **Browse...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

25.3 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.

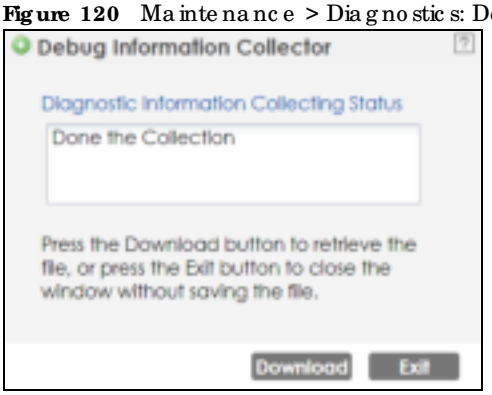
Click **Maintenance > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 119 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 120 Maintenance > Diagnostics: Debug Information Collector



25.4 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 121 Maintenance > Log > View Log

The following table describes the labels in this screen.

Table 82 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 **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
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: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
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 **Message**, **Source**, **Destination** and **Note** 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 82 Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
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 **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** 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 26
Troubleshooting

26.1 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

26.2 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 28.
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.

26.3 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 26.6 on page 205.

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 28.

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 26.6 on page 205.

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 Telnet. 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 26.6 on page 205.

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 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.

4 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 26.6 on page 205.

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 73).
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 71). 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 1.4 on page 18), 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.

26.4 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 28). See the Quick Start Guide and Section 26.2 on page 198.
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 wireless settings on the wireless 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 28. 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.

26.5 WiFi Network

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 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.

Wireless clients are not being load balanced among my Zyxel Devices.

- Make sure that all the Zyxel Devices used by the wireless clients in question share the same SSID, security, and radio settings.
- Make sure that all the Zyxel Devices are in the same broadcast domain.
- Make sure that the wireless clients are in range of the other Zyxel Devices; if they are only in range of a single Zyxel Device, then load balancing may not be as effective.

In the **Monitor > Wireless > AP Information > Radio List** screen, there is no load balancing indicator associated with any Zyxel Devices assigned to the load balancing task.

- Check that the AP profile which contains the load balancing settings is correctly assigned to the Zyxel Devices in question.

- The load balancing task may have been terminated because further load balancing on the Zyxel Devices in question is no longer required.

26.6 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.

26.7 Getting More Troubleshooting Help

Search for support information for your model at 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.

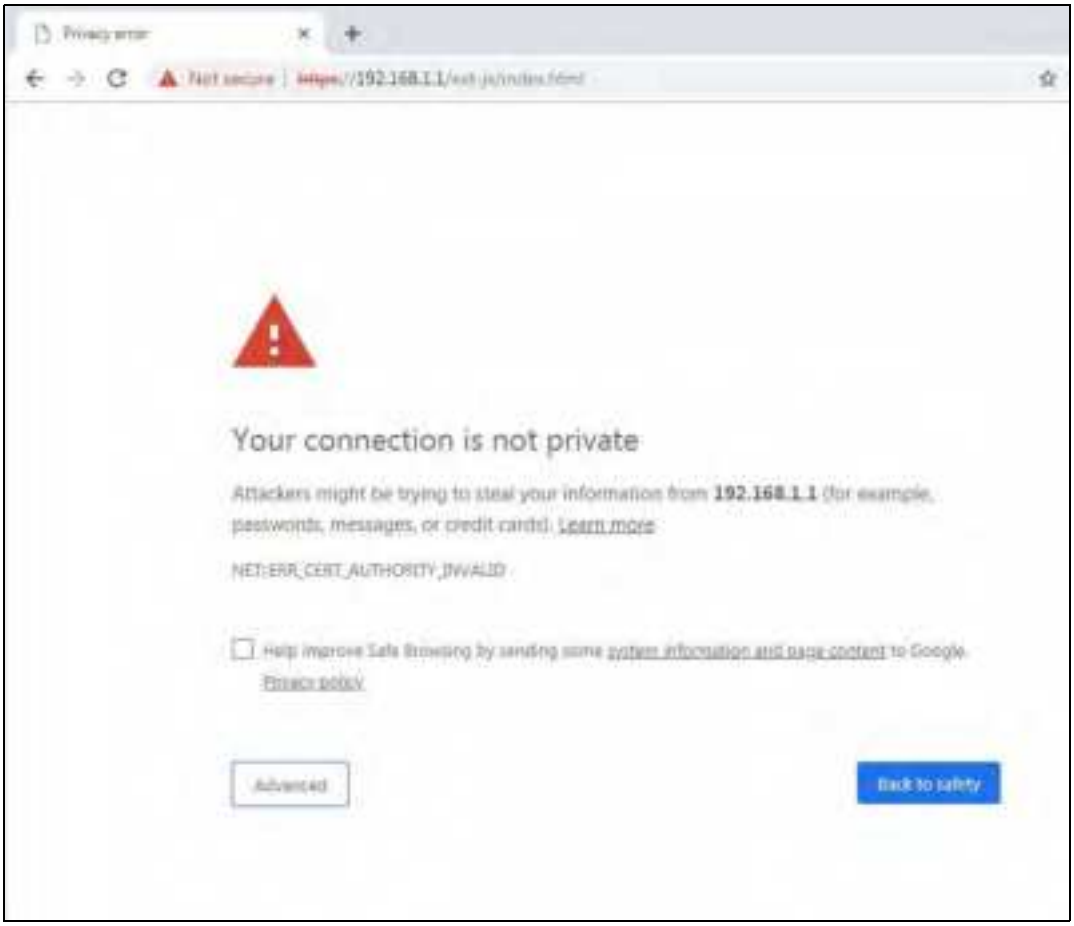
Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon () somewhere in the main browser window (not all browsers show the padlock in the same location).

Google Chrome

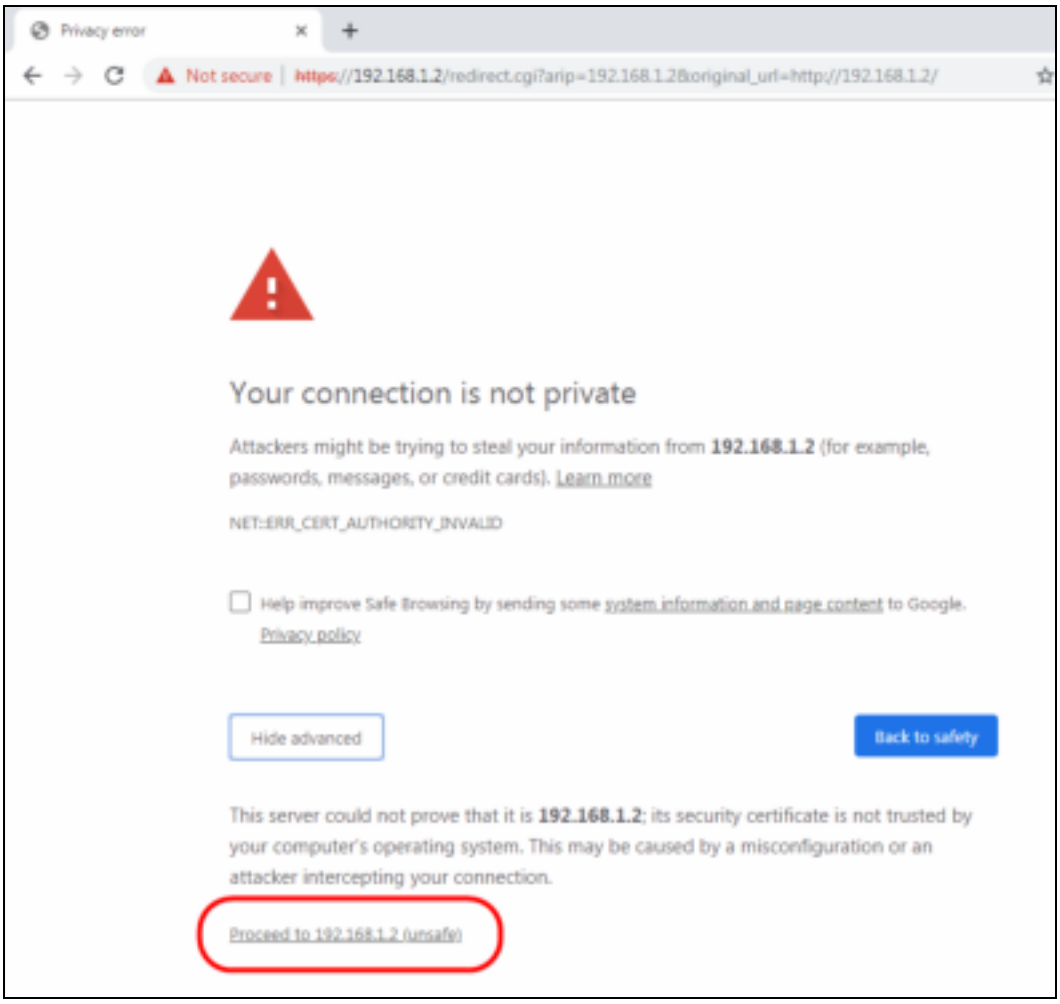
The following example uses Google Chrome on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

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.

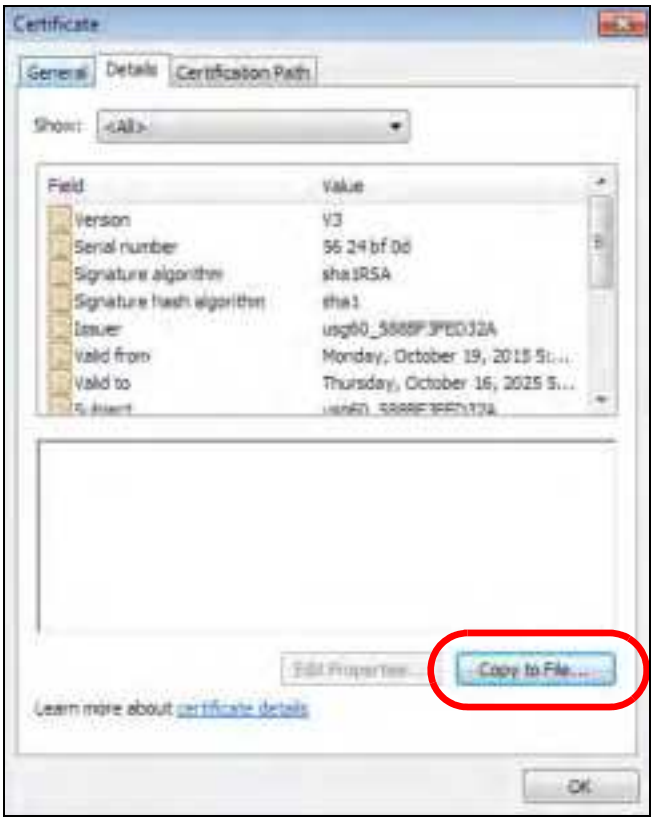


2 Click **Advanced > Proceed to *x.x.x.x* (unsafe)**.



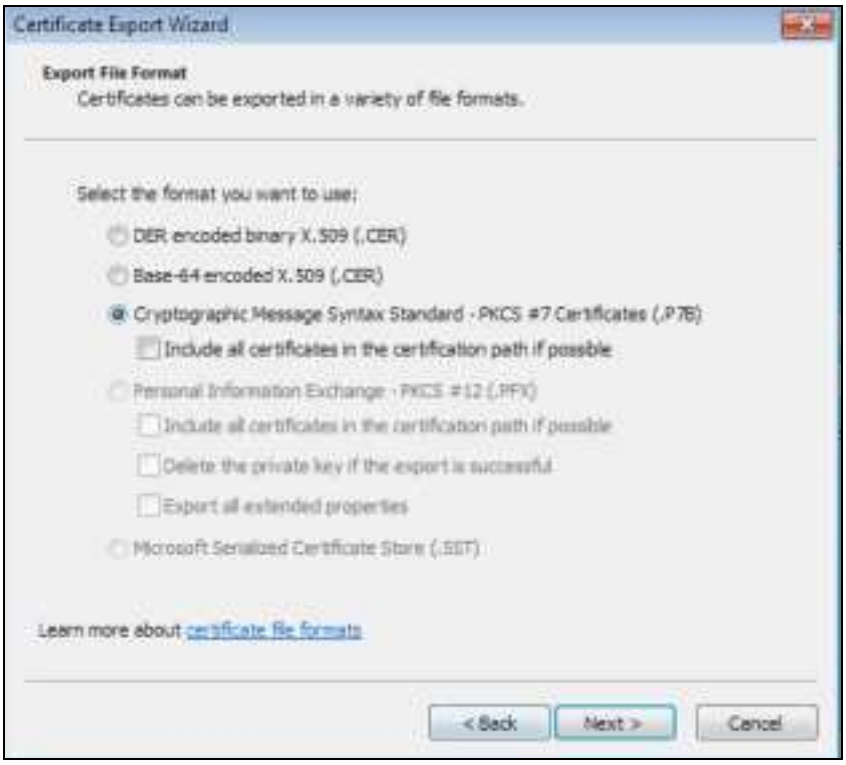
3 In the **Address Bar**, click **Not Secure > Certificate (Invalid)**.

4 In the **Certificate** dialog box, click **Details > Copy to File**.

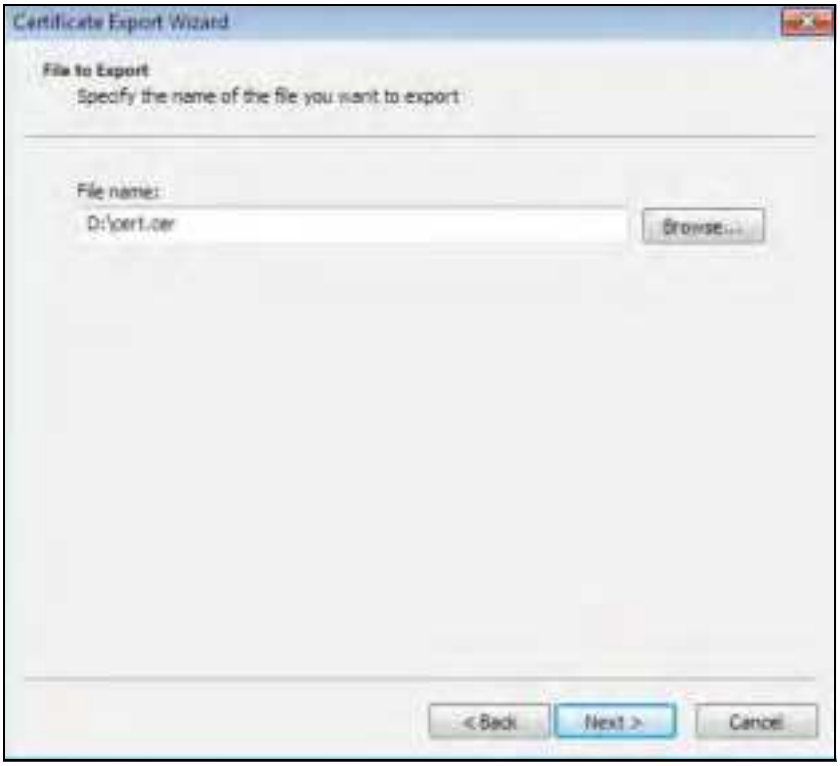


5 In the **Certificate Export Wizard**, click **Next**.

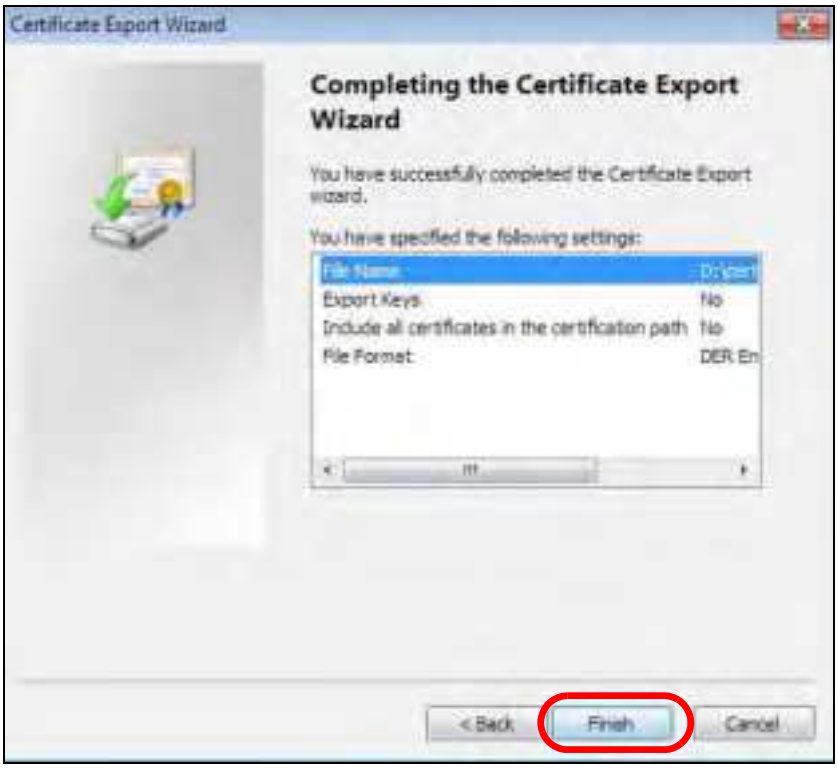
6 Select the format and settings you want to use and then click **Next**.



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**.

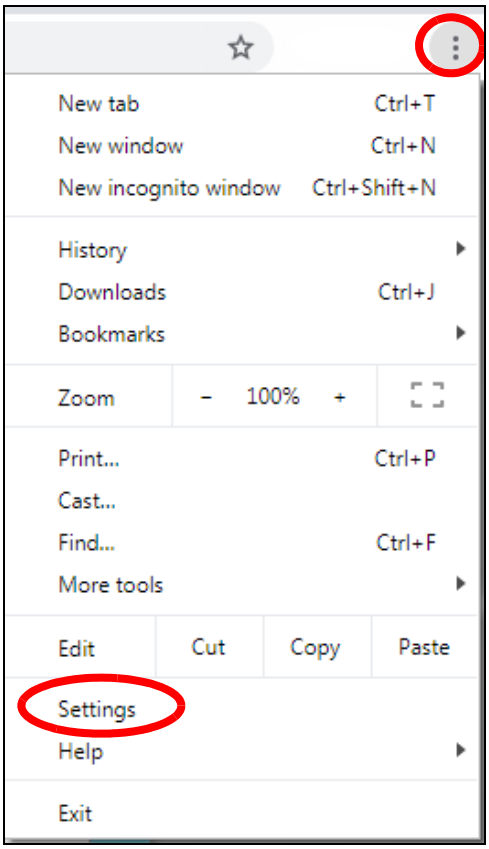


9 Finally, click **OK** when presented with the successful certificate export message.

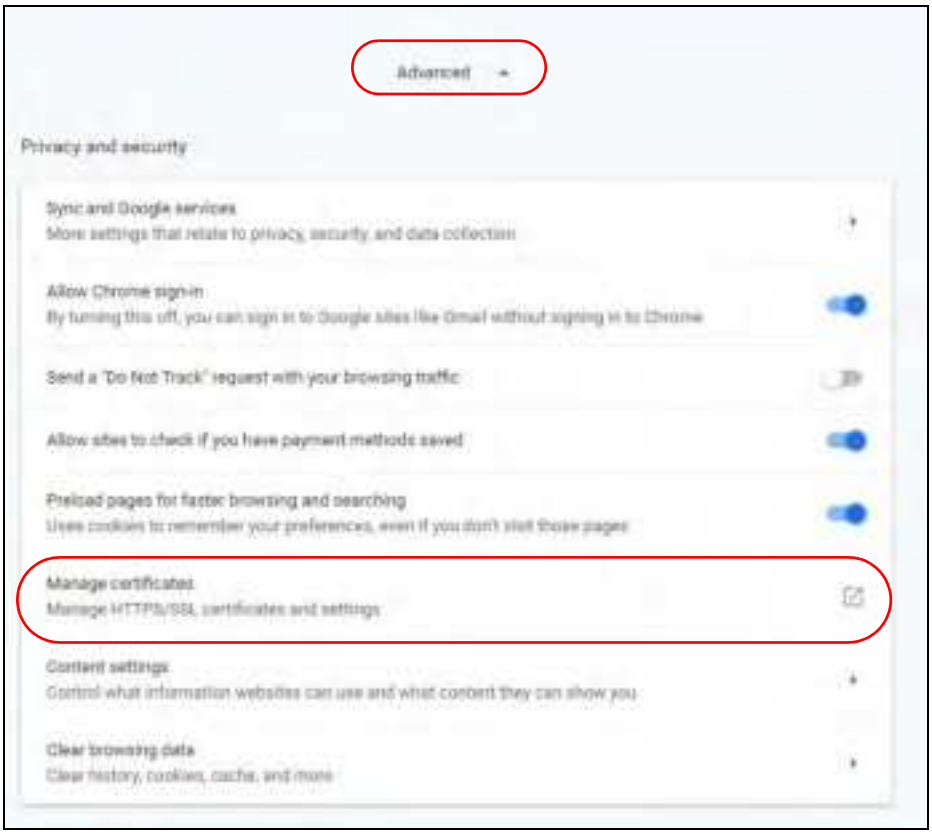
Import a Certificate

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:

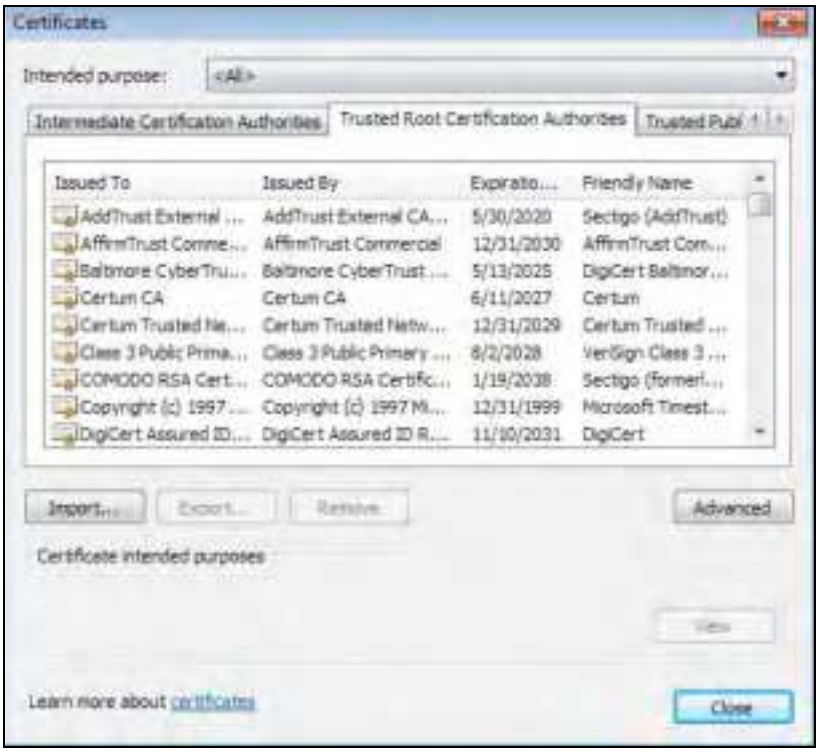
1 Open your web browser, click the menu icon, and click **Settings**.



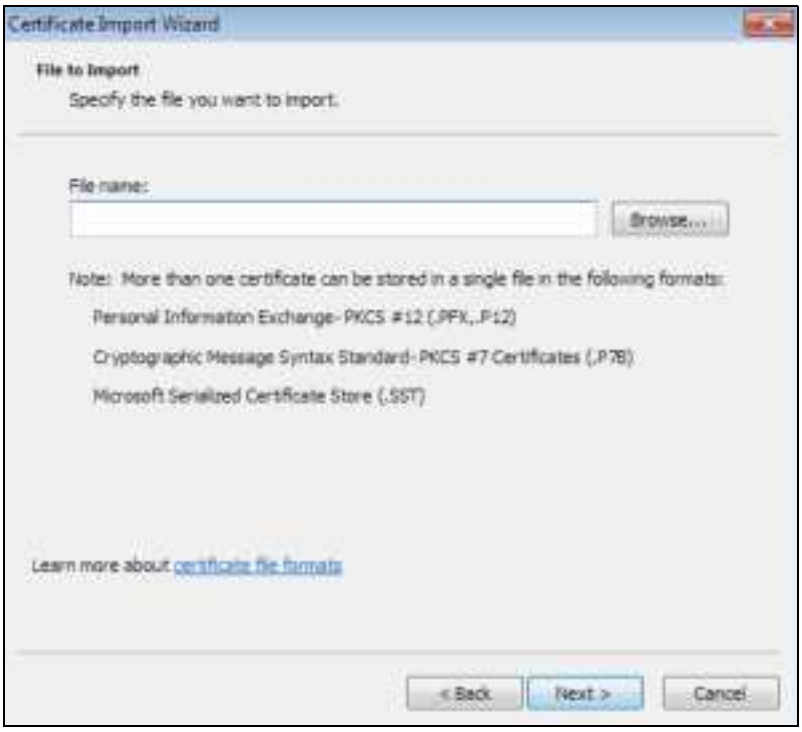
2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



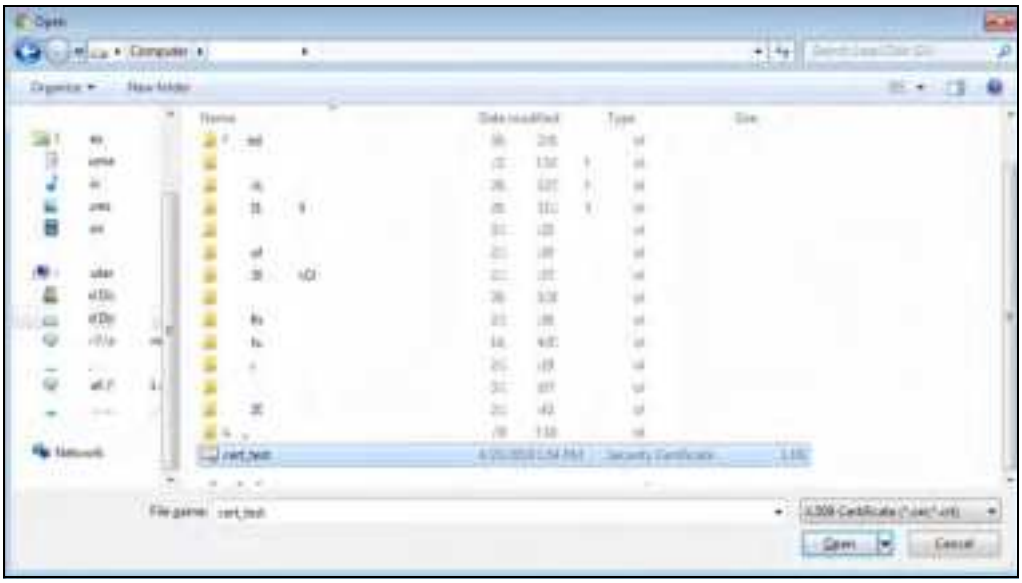
3 In the **Certificates** pop-up screen, click **Trusted Root Certification Authorities**. Click **Import** to start the **Certificate Import Wizard**.



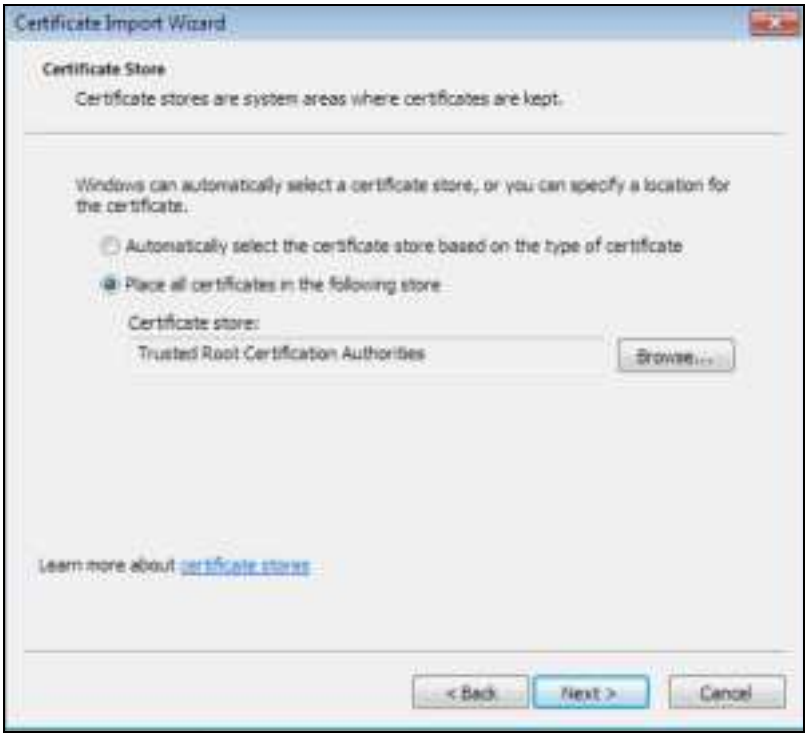
4 Click **Next** when the wizard pops up, and then on the following screen click **Browse**.



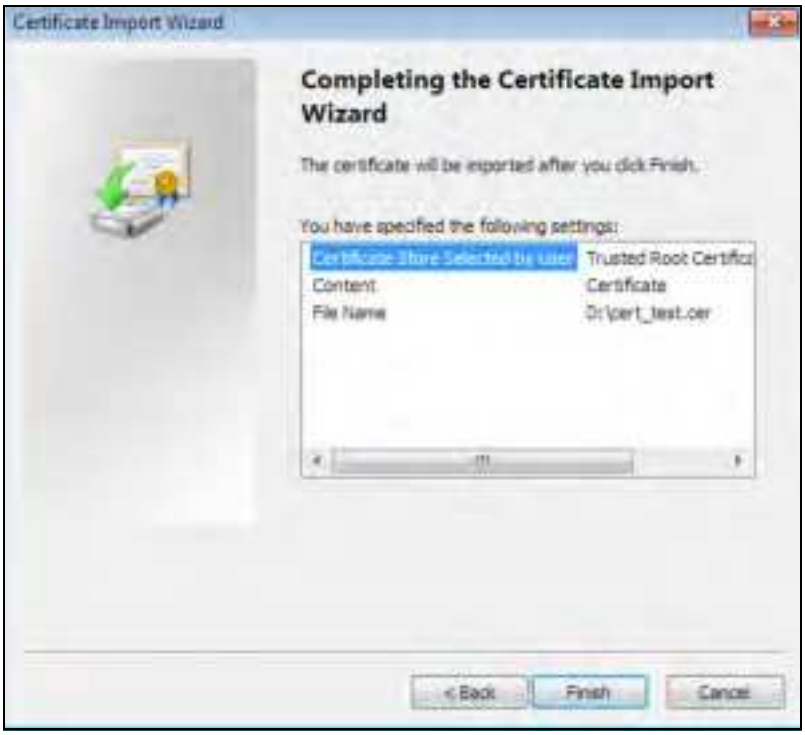
5 Select the certificate file you want to import and click **Open**.



6 Click **Next**.



7 Confirm the settings displayed and click **Finish**.



8 If presented with a security warning, click **Yes**.

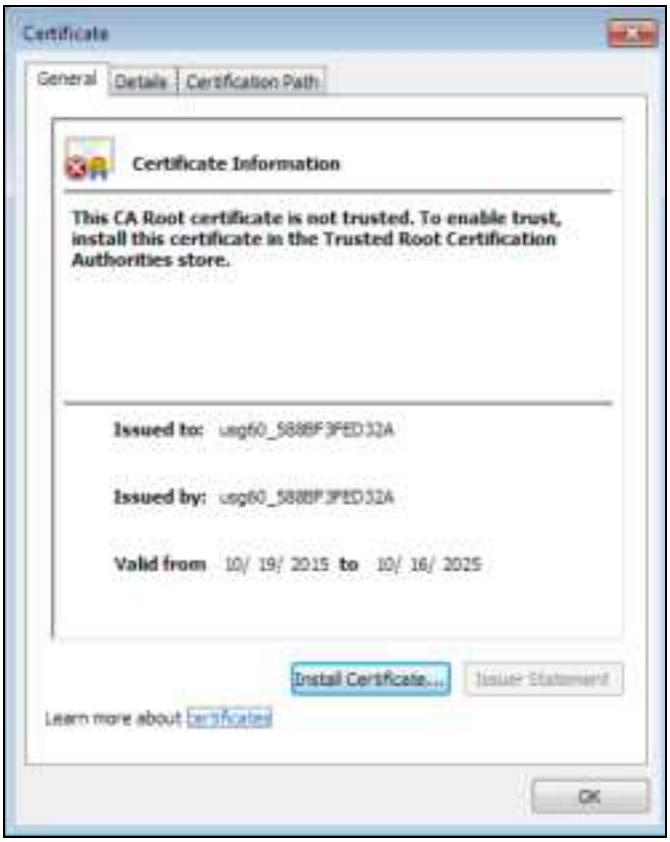
9 Finally, click **OK** when you are notified of the successful import.

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.

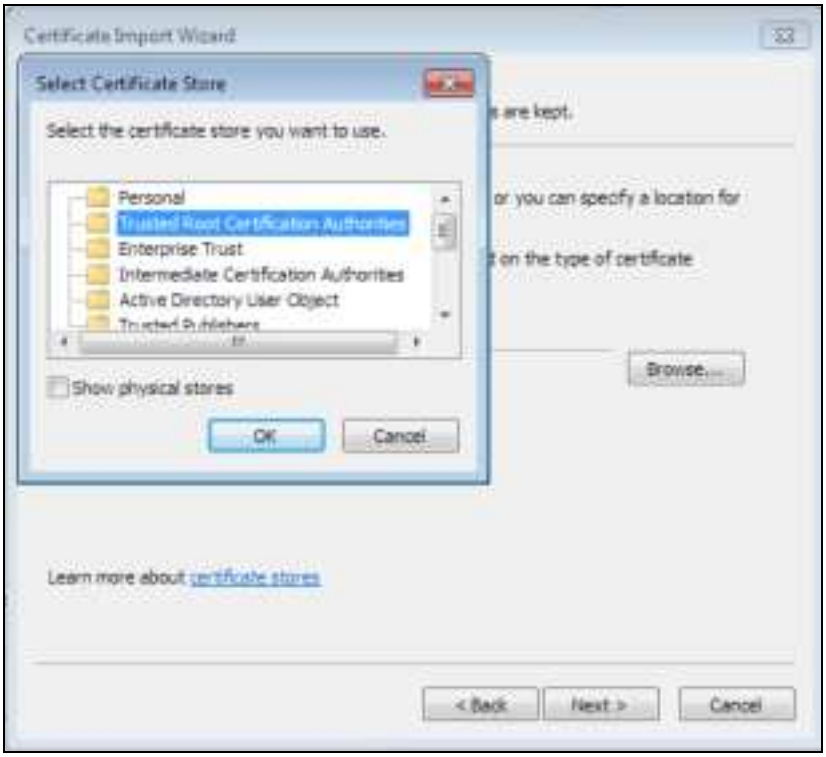
1 Double-click the public key certificate file.

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**.

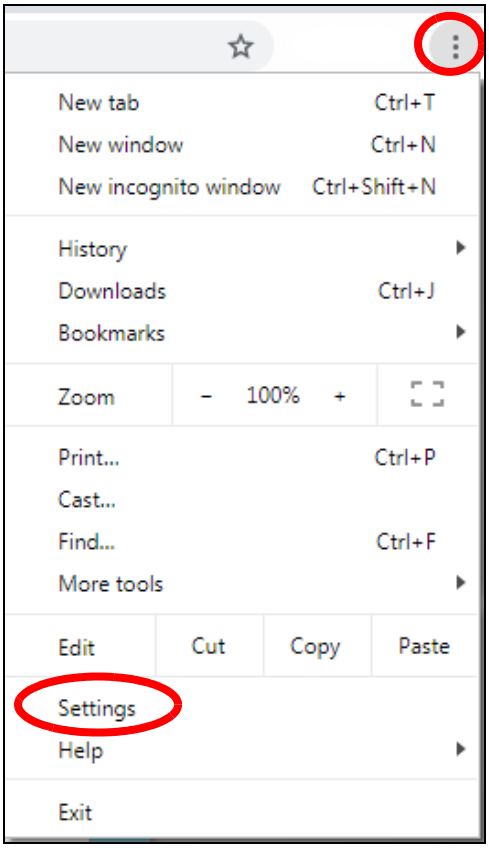
6 If presented with a security warning, click **Yes**.

7 Finally, click **OK** when you are notified of the successful import.

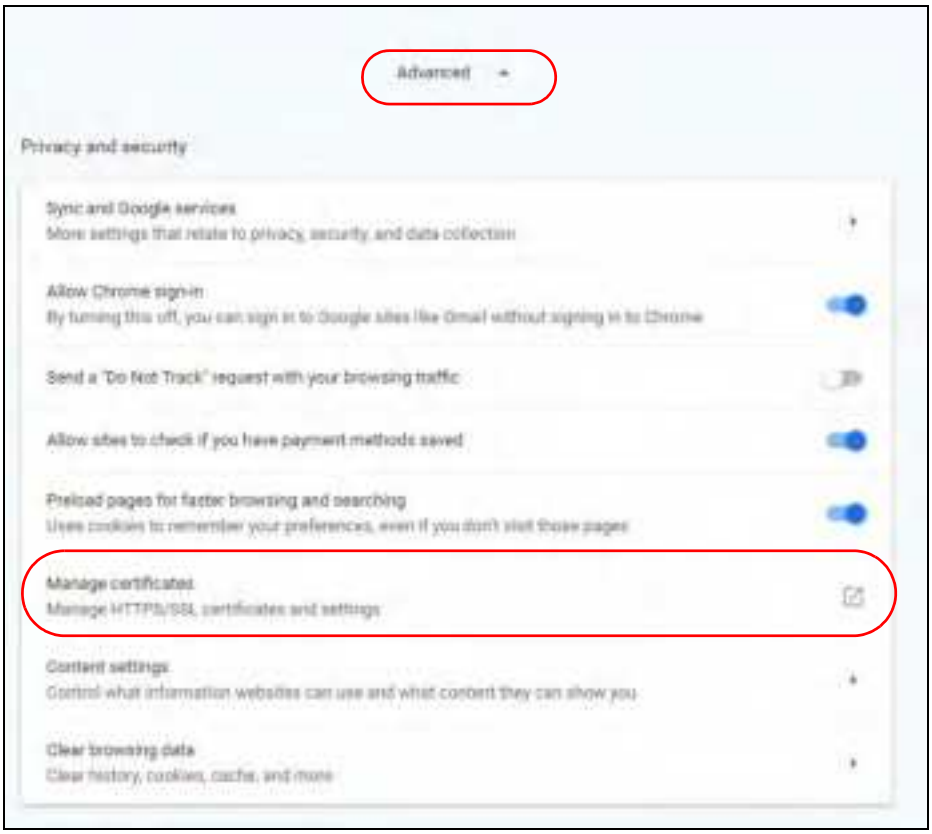
Remove a Certificate in Google Chrome

This section shows you how to remove a public key certificate in Google Chrome on Windows 7.

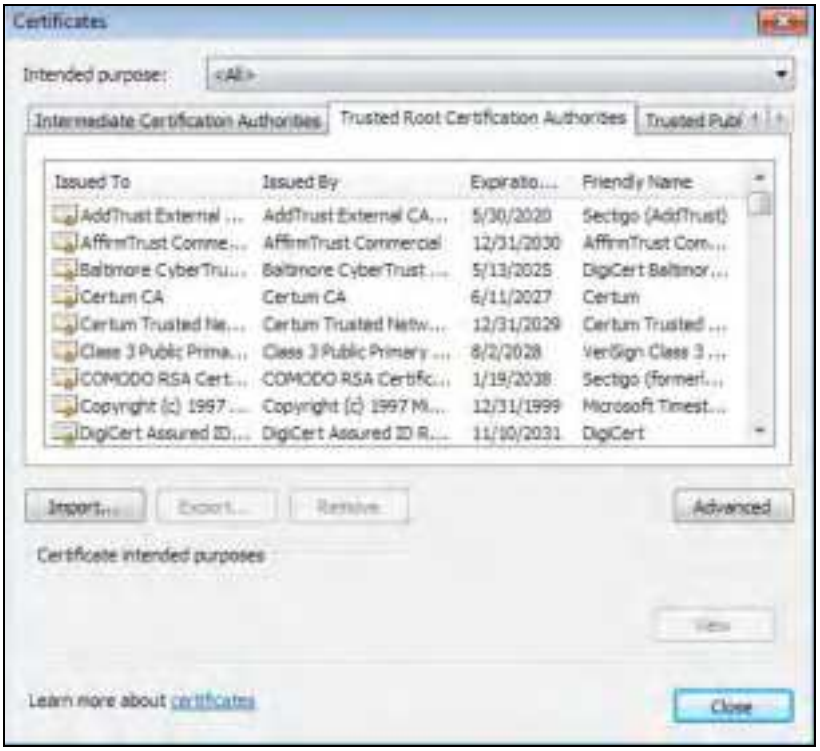
1 Open your web browser, click the menu icon, and click **Settings**.



2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.

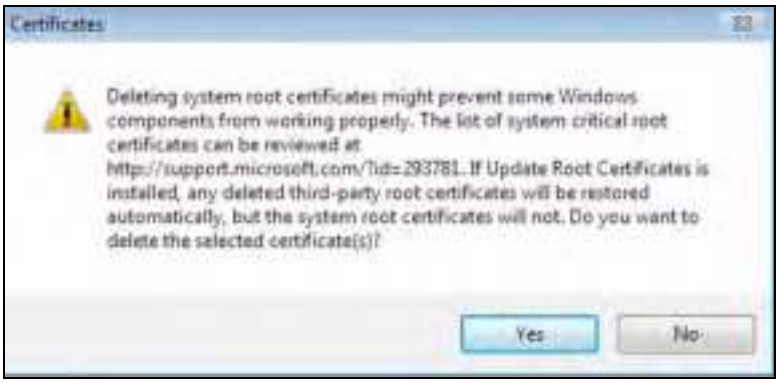


3 In the Certificates pop-up screen, click **Trusted Root Certification Authorities**.

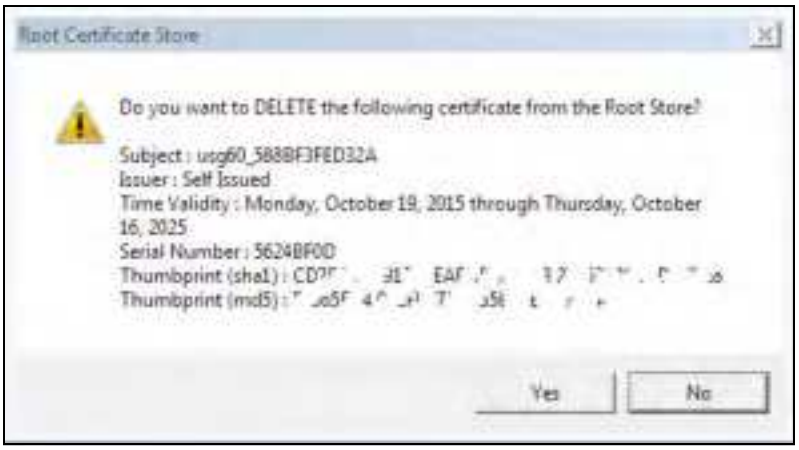


4 Select the certificate you want to remove and click **Remove**.

5 Click **Yes** when you see the following warning message.



6 Confirm the details displayed in the warning message and click **Yes**.

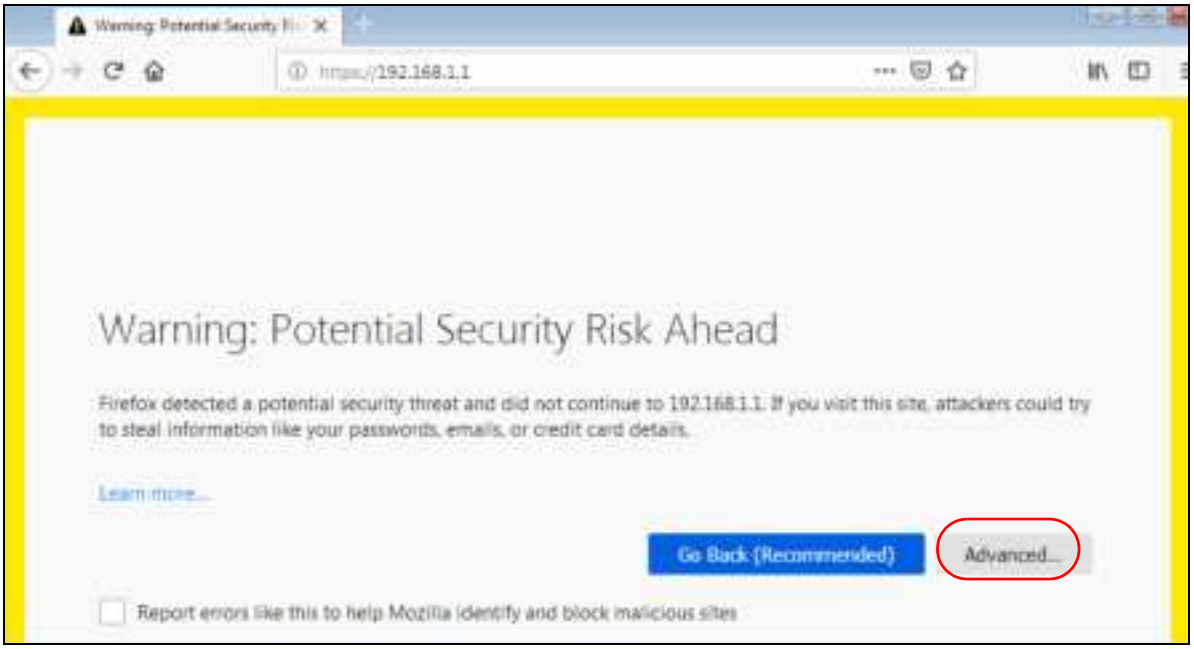


Firefox

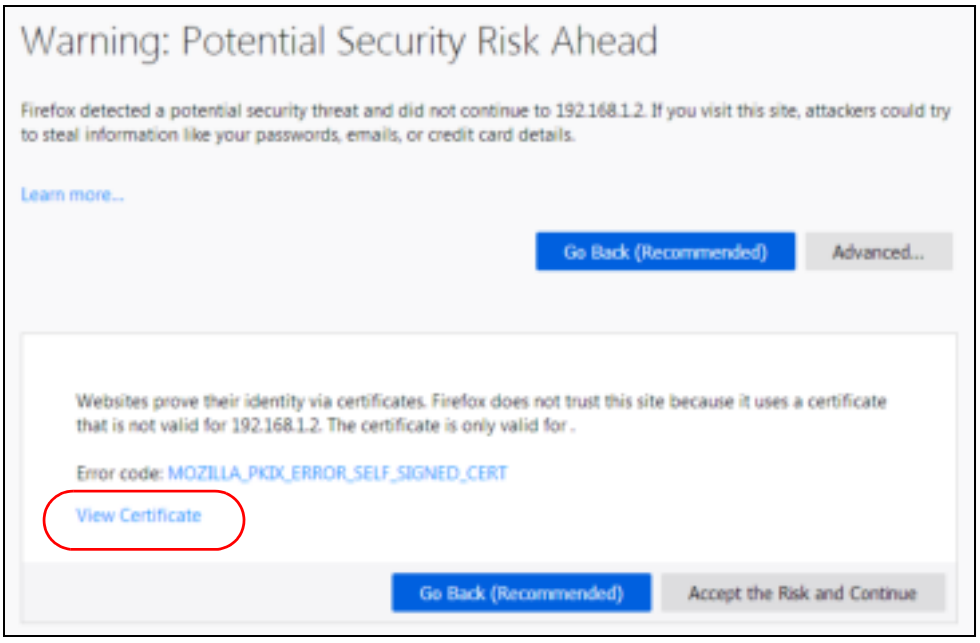
The following example uses Mozilla Firefox on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

Export a Certificate

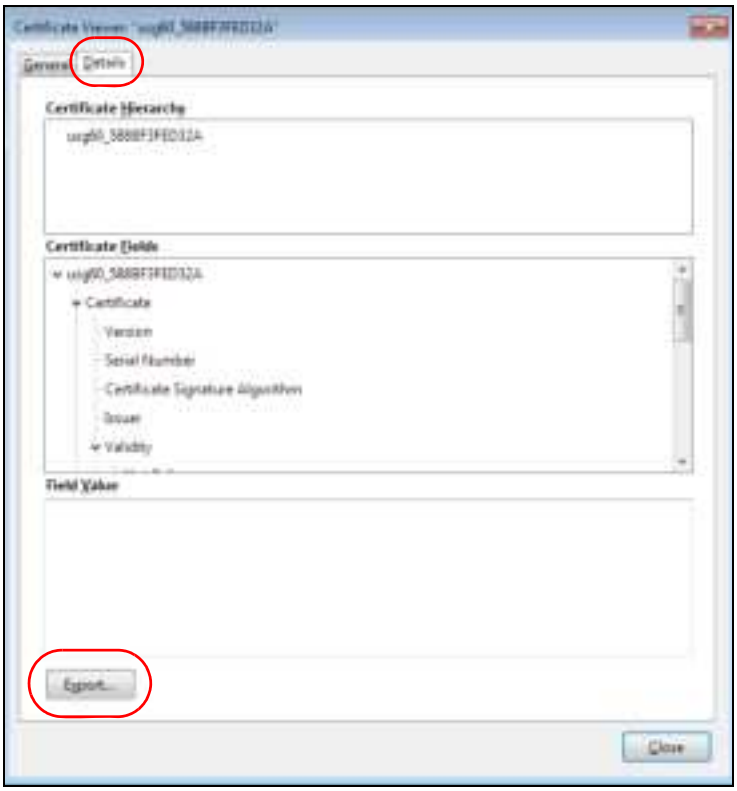
1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error. Click **Advanced**.



2 Click **View Certificate**.



3 Click **Details** > **Export.**

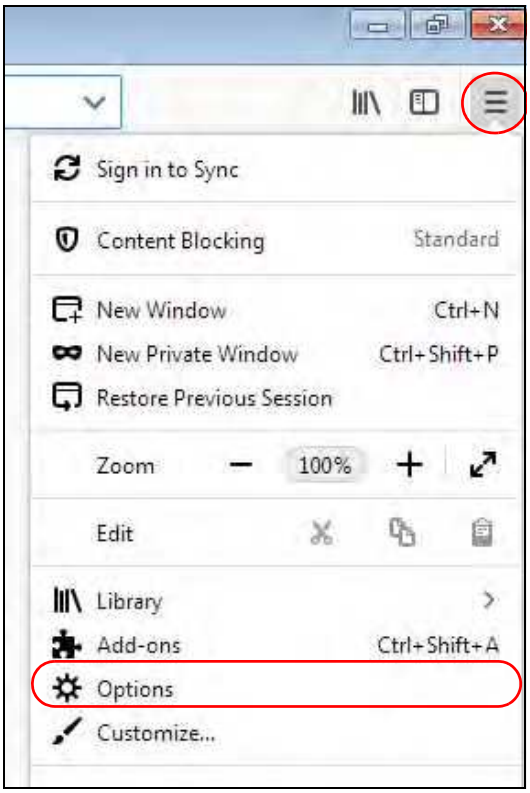


4 Type a filename and click **Save**.

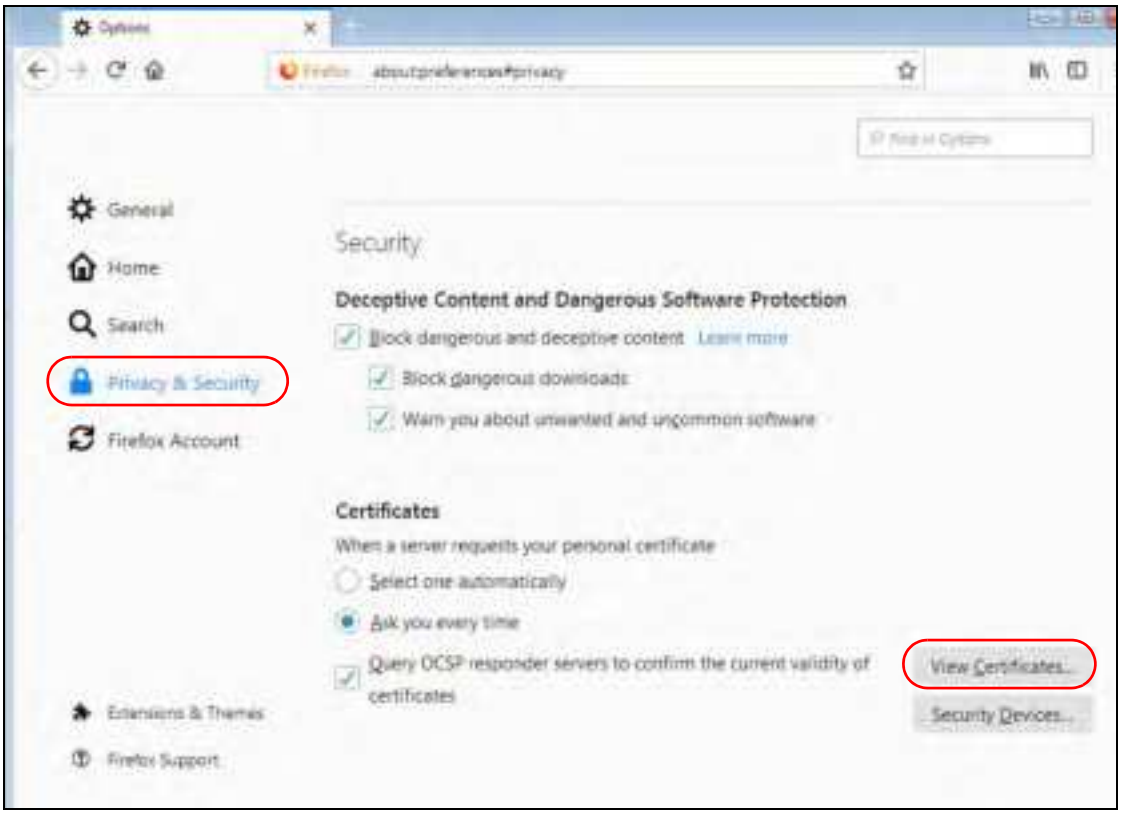
Import a Certificate

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**.