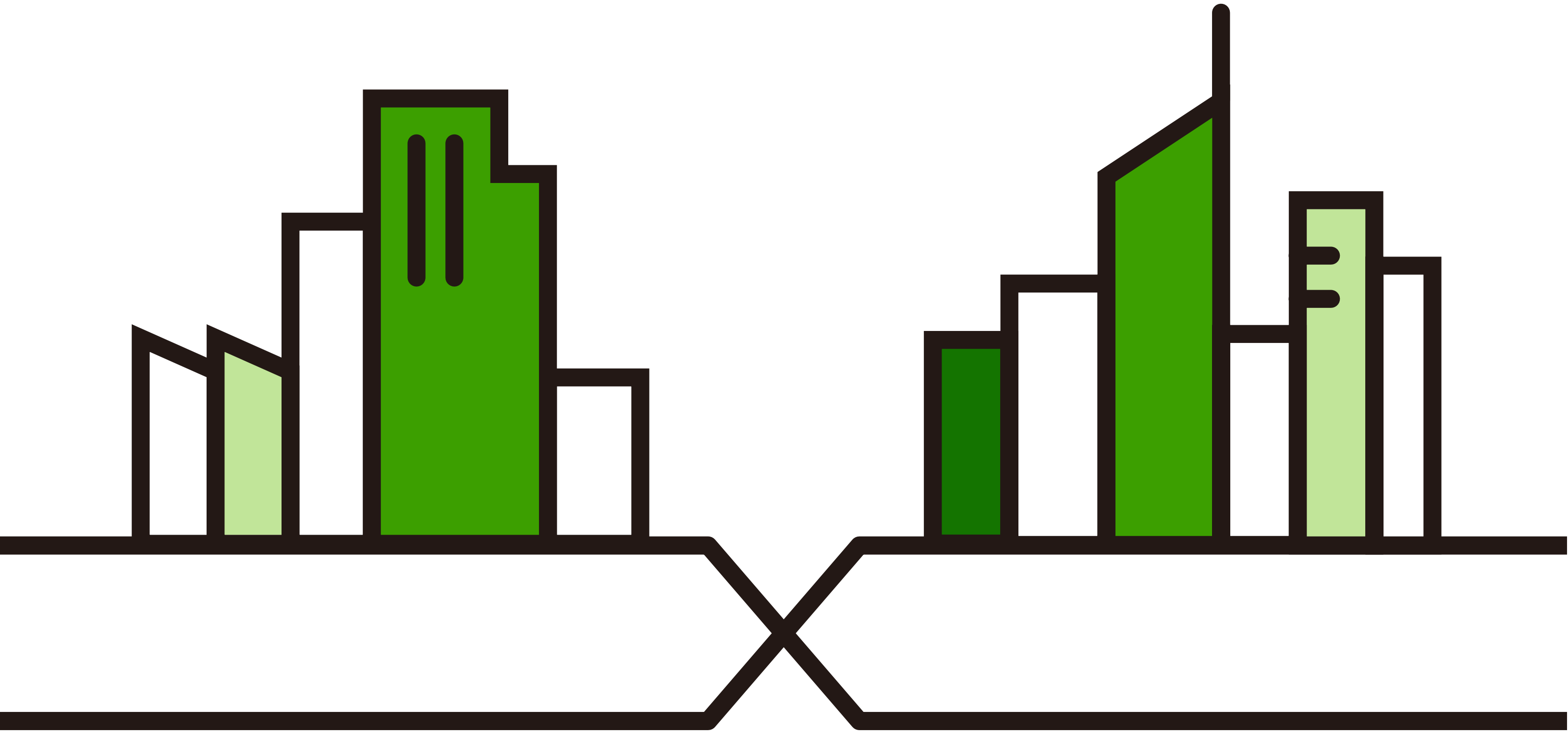
User's Guide

Root Plus

802.11be (WiFi 7) 5G/6G 4X4 Dual-Radio PTMP Base Station

Default Login Details	
Management IP Address	http://DHCP-assigned IP OR http://192.168.1.2
User Name	admin
Password	See Zyxel Device label

Version 7.30 Edition 1, 03/2026



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, **Maintenance** > **File Manager** > **Firmware Package** means you first click **Maintenance** in the navigation panel, then the **File Manager** sub menu and finally the **Firmware Package** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device 	Router 	Switch 	Internet
Server 	Desktop 	Laptop 	IP Phone
Printer 	Smart TV 		

Accessibility and Compatibility

Introduction

This User’s Guide complies with the accessibility requirements set out in EAA (European Accessibility Act) (EU) 2019/882.

Accessibility makes this User’s Guide usable for people with disabilities, including those with visual, auditory, motor, and cognitive impairments. Compatibility ensures this User’s Guide works well with a wide range of devices, software, and assistive technologies.

Accessibility Feature – Screen Reader Support

The visually impaired may use screen readers, such as NVDA to read contents.

To use the screen reader, do the following:

1. Open your screen reader software.
2. Navigate to this User’s Guide; the screen reader should automatically start reading the contents.
3. Use the keyboard shortcuts to navigate through this User’s Guide (refer to the screen reader documentation).

Accessibility Feature – Keyboard Navigation

Keyboard navigation allows you to read the contents in this User’s Guide without a mouse. Use the following keys.

- **Tab** key: navigate between interactive elements (for example, buttons, links, fields).
- **Enter** key: select or activate the highlighted item.
- Arrow keys: move between options in menus or lists.
- **Esc** (Escape) key: close pop-up windows or cancel actions.

How to Access Support Services

We offer the following ways to contact our Zyxel support team.

Email Support: support.zyxel.com

Send a detailed description of your issue, including any error messages, screenshots, or steps you have already taken to resolve the problem. The response time is typically within 24 hours.

User Forums and Community Support: *https://community.zyxel.com/en*

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 GUI Web Configurator in Nebula Cloud-managed mode. For more information about Access Point (AP) management, see Management Mode.

Use the Zyxel Device to set up a WiFi network with other IEEE 802.11a/b/g/n/ac/ax/be compatible devices in either 5 GHz or 6 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 Zyxel Device Roles 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. The Zyxel Device can serve as a:

- Access Point (AP) – This is used to allow WiFi clients to connect to the Internet.
- Radio Frequency (RF) monitor – Your Zyxel Device supports rogue APs detection. It can serve as an RF monitor and searches for rogue APs to help eliminate network threats. An RF monitor can simultaneously act as an AP.
- Root AP – A root AP connects to the gateway or switch through a wired Ethernet connection and has wireless repeaters connected to it to extend its range.

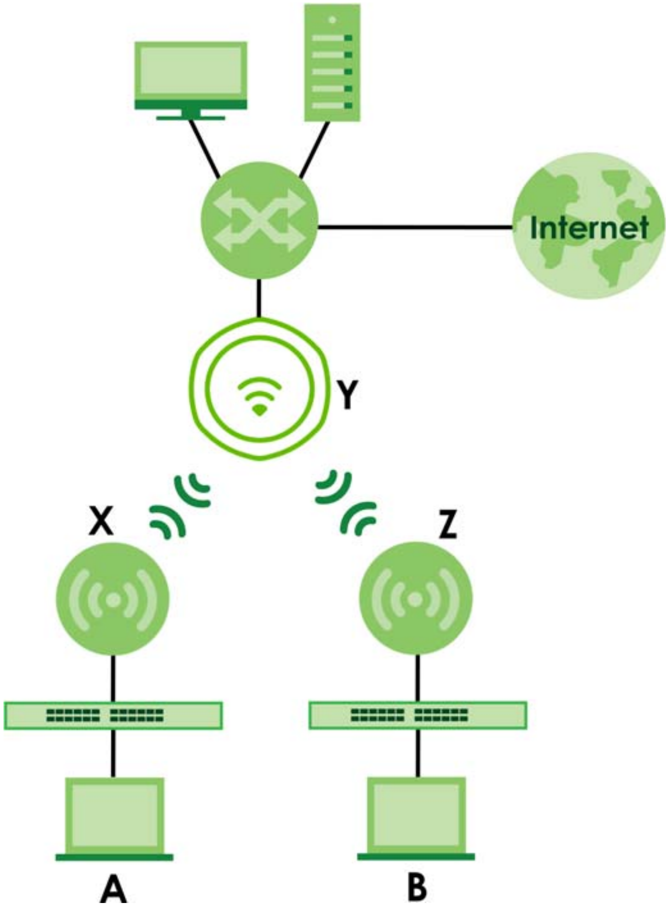
If a client (**D**) tries to set up his own AP (**R**) with weak security settings, the network becomes exposed to threats. The RF monitor scans the area to detect all APs, which can help the network administrator discover these rogue APs and remove them.

Wireless Distribution System (WDS)

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

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

Figure 1 Wireless Distribution System Network Example



Access Point (AP)

The Zyxel Device can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing).

Root AP

The Zyxel Device acts as an AP and also supports the WiFi connections with other APs (in repeater mode) to form a WDS to extend its WiFi network.

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

When the Zyxel Device is in **Root AP** mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key.

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

1.2.1 Radio Frequency (RF) Monitor

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

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

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

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

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

1.3.2 Dual-Radio

The Zyxel Device is equipped with two WiFi radios. The Zyxel Device uses the WiFi radios to transmit WiFi signals. This means you can configure different WiFi networks on the 5G/6G bands to operate simultaneously.

Note: Due to each country’s regulations on frequency band usage, the available radio bands (5 GHz and 6 GHz) may differ by countries or markets the Zyxel Device products are sold to.

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

Multi-Link Operation (MLO)

An AP can support multiple frequency bands (5 GHz and 6 GHz), but a WiFi client can only connect to the AP using one of these frequency bands. The other frequency band is unused. The client's data transmission speed depends on the frequency band they are connected to.

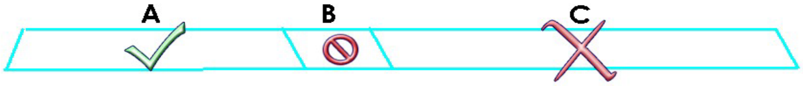
WiFi 7 MLO allows a WiFi client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.

To use MLO, both the AP and the WiFi client have to support MLO.

Preamble Puncturing

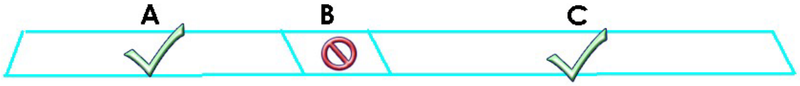
In WiFi 6 and earlier, any interference would cause the entire WiFi channel to become unavailable. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) becomes unavailable.

Figure 2 Without Preamble Puncturing



WiFi 7 preamble puncturing allows you to block the specific portion of the channel that is experiencing interference while continuing to use the rest of the WiFi channel. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) is still available.

Figure 3 Preamble Puncturing Example



CHAPTER 2 AP Management

2.1 Management Mode

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

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

Table 1 Zyxel Device Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP ADDRESS	UPDATE FIRMWARE THROUGH
Nebula Control Center	Dynamic	NCC Portal / Built-in Web Configurator
Local GUI Web Configurator in Nebula Cloud-managed mode	Dynamic or Static (192.168.1.2)	Built-in Web Configurator

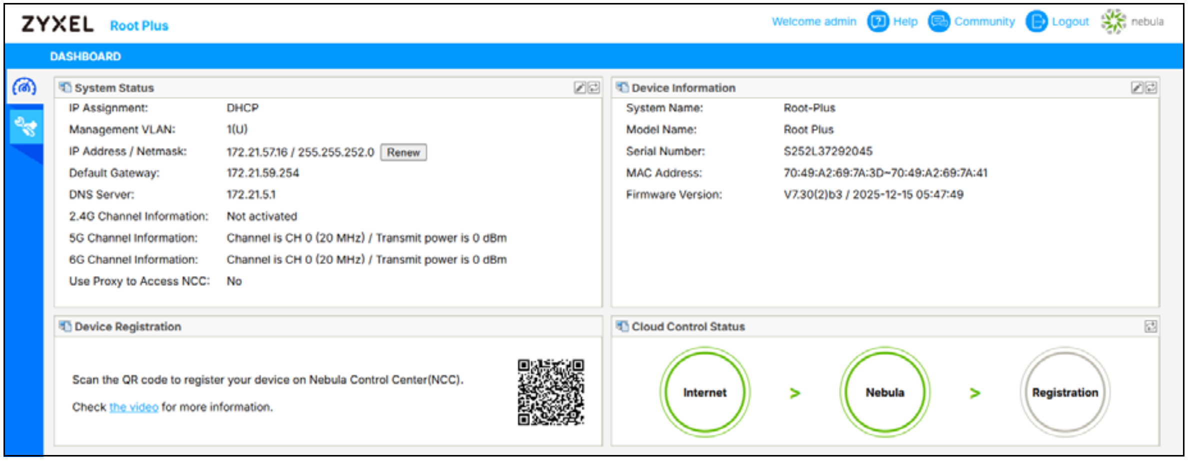
When the Zyxel Device is using the local GUI Web Configurator in Nebula Cloud-managed mode and connects to a DHCP server, it uses the IP address assigned by the DHCP server. Otherwise, the Zyxel Device uses the default static management IP address (192.168.1.2).

When the Zyxel Device is managed by the NCC, it acts as a DHCP client and obtains an IP address from NCC. You can configure the Zyxel Device using the Web Configurator when the Zyxel Device is not connected to NCC.

2.1.1 Local GUI Web Configurator in Nebula Cloud-managed Mode

When using the local GUI Web Configurator in Nebula Cloud-managed mode, the Zyxel Device is configured with its built-in Web Configurator (preferred) or CLI. You can only connect to and set up one Zyxel Device at a time in this mode.

Figure 4 Local GUI Web Configurator in Nebula Cloud-managed Mode



System Status

IP Assignment:	DHCP
Management VLAN:	1(U)
IP Address / Netmask:	172.21.57.16 / 255.255.252.0
Default Gateway:	172.21.59.254
DNS Server:	172.21.5.1
2.4G Channel Information:	Not activated
5G Channel Information:	Channel is CH 0 (20 MHz) / Transmit power is 0 dBm
6G Channel Information:	Channel is CH 0 (20 MHz) / Transmit power is 0 dBm
Use Proxy to Access NCC:	No

Device Information

System Name:	Root-Plus
Model Name:	Root Plus
Serial Number:	S252L37292045
MAC Address:	70:49:A2:69:7A:3D~70:49:A2:69:7A:41
Firmware Version:	V7.30(2)b3 / 2025-12-15 05:47:49

Device Registration

Scan the QR code to register your device on Nebula Control Center(NCC).

Check the video for more information.

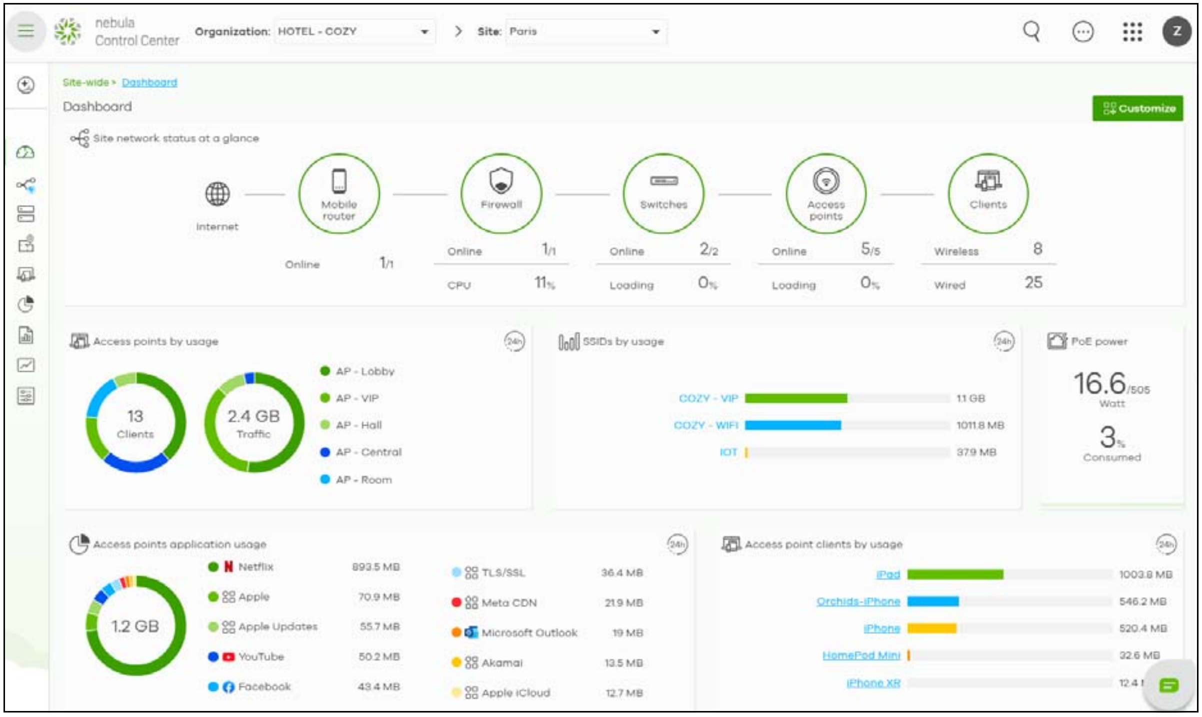
Cloud Control Status

See Web Configurator for detailed information about the local GUI Web Configurator in Nebula Cloud-managed mode screens.

2.1.2 Nebula Control Center

In this mode, which is also called cloud managed 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 Cloud Managed Mode for an example NCC managed network topology.

Figure 5 NCC Dashboard



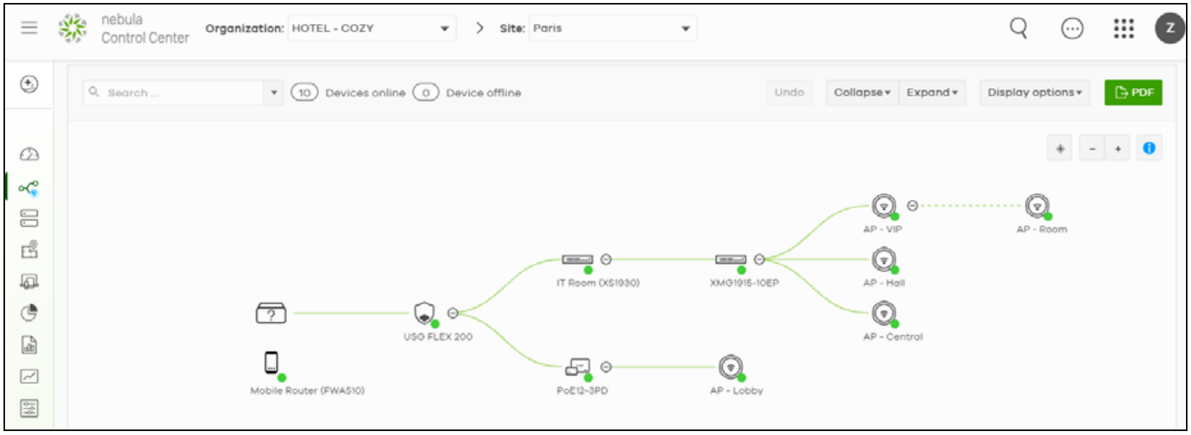
Each Zyxel Device must belong to a site which must be in an organization. You can configure each Zyxel Device on its own or configure a set of Zyxel Devices together in a site. You can also monitor groups of sites in organizations.

Table 2 Sites and Organizations

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

You can use the **Topology** in NCC which graphically presents your device and network statistics. It shows an overview of your network topology, as shown in the following figure. See the NCC User's Guide for how to configure Nebula managed devices.

Figure 6 NCC Topology



Organization: HOTEL - COZY

Site: Paris

10 Devices online

0 Device offline

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

2.2 Switching to Nebula Cloud-managed Mode

This section shows you how to switch the Zyxel Device's management mode to cloud-managed mode.

To change the Zyxel Device management mode, use the **Reset** button to restore the default configuration. Alternatively, you need to check 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 it.

Switch to Nebula Cloud-managed Mode

Register the Zyxel Device on the NCC website and then turn on the Zyxel Device. The NCC manages the Zyxel Device automatically when it is discovered. Settings on the Zyxel Device will be overwritten with what you have configured on the NCC website.

NCC to the Factory-default non Cloud-managed Mode

Back up your configurations first, then unregister the Zyxel Device from NCC. Press the **Reset** button. The Zyxel Device will reset to factory defaults.

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 though 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 computer, 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)
- Windows 10 (both 32-bit / 64-bit versions)
- Windows 11 (64-bit version)

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

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

Hardware

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

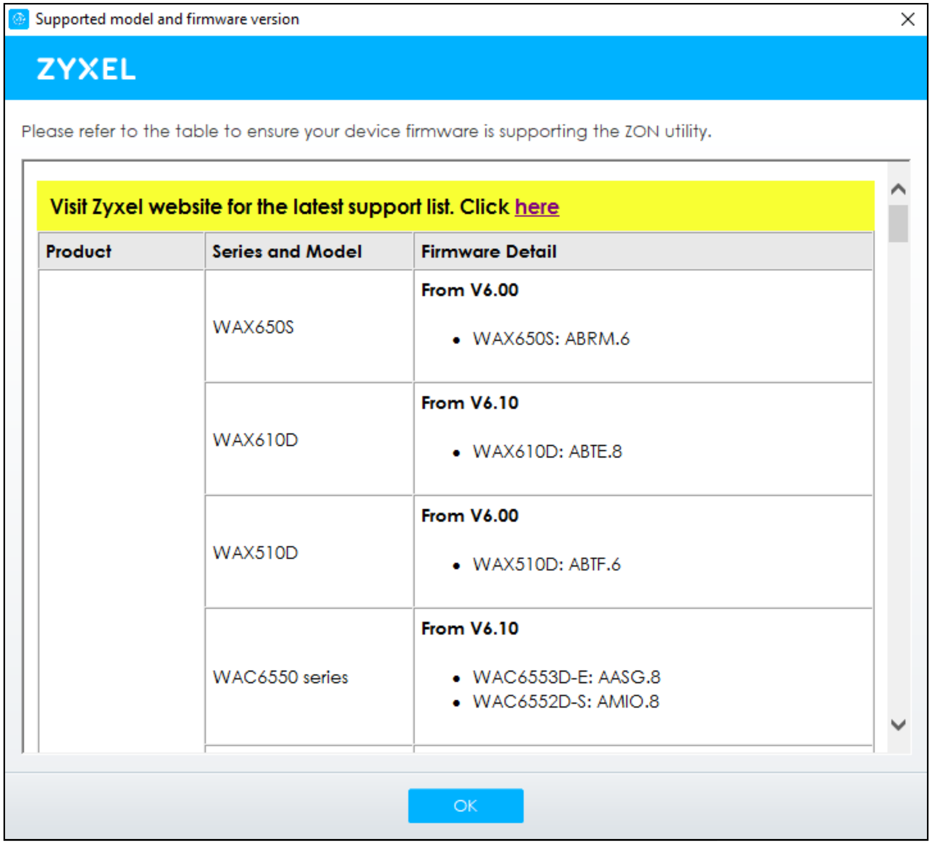
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

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 Zyxel Device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 7 Supported Devices and Versions



Supported model and firmware version

ZYXEL

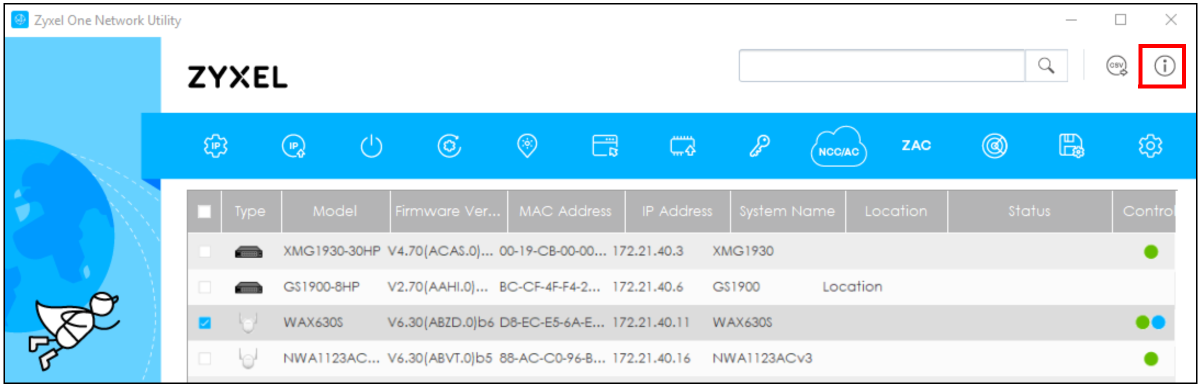
Please refer to the table to ensure your device firmware is supporting the ZON utility.

Visit Zyxel website for the latest support list. Click here

Product	Series and Model	Firmware Detail
	WAX650S	**From V6.00** • WAX650S: ABRM.6
	WAX610D	**From V6.10** • WAX610D: ABTE.8
	WAX510D	**From V6.00** • WAX510D: ABTF.6
	WAC6550 series	**From V6.10** • WAC6553D-E: AASG.8 • WAC6552D-S: AMIO.8

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 8 ZON Utility Screen



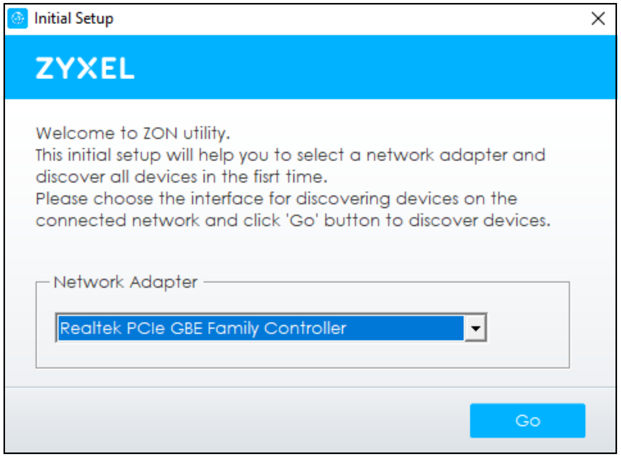
Zyxel One Network Utility

ZYXEL

□	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	Control
□		XMG1930-30HP	V4.70(ACAS.0)...	00-19-CB-00-00...	172.21.40.3	XMG1930			●
□		GS1900-8HP	V2.70(AAHI.0)...	BC-CF-4F-F4-2...	172.21.40.6	GS1900	Location		
☑		WAX630S	V6.30(ABZD.0)b6	D8-EC-E5-6A-E...	172.21.40.11	WAX630S			●●
□		NWA1123AC...	V6.30(ABVT.0)b5	88-AC-C0-96-B...	172.21.40.16	NWA1123ACv3			●

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

Figure 9 Network Adapter

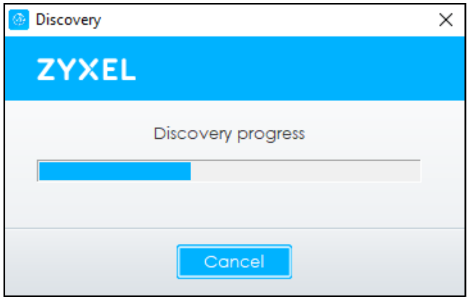


Welcome to ZON utility.
This initial setup will help you to select a network adapter and discover all devices in the fisrt time.
Please choose the interface for discovering devices on the connected network and click 'Go' button to discover devices.

Network Adapter: Realtek PCIe GBE Family Controller

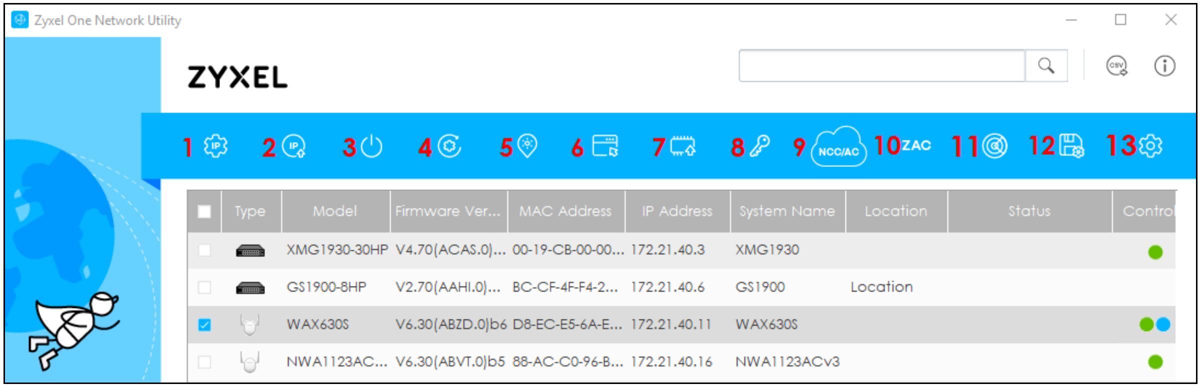
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 10 Discovery



5 The ZON Utility screen shows the devices discovered.

Figure 11 ZON Utility Screen

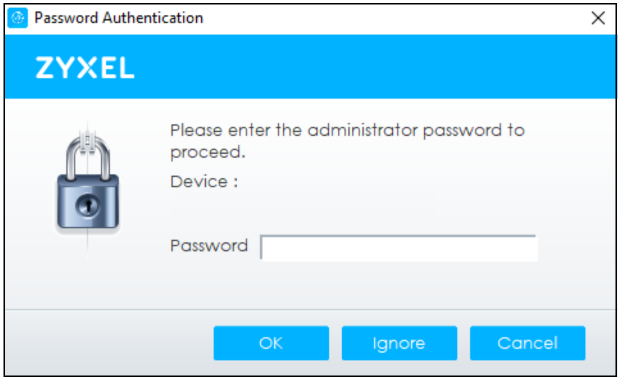


☐	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	Control
☐		XMG1930-30HP	V4.70(ACAS.0)...	00-19-CB-00-00...	172.21.40.3	XMG1930			●
☐		GS1900-8HP	V2.70(AAHI.0)...	BC-CF-4F-F4-2...	172.21.40.6	GS1900	Location		
☑		WAX630S	V6.30(ABZD.0)b6	D8-EC-E5-6A-E...	172.21.40.11	WAX630S			●●
☐		NWA1123AC...	V6.30(ABVT.0)b5	88-AC-C0-96-B...	172.21.40.16	NWA1123ACv3			●

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 Zyxel Device admin password before taking actions on the Zyxel Device using the ZON Utility icons. If the selected Zyxel Device is being managed or has been managed by the NCC, check **Local credentials** in the NCC's **Site-wide** > **Configure** > **Site settings** screen for the selected Zyxel Device's current password.

Figure 12 Password Prompt



Please enter the administrator password to proceed.

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

Table 3 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. The ZON only supports a local GUI Web Configurator in Nebula Cloud-managed mode AP for the firmware upgrade, it does not support to upgrade the firmware for a managed mode AP.
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.
9 Configure Controller Discovery and NCC Discovery	The option is available if the selected device supports AP controller (APC) discovery or Nebula Control Center (NCC) discovery. You must have Internet access to use this feature. Use this icon on the selected device to enable or disable the: • AP controller (APC) discovery feature • Nebula Control Center (NCC) discovery feature If the feature is enabled, the selected device will try to connect to the APC or NCC. If the selected device has successfully connected to an APC, it will change to the controller managed mode. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the cloud managed 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 4 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.
Controller Discovery	This field displays if the discovered device supports the: • AP controller (APC) discovery feature. • Nebula Control Center (NCC) discovery feature. If the feature is enabled, the selected device will try to connect to the APC or NCC. If the selected device has successfully connected to an AP controller, it will change to the AP controller managed mode. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the cloud managed mode. 🟢 means NCC discovery is enabled. 🔵 means controller discovery is enabled. ● means discovery is disabled.
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.
IPv6 Address	This field displays the IPv6 address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.

2.4 Ways to Access the Zyxel Device

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

Web Configurator

The Web Configurator allows easy Zyxel Device setup and management using an Internet browser. If your Zyxel Device is managed by the NCC, 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 managed mode (NCC). 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 Zyxel One Network (ZON) Utility.

Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the Zyxel Device. You can access it using remote management (SSH) or through 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 is 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 Grounding

Earth grounding helps protect against lightning and interference.

Note: The power installation must be performed by qualified service personnel and should conform to the National Electrical Code.

The Zyxel Device must be connected to earth ground to adequately ground the Zyxel Device and protect the operator from electrical hazards.

Qualified service personnel must confirm that the protective earthing terminal of the building is a valid terminal.

Before connecting the ground, ensure that a qualified service personnel has attached an appropriate ground lug to the ground cable.

1 Remove one of the ground screws from the Zyxel Device’s rear panel.

2 Secure a green/yellow ground cable (18 AWG or smaller) to the Zyxel Device’s rear panel using the ground screw.

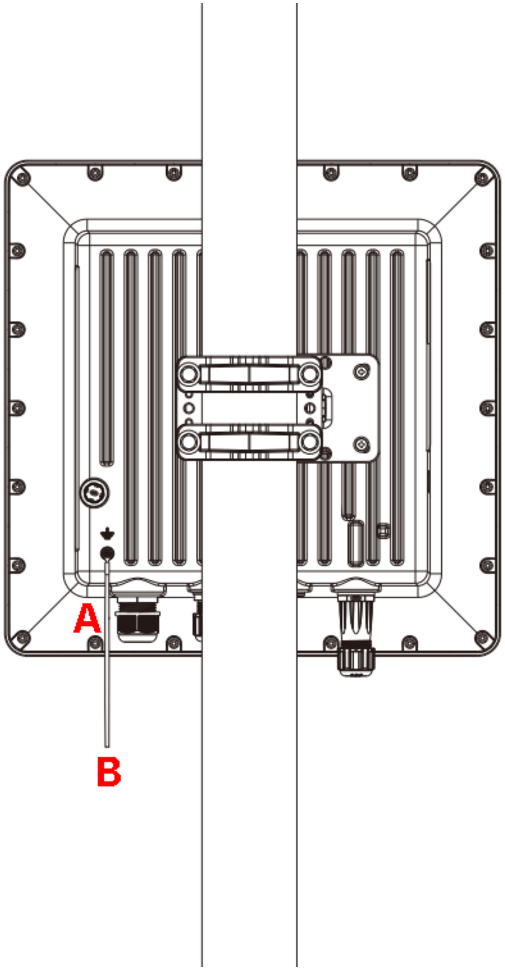
3 Attach the other end of the cable to the ground, either to the same ground electrode as the pole you installed the Zyxel Device on or to the main grounding electrode of the building.

Note: Follow your country's regulations and safety instructions to electrically ground the Zyxel Device properly. If you are uncertain that suitable grounding is available, contact the appropriate electrical inspection authority or an electrician.

Warning! Connect the ground cable before you connect any other cables or wiring.

The figure below illustrates how the ground cable (**A**) is attached to the Zyxel Device and goes to the earth ground (**B**).

Figure 13 Grounding Example



The Zyxel Device should be installed at a 90-degree angle perpendicular to the ground.

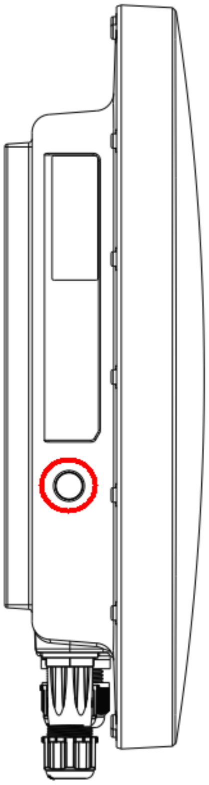
3.2 Zyxel Device LED

802.11be (WiFi 7) 5G / 6G 4X4 Dual-Radio PTMP Base Station

Root Plus

The **Status** LED is located on the right side panel of the Zyxel Device when the back panel is facing you.

Figure 14 Root Plus **Status** LED



The following are the LED descriptions for your Zyxel Device.

Table 5 Zyxel Device **Status** LEDs

COLOR		STATUS	DESCRIPTION
🟨 ↕ 🟩	Amber Green	Blinks between amber and green alternately (300 milliseconds interval).	The Zyxel Device is booting up.
🟩	Green	Blinking (On for 300 milliseconds, Off for 300 milliseconds)	The Zyxel Device is connected to NCC and registered, but no WiFi clients are connected to the Zyxel Device.
🟩	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device is connected to NCC and registered, with WiFi clients connected to the Zyxel Device.
🟨	Amber	Steady On	The Zyxel Device is not connected to NCC, but WiFi clients are connected to the Zyxel Device.
🟨	Amber	Blinking (On for 300 milliseconds, Off for 300 milliseconds)	The Zyxel Device is not connected to NCC, and no WiFi clients are connected to the Zyxel Device.
🟦	Bright Blue	Steady On	The Zyxel Device has completed the boot up process.
⬜	White	Blinking (On for 1 second, Off for 1 second)	The Zyxel Device WiFi is disabled or has failed. Note: This LED behavior appears only when the Zyxel Device is not using the factory default SSID.
🟦	Blue	Blinking (On for 1 second, Off for 1 second)	The Zyxel Device is performing a Channel Availability Check (CAC) with Dynamic Frequency Selection (DFS) to avoid radar channel interference.
🟥	Red	Steady On	The Zyxel Device failed to complete the boot up process.

Table 5 Zyxel Device **Status** LEDs (continued)

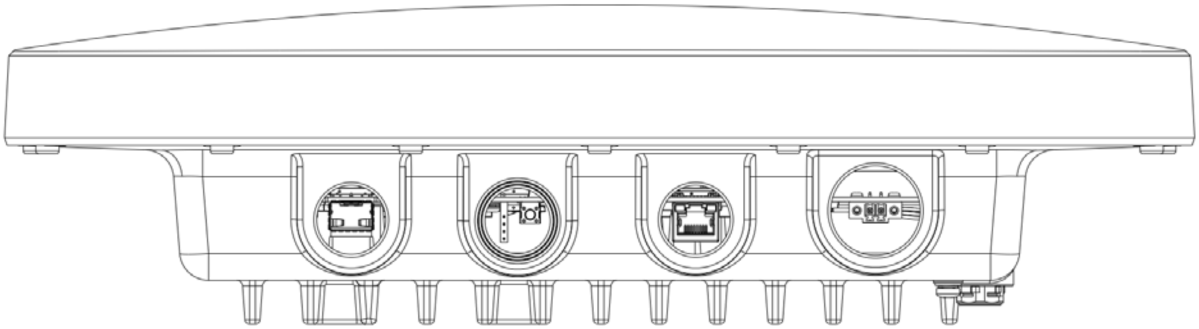
COLOR		STATUS	DESCRIPTION
🟥	Red	Fast Blinking (On for 50 milliseconds, Off for 50 milliseconds)	The Zyxel Device is undergoing firmware upgrade.
🟥	Red	Slow Blinking (On for 1 second, Off for 5 seconds)	The Zyxel Device is connected to NCC, but not registered with NCC.

3.3 Ports

Root Plus

Place the Zyxel Device with the ports facing you and the top panel on top.

Figure 15 Root Plus Ports and Buttons



The following are the items on the ports panels for your Zyxel Device.

Table 6 Root Plus Ports and Buttons

LABEL	DESCRIPTION
DC in 24–48 V	Connect the power to start the Zyxel Device. See DC Power Connection for more information on connecting the DC power to the Zyxel Device.
Ethernet PoE (IEEE 802.3bt 60 W standard)	Connect the Zyxel Device to the PoE injector’s power port to power the Zyxel Device. Then connect a router or computer to the PoE injector’s LAN port to connect the Zyxel Device to the backbone of your network.

Table 6 Root Plus Ports and Buttons (continued)

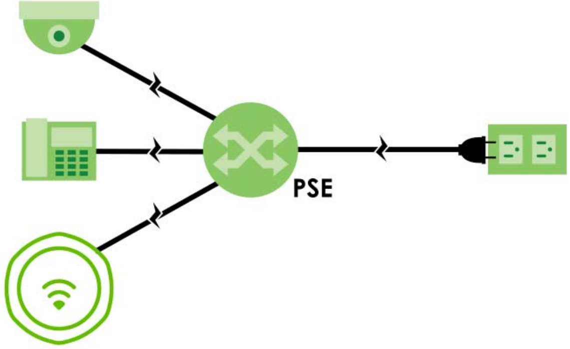
LABEL	DESCRIPTION
Reset /	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
Console	You can use the 4-pin console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
SFP+	Use an SFP+ transceiver in this port for high-bandwidth backbone connections.

3.4 PoE

Power Over Ethernet (PoE) is a technology that allows Ethernet cables to supply power and transmit data simultaneously through a single Ethernet cable. You can use PoE when the Zyxel Device is hard to reach a power outlet or to simplify cabling.

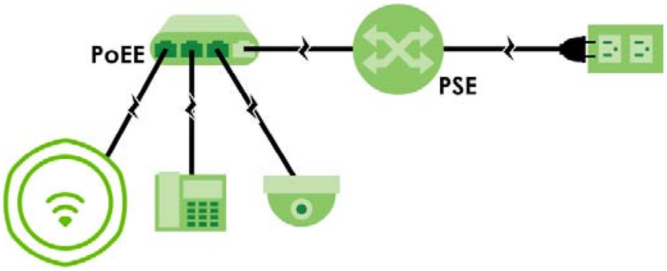
The following example shows a Power Sourcing Equipment (**PSE**) supplying power and transmitting data to the Zyxel Device, along with other Powered Devices (PDs) such as an IP camera and an IP telephone.

Figure 16 PoE Example Application – PSE



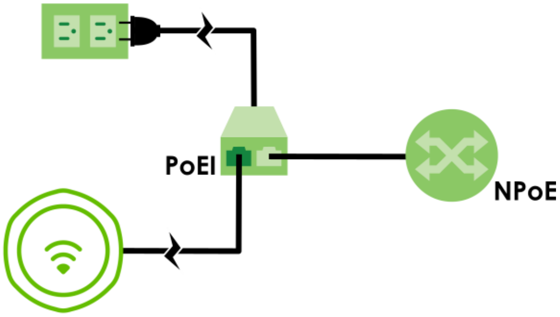
The following example shows a **PSE** using a PoE Extender (**PoEE**) to supply power and transmit data to the Zyxel Device, along with other PDs such as an IP camera and an IP telephone.

Figure 17 PoE Example Application – PSE with PoE Extender



The following example shows the PoE Injector (**PoEI**) delivering power from the power outlet and transmitting data from the non-PoE (**NPoE**) device to the Zyxel Device.

Figure 18 PoE Example Application – PoE Injector



Use Ethernet cables that correspond to the PoE standard your Zyxel Device supports (see PoE Standards).

PoE standards are:

- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet + (PoE+)
- IEEE 802.3bt Power over Ethernet ++ (PoE++)

The following table describes the PoE standards.

Table 7 PoE Standards

POE FEATURES	POE	POE+	POE++
IEEE Standard	IEEE 802.3af	IEEE 802.3at	IEEE 802.3bt
PoE Type	Type 1	Type 2	Type 3
PSE Port Power	PSE Port Power	PSE Port Power	PSE Port Power
IEEE Power Classification	Class 0, 1, 2, 3	Class 4	Class 5, 6
Maximum Power Per Port	15.4 W	30 W	60 W
Port Voltage Range	44 – 57 V	50 – 57 V	50 – 57 V
Cables	Cables	Cables	Cables
Twisted Pairs Used	2-pair	2-pair	4-pair
Supported Cables	Cat3 or better	Cat5 or better	Cat5 or better

3.5 DC Power Connection

The Zyxel Device uses a single D-sub series terminal block plug with two pins. Use two wires to connect to the terminal block: one for the positive terminal and one for the negative terminal.

Note: The current rating of the power wires must be greater than 16 AWG. The power supply to which the Zyxel Device connects must have a built-in circuit breaker or switch to toggle the power.

Note: When installing the Zyxel Device power wire, push the wire firmly into the terminal as deep as possible and make sure that no exposed (bare) wire can be seen or touched.

Exposed power wire is dangerous. Use extreme care when connecting a DC power source to the Zyxel Device.

WARNING! Working with high-voltage DC power is dangerous. To ensure safety of equipment and regulatory compliance, the DC power connection must be performed by a certified technician.

To connect a power supply:

1 Use a screwdriver to loosen the captive screws on the D-sub's terminal block.

2 Connect one end of a power wire to the Zyxel Device's 48 V (return) pin and tighten the captive screw.

3 Connect the other end of the power wire to the positive terminal on the DC power supply.

4 Connect one end of a power wire to the Zyxel Device's –48 V (input) pin and tighten the captive screw.

5 Connect the other end of the power wire to the negative terminal on the power supply.

6 Insert the D-sub terminal block's male connector plug into the Zyxel Device's **DC in 24–48 V** port and tighten the two captive screws.

3.5.1 SFP+ Slot

This is the slot for SFP+ (Small Form-Factor Pluggable) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Zyxel Device does not come with a transceiver. You must use a transceiver that comply with the Small Form-factor Pluggable (SFP+) Transceiver MultiSource Agreement (MSA). See the SFF committee's specifications.

You can change a transceiver while the Zyxel Device is operating. You can use a different transceiver to connect to devices with different types of fiber optic or even copper cable connectors.

WARNING! To avoid possible eye injury, do not look into an operating fiber optic module's connectors.
HANDLING! All transceivers are static sensitive. To prevent damage from electrostatic discharge (ESD), it is recommended you attach an ESD preventive wrist strap to your wrist and to a bare metal surface when you install or remove a transceiver.

STORAGE! All modules are dust sensitive. When not in use, always keep the dust plug on. Avoid getting dust and other contaminant into the optical bores, as the optics do not work correctly when obstructed with dust.

3.5.1.1 Transceiver Installation

Use the following steps to install a transceiver.

1. Attach an ESD preventive wrist strap to your wrist and to a bare metal surface.
2. Align the transceiver in front of the slot opening.
3. Make sure the latch is in the lock position (latch styles vary), then insert the transceiver into the slot with the exposed section of PCB board facing down.
4. Press the transceiver firmly until it clicks into place.
5. The Zyxel Device automatically detects the installed transceiver.
6. Remove the dust plugs from the transceiver and cables (dust plug styles vary).
7. Identify the signal transmission direction of the fiber optic cables and the transceiver. Insert the fiber optic cable into the transceiver.

Figure 19 Latch in the Lock Position

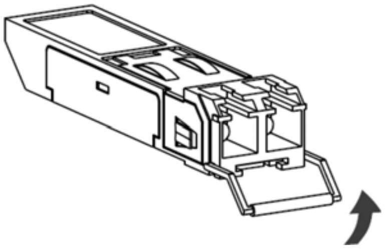


Figure 20 Transceiver Installation Example

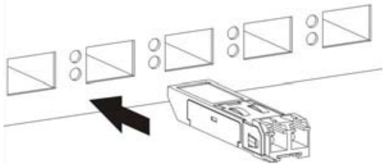
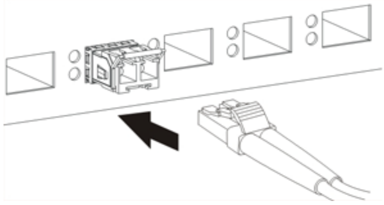


Figure 21 Connecting the Fiber Optic Cables



3.5.1.2 Transceiver Removal

Use the following steps to remove an SFP transceiver.

1. Attach an ESD preventive wrist strap to your wrist and to a bare metal surface on the chassis.

2 Remove the fiber optic cables from the transceiver.

3 Pull out the latch and down to unlock the transceiver (latch styles vary).

Note: Make sure the transceiver's latch is pushed all the way down, so the transceiver can be pulled out successfully.

4 Pull the latch, or use your thumb and index finger to grasp the tabs on both sides of the transceiver, and carefully slide it out of the slot.

Note: Do NOT pull the transceiver out by force. You could damage it. If the transceiver will not slide out, grasp the tabs on both sides of the transceiver with a slight up or down motion and carefully slide it out of the slot. If unsuccessful, contact Zyxel Support to prevent damage to your Zyxel Device and transceiver.

5 Insert the dust plug into the ports on the transceiver and the cables.

Figure 22 Removing the Fiber Optic Cables

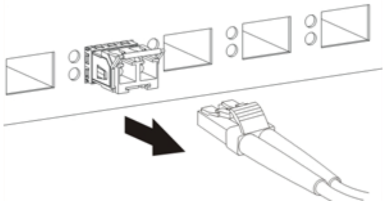


Figure 23 Opening the Transceiver's Latch Example

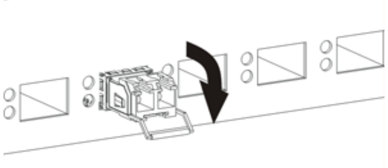
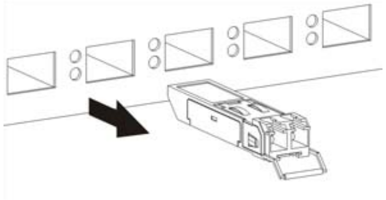


Figure 24 Transceiver Removal Example



CHAPTER 4
Web Configurator

4.1 Overview

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

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

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

4.2 Accessing the Web Configurator

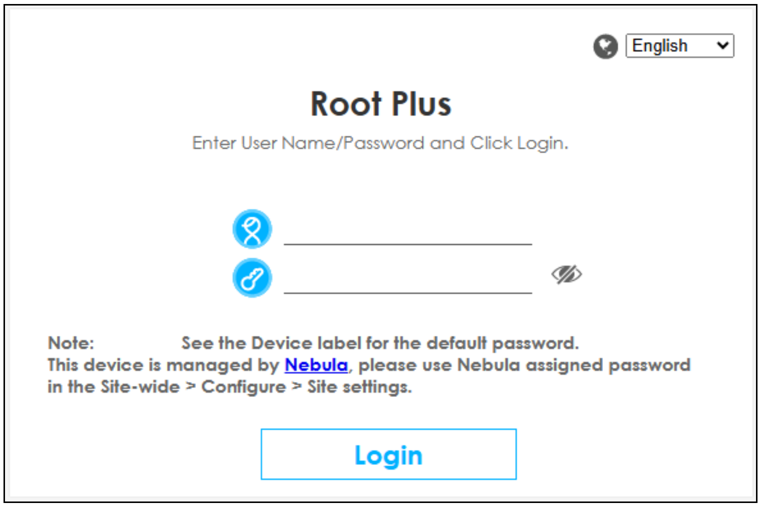
This section shows how to access the Web Configurator for the first time.

1 Ensure your Zyxel Device hardware is properly connected. See the Quick Start Guide.

2 Access the Web Configurator login screen through a wired connection.

Use an Ethernet cable to connect your computer to the Zyxel Device. Open your web browser and enter the Zyxel Device's DHCP-assigned IP address or http://192.168.1.2. If the Zyxel Device and your computer are not connected to a DHCP server, ensure your computer's IP address is between "192.168.1.3" and "192.168.1.254".

3 Enter the user name (default: "admin") and default password. The default password is unique to each Zyxel Device and shown on the label.



Root Plus

Enter User Name/Password and Click Login.

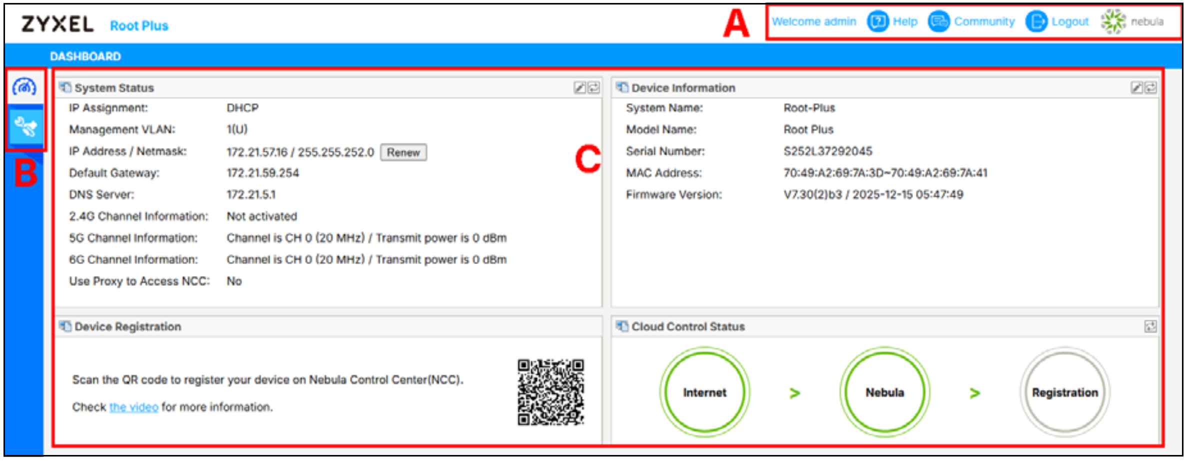
Note: See the Device label for the default password.
This device is managed by Nebula, please use Nebula assigned password in the Site-wide > Configure > Site settings.

4 Select the language you prefer for the Web Configurator. Click **Login**.

4.3 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Dashboard** screen. The figures below show the **Dashboard** screen.

Figure 25 Web Configurator's Dashboard



System Status

IP Assignment:	DHCP
Management VLAN:	1(U)
IP Address / Netmask:	172.21.57.16 / 255.255.252.0
Default Gateway:	172.21.59.254
DNS Server:	172.21.5.1
2.4G Channel Information:	Not activated
5G Channel Information:	Channel is CH 0 (20 MHz) / Transmit power is 0 dBm
6G Channel Information:	Channel is CH 0 (20 MHz) / Transmit power is 0 dBm
Use Proxy to Access NCC:	No

Device Information

System Name:	Root-Plus
Model Name:	Root Plus
Serial Number:	S252L37292045
MAC Address:	70:49:A2:69:7A:3D~70:49:A2:69:7A:41
Firmware Version:	V7.30(2)b3 / 2025-12-15 05:47:49

Device Registration

Scan the QR code to register your device on Nebula Control Center(NCC).

Check the video for more information.

Cloud Control Status

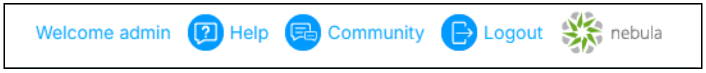
The Web Configurator's main screen is divided into these parts:

- **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.

Figure 26 Title Bar



The icons provide the following functions.

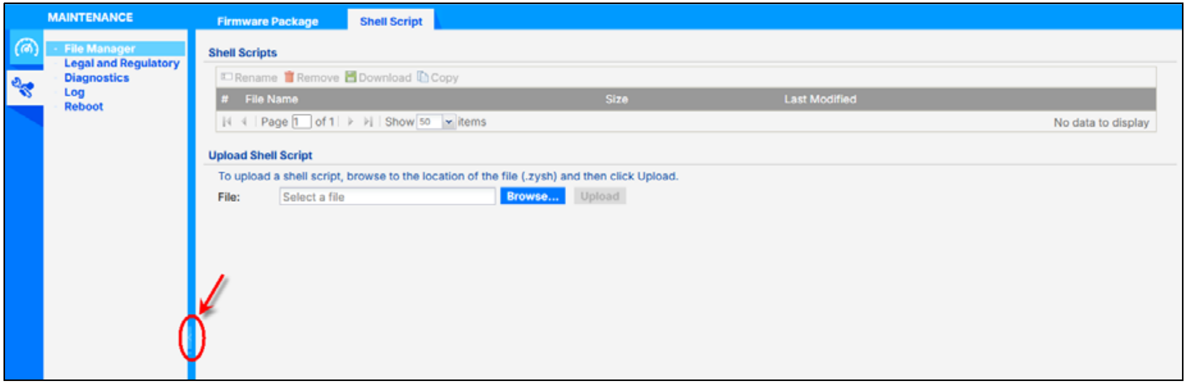
Table 8 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Help	Click this to open the help page for the current screen.
Community	Click this to log into the Zyxel forum to post questions, contribute to a discussion and get feedback on Zyxel Device.
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.

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 27 Navigation Panel



To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

4.3.3 Local GUI Web Configurator Navigation Panel Menus

If your Zyxel Device is in cloud managed mode, you can use the Web Configurator for troubleshooting if your Zyxel Device cannot connect to the Internet.

The following are the screens available in the local GUI Web Configurator.

Dashboard

The dashboard displays information such as general device information, system status, Zyxel Device registration on NCC, and cloud control status in widgets that you can rearrange to suit your needs.

Maintenance Menu

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

Table 9 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Firmware Package	View the current firmware version and to upload firmware.
File Manager	Shell Script	Manage and run shell script files for the Zyxel Device.
Legal and Regulatory	Legal and Regulatory	View the legal and regulatory information of the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information.
Diagnostics	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
Log	View Log	Display log entries for the Zyxel Device.
Reboot	Reboot	Restart the Zyxel Device.

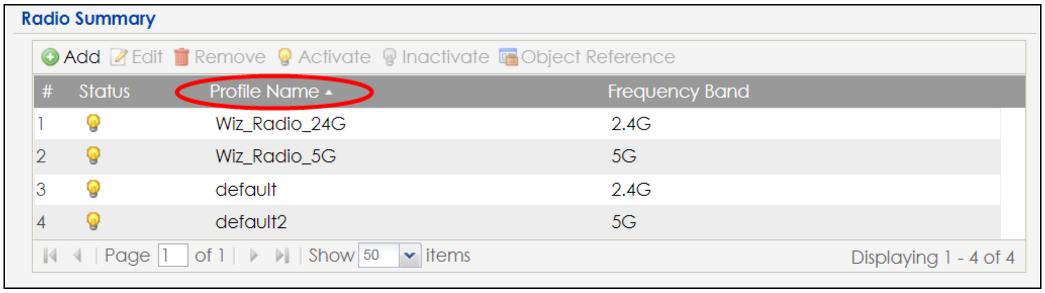
4.3.4 Tables and Lists

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

4.3.4.1 Manipulating Table Display

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

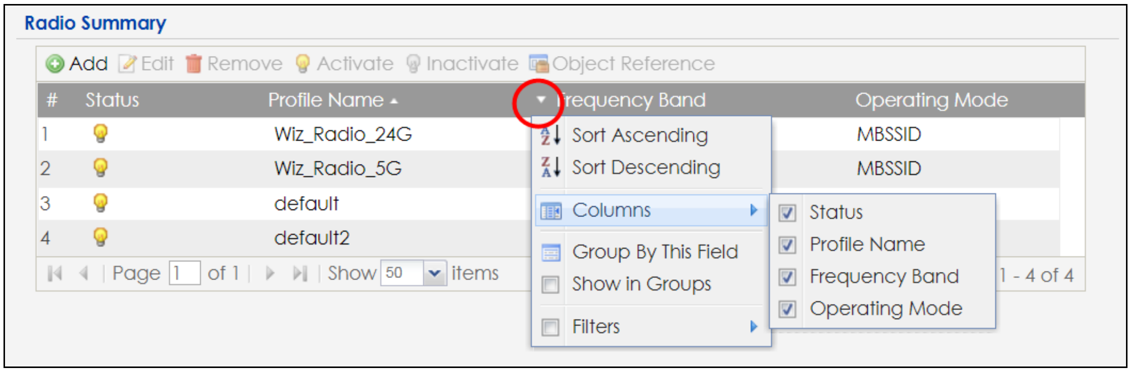
1 Click a column heading to sort the table's entries according to that column's criteria.



#	Status	Profile Name ▲	Frequency Band
1	💡	Wiz_Radio_24G	2.4G
2	💡	Wiz_Radio_5G	5G
3	💡	default	2.4G
4	💡	default2	5G

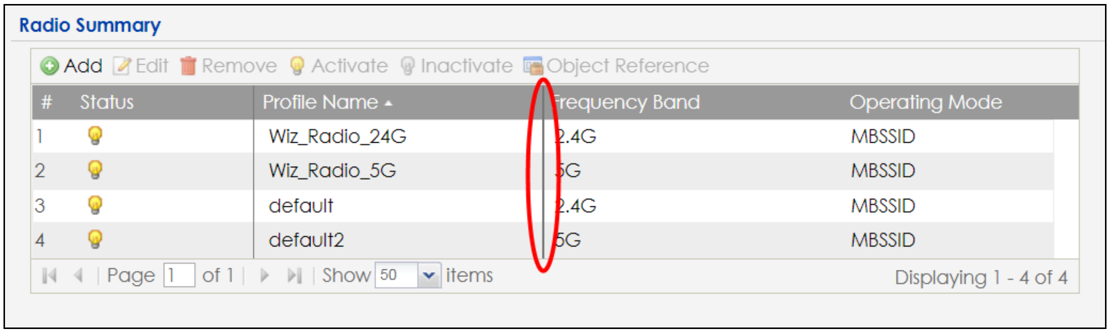
2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

- 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.



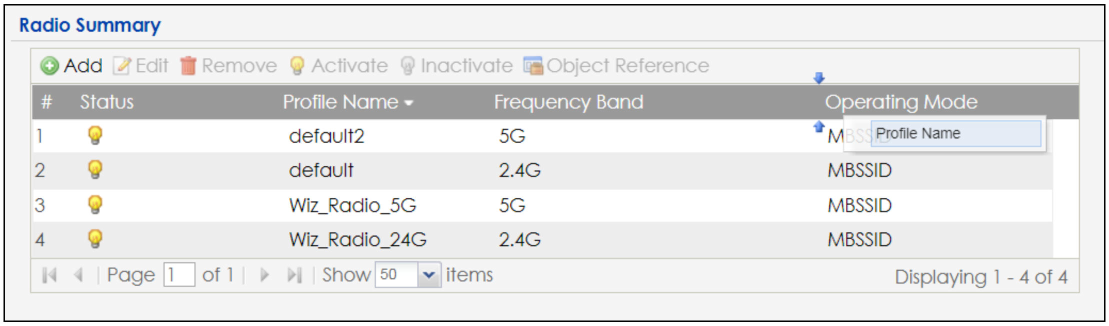
#	Status	Profile Name ▴	Frequency Band	Operating Mode
1	💡	Wiz_Radio_24G		MBSSID
2	💡	Wiz_Radio_5G		MBSSID
3	💡	default		
4	💡	default2		

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



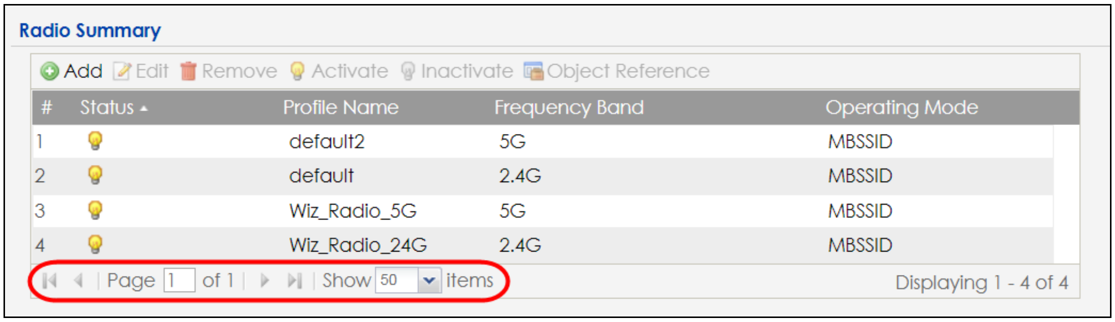
#	Status	Profile Name ▴	Frequency Band	Operating Mode
1	💡	Wiz_Radio_24G	2.4G	MBSSID
2	💡	Wiz_Radio_5G	5G	MBSSID
3	💡	default	2.4G	MBSSID
4	💡	default2	5G	MBSSID

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.



#	Status	Profile Name ▾	Frequency Band	Operating Mode
1	💡	default2	5G	MBSSID
2	💡	default	2.4G	MBSSID
3	💡	Wiz_Radio_5G	5G	MBSSID
4	💡	Wiz_Radio_24G	2.4G	MBSSID

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.



#	Status ▴	Profile Name	Frequency Band	Operating Mode
1	💡	default2	5G	MBSSID
2	💡	default	2.4G	MBSSID
3	💡	Wiz_Radio_5G	5G	MBSSID
4	💡	Wiz_Radio_24G	2.4G	MBSSID

PART I

Local Troubleshooting - Cloud Managed Mode

CHAPTER 5 Cloud Managed Mode

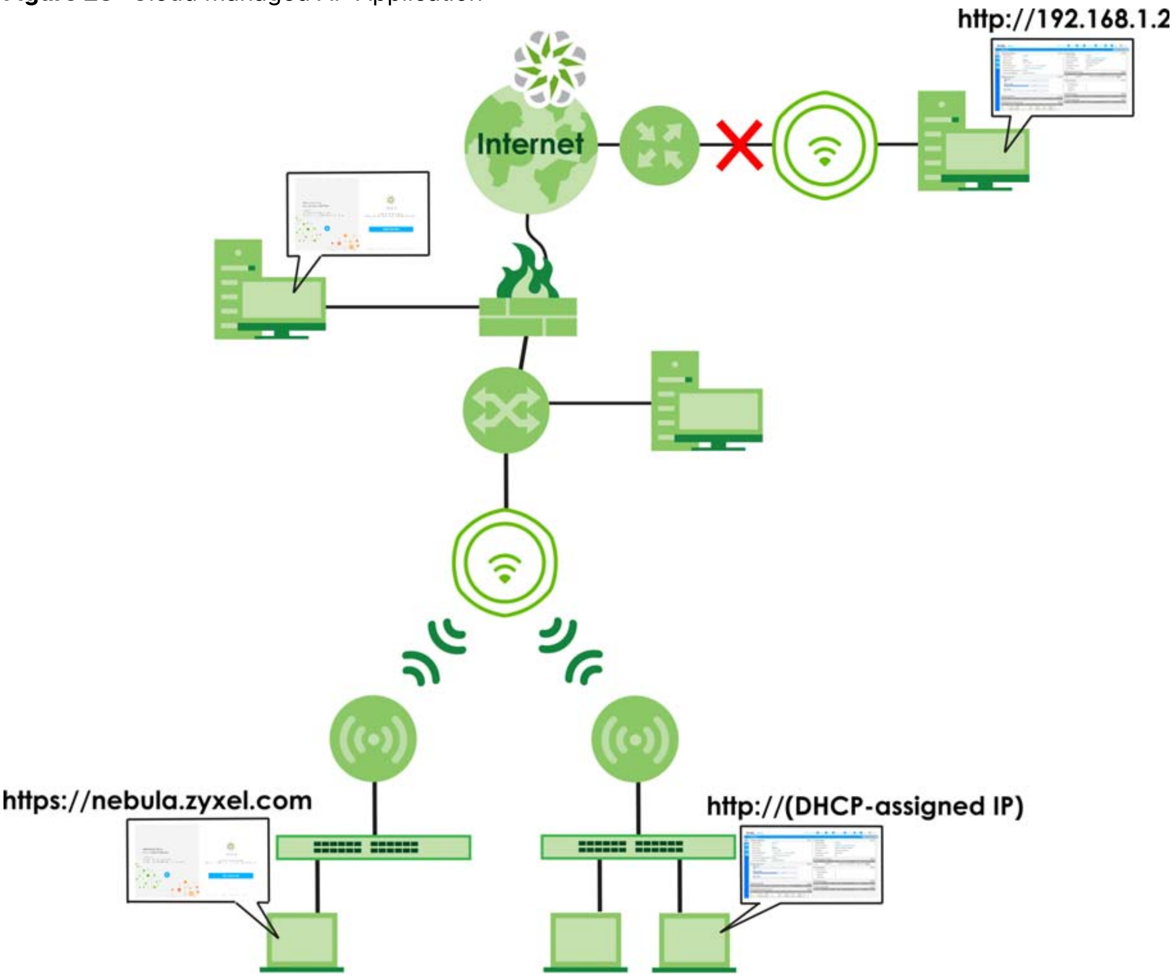
5.1 Overview

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 with the NCC.

If you cannot access the Zyxel Device from the NCC, you need to access the local GUI screens in cloud managed mode by connecting directly to the LAN port of the PoE injector of the Zyxel Device, and check if the Zyxel Device's VLAN setting or IP address has changed. To find the Zyxel Device's current LAN IP address, in NCC, go to **Site-wide** > **Devices** > **Access points** screen or the gateway to which the AP is connected.

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 28 Cloud Managed AP Application



5.2 Local GUI Screens in Cloud Managed Mode

When your Zyxel Device is managed by NCC, you can access only the following screens through the Web Configurator:

- **Dashboard**
- **Maintenance** > **File Manager** > **Firmware Package**
- **Maintenance** > **File Manager** > **Shell Script**
- **Maintenance** > **Legal and Regulatory** > **Legal and Regulatory**
- **Maintenance** > **Diagnostics** > **Diagnostics**
- **Maintenance** > **Diagnostics** > **Remote Capture**
- **Maintenance** > **Log** > **View Log**
- **Maintenance** > **Reboot** > **Reboot**

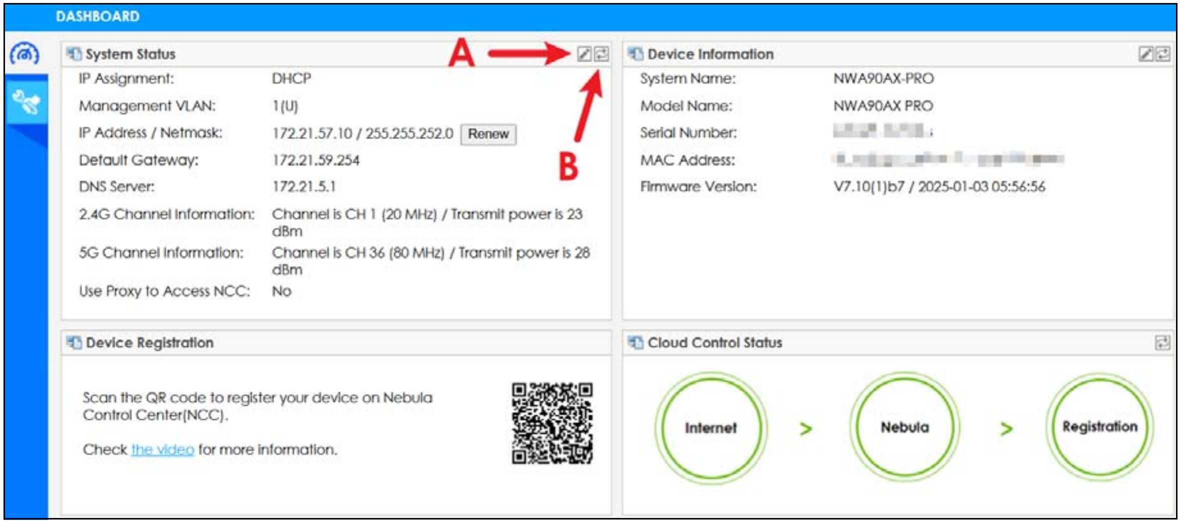
CHAPTER 6 Dashboard

6.1 Overview

This screen displays general AP information, and NCC information in widgets that you can rearrange to suit your needs. You can also edit and refresh individual widgets.

These screens also have fewer options. The rest of the Zyxel Device’s features must be configured through NCC.

Figure 29 Dashboard



System Status

IP Assignment:	DHCP
Management VLAN:	1(U)
IP Address / Netmask:	172.21.57.10 / 255.255.252.0
Default Gateway:	172.21.59.254
DNS Server:	172.21.5.1
2.4G Channel Information:	Channel is CH 1 (20 MHz) / Transmit power is 23 dBm
5G Channel Information:	Channel is CH 36 (80 MHz) / Transmit power is 28 dBm
Use Proxy to Access NCC:	No

Device Information

System Name:	NWA90AX-PRO
Model Name:	NWA90AX PRO
Serial Number:	[redacted]
MAC Address:	[redacted]
Firmware Version:	V7.10(1)b7 / 2025-01-03 05:56:56

Device Registration

Scan the QR code to register your device on Nebula Control Center(NCC).

Check the video for more information.

Cloud Control Status

The following table describes the labels in this screen.

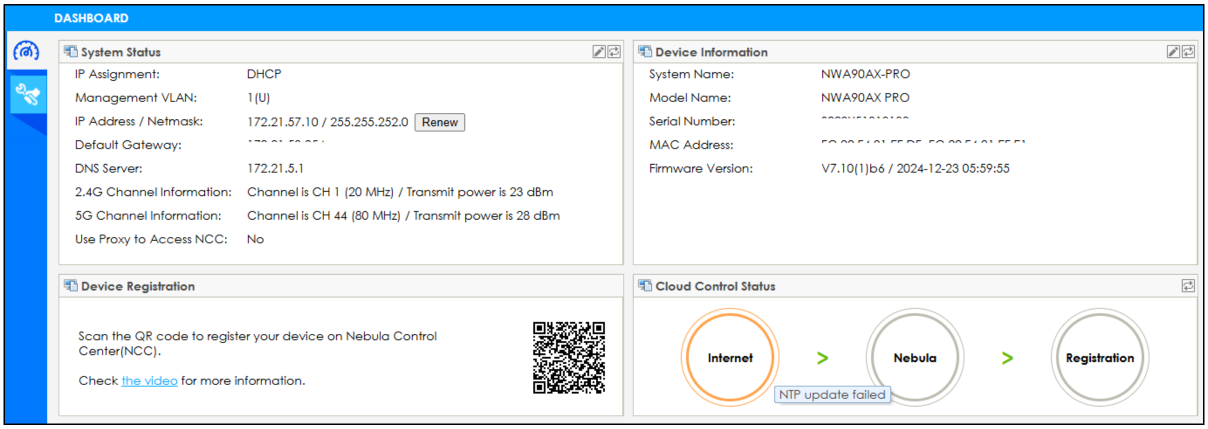
Table 10 Dashboard

LABEL	DESCRIPTION
Edit (A)	Click this to open the setup window to configure settings such as the IP address, VLAN, system name, and other network parameters.
Refresh Now (B)	Click this to update the widget’s information immediately.
System Status	
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.
Management VLAN	This field displays the management VLAN ID for the Zyxel Device.

Table 10 Dashboard (continued)

LABEL	DESCRIPTION
IP Address / 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 through DHCP. If the interface has a dynamic IP address, click **Renew** to update the IP address for the interface.
Default Gateway	This field displays the IP address of the default outgoing gateway.
DNS Server	This field display the IP address of the DNS server.
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.
6G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 6 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
Use Proxy to Access NCC	This displays whether the Zyxel Device uses a proxy server to access the NCC.
Device Information	
System Name	This field displays the name used to identify the Zyxel Device on any network.
Model Name	This field displays the model name of this Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
MAC Address	This field displays the MAC address of the Zyxel Device.
Firmware Version	This field displays the firmware version of the Zyxel Device.
Device Registration	This field displays the information on NCC registration.
Cloud Control Status	This field displays: • The Zyxel Device Internet connection status. • The connection status between the Zyxel Device and NCC. • The Zyxel Device registration status on NCC. Mouse over the circles to display detailed information. To pass your Zyxel Device management to NCC, first make sure your Zyxel Device is connected to the Internet. Then go to NCC and register your Zyxel Device. **1. Internet** Green – The Zyxel Device is connected to the Internet. Orange – The Zyxel Device is not connected to the Internet. **2. Nebula** Green – The Zyxel Device is connected to NCC. Orange – The Zyxel Device is not connected to NCC. **3. Registration** Green – The Zyxel Device is registered on NCC. Gray – The Zyxel Device is not registered on NCC.

If the Zyxel Device cannot connect to the Internet or to NCC, move the mouse over the status circle to check the error message. See the NCC (Nebula Control Center) User’s Guide for more information.



DASHBOARD

System Status

IP Assignment:	DHCP
Management VLAN:	1 (U)
IP Address / Netmask:	172.21.57.10 / 255.255.252.0 Renew
Default Gateway:	[redacted]
DNS Server:	172.21.5.1
2.4G Channel Information:	Channel is CH 1 (20 MHz) / Transmit power is 23 dBm
5G Channel Information:	Channel is CH 44 (80 MHz) / Transmit power is 28 dBm
Use Proxy to Access NCC:	No

Device Information

System Name:	NWA90AX-PRO
Model Name:	NWA90AX PRO
Serial Number:	[redacted]
MAC Address:	[redacted]
Firmware Version:	V7.10(1)b6 / 2024-12-23 05:59:55

Device Registration

Scan the QR code to register your device on Nebula Control Center(NCC).

Check the video for more information.

Cloud Control Status

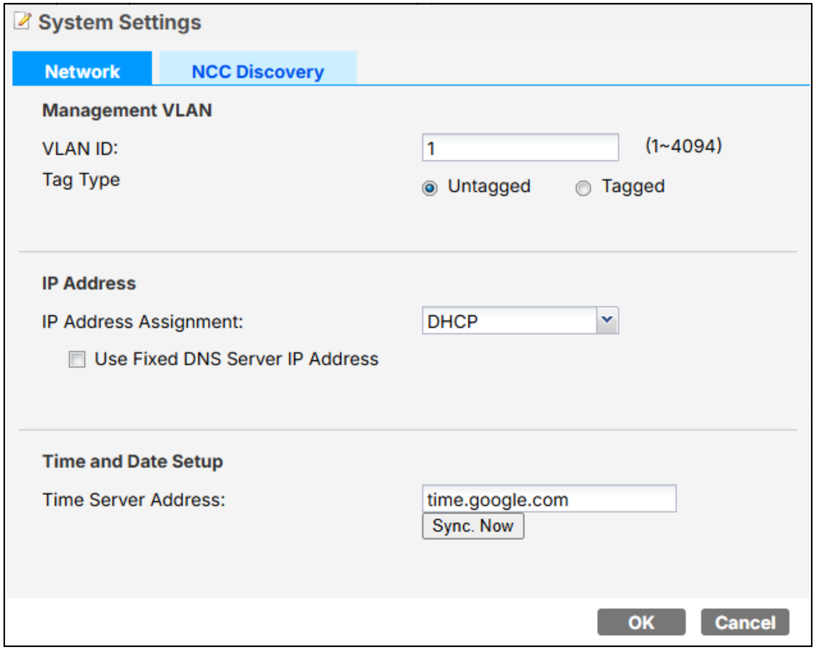
6.2 Edit System Status

Use this screen to configure the Zyxel Device's network setting and allow a proxy to access NCC.

6.2.1 Network

Use this screen to configure the VLAN ID, IP address and time server. To access this screen, click **Dashboard** > Edit (**System Status**) > **Network**.

Figure 30 Dashboard > Edit (System Status) > Network



System Settings

Management VLAN

VLAN ID: 1 (1~4094)

Tag Type ● Untagged ○ Tagged

IP Address

IP Address Assignment: DHCP

□ Use Fixed DNS Server IP Address

Time and Date Setup

Time Server Address: time.google.com

Each field is described in the following table.

Table 11 Dashboard > Edit (System Status) > Network

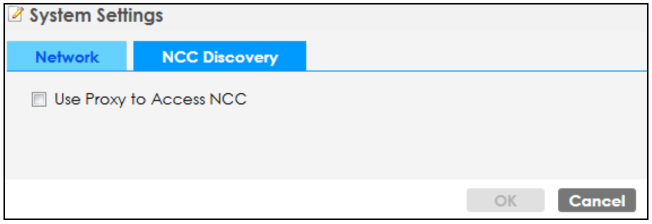
LABEL	DESCRIPTION
Management VLAN	
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID. Make sure your VLAN settings allow the Zyxel Device to connect to the Internet so you could manage it with NCC.
Tag Type	Select **tagged** to make the Zyxel Device adds the Management VLAN ID to outbound traffic transmitted through its Ethernet port. If you select **Untagged**, the outbound traffic transmitted through the Zyxel Device Ethernet port will NOT be tagged with the Management VLAN ID.
IP Address	
IP Address Assignment	Select **DHCP** to make the interface a DHCP client and automatically get the IP address, subnet mask, gateway and DNS Server IP address from a DHCP server. Select **Static IP** to specify the IP address, subnet mask, gateway and DNS server IP address manually.
Use Fixed DNS Server IP Address	Select this if you have a preferred DNS server that you want to specify manually even if the IP type is DHCP. Setting a fixed DNS server IP address may help if you experience unreliable DNS resolution.
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.
Time and Date Setup	
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 the time server (see the **Time Server Address** field). This also saves your changes.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

6.2.2 NCC Discovery

Use this screen to allow a proxy to access NCC. To access this screen, click **Dashboard** > Edit (**System Status**) > **NCC Discovery**.

Select the checkbox and click **OK** so that the Zyxel Device can access the NCC through the proxy server.

Figure 31 Dashboard > Edit (System Status) > NCC Discovery

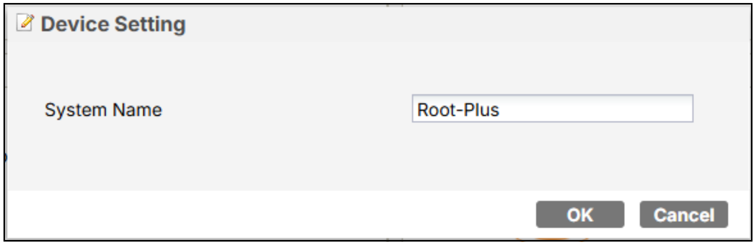


6.3 Edit Device Information

Use this screen to configure the Zyxel Device’s system name. To access this screen, click **Dashboard** > Edit (**Device Information**).

Enter the system name and click **OK** to save the change.

Figure 32 Dashboard > Edit (Device Information)



Device Setting

System Name: Root-Plus

CHAPTER 7 Maintenance

7.1 Overview

When the Zyxel Device is set to work in cloud managed mode, the **Maintenance** screens allow you to upload firmware, manage shell script files, generate a diagnostic file, view log messages, or reboot the Zyxel Device.

7.1.1 What You Can Do in this Chapter

- The **File Manager** > **Firmware Package** screen (Firmware Package) displays current firmware information and allows you to upload firmware file.
- The **File Manager** > **Shell Script** screen (Shell Script) allows you to store, name, download, and upload shell script files.
- The **Legal and Regulatory** > **Legal and Regulatory** screen (Legal and Regulatory) allows you to view the legal and regulatory information.
- The **Diagnostics** > **Diagnostics** screen (Diagnostics) allows you to generate a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Diagnostics** > **Remote Capture** screen (Remote Capture) allows you to enable remote packet captures on wired or wireless interfaces through an external packet analyzer.
- The **Log** > **View Log** screen (View Log) displays the Zyxel Device's current log messages when it is disconnected from the NCC.
- The **Reboot** > **Reboot** screen (Reboot) allows you to reboot the Zyxel Device.

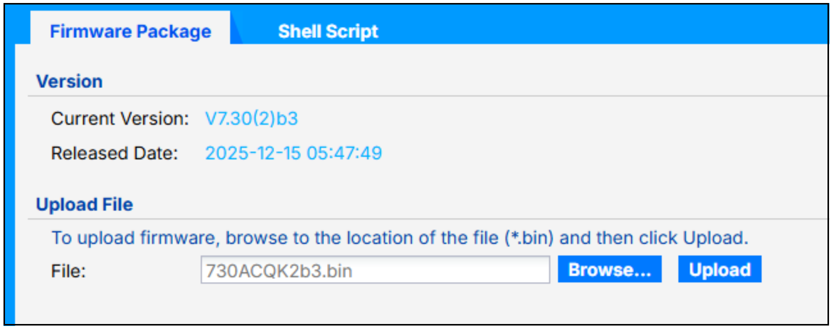
7.2 Firmware Package

Click **Maintenance** > **File Manager** > **Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware information and upload firmware to the Zyxel Device. You can manually download the new firmware from the Zyxel website.

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.

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 33 Maintenance > File Manager > Firmware Package



Version

Current Version: V7.30(2)b3

Released Date: 2025-12-15 05:47:49

Upload File

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File: 730ACQK2b3.bin

The following table describes the labels in this screen.

Table 12 Maintenance > File Manager > Firmware Package

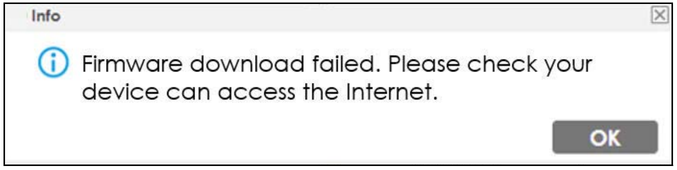
LABEL	DESCRIPTION
Version	
Current Version	This is the firmware version.
Released Date	This is the date that the version of the firmware was created.
Upload File	
File Path	Enter the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** 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.

Firmware Download Failed

The following pop-up messages display the causes and solutions for firmware download failure.

Firmware download failed due to an Internet error. Refer to Internet Access for more information.

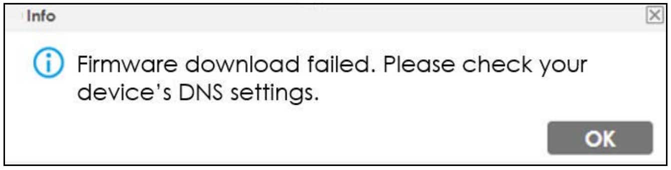
Figure 34 Firmware Download Failed. Check Internet Access



Firmware download failed. Please check your device can access the Internet.

Firmware download failed due to a DNS problem. Please check your device's DNS settings.

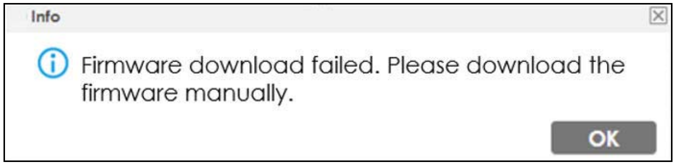
Figure 35 Firmware Download failed. Check DNS Setting



Firmware download failed. Please check your device’s DNS settings.

Firmware download failed. Download the new firmware manually from the Zyxel website. Then, go to the **Maintenance** > **File Manager** > **Firmware Package** screen to upload the new firmware.

Figure 36 Firmware Download Failed. Download Manually



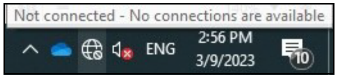
Info

Firmware download failed. Please download the firmware manually.

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

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

Figure 37 Network Temporarily Disconnected



Not connected - No connections are available

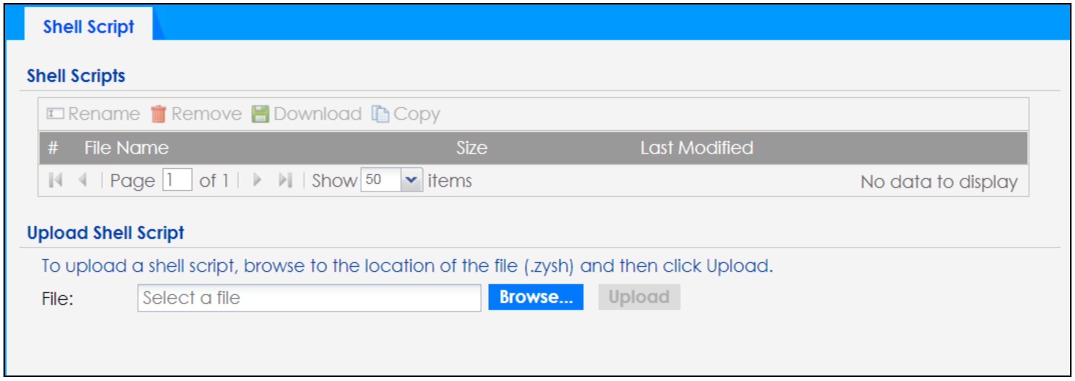
After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

7.3 Shell Script

A shell script is a list of commands to manage the Zyxel Device. Use a text editor to create the shell script files. They must use a ".zysh" filename extension. For example, test.zysh.

Click **Maintenance** > **File Manager** > **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 38 Maintenance > File Manager > Shell Script



Shell Scripts

#	File Name	Size	Last Modified

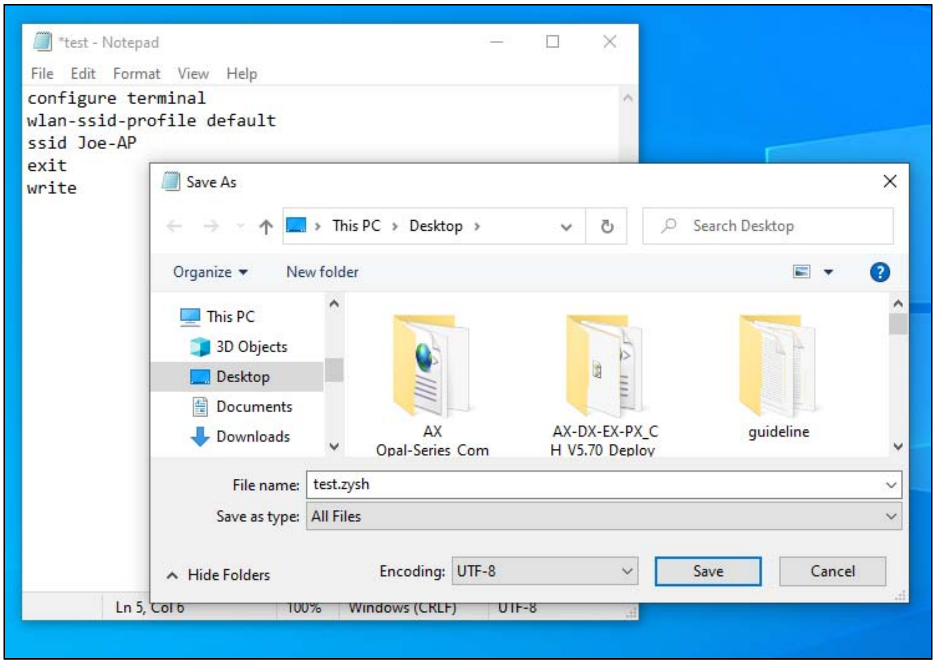
No data to display

Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

File: Select a file

1 In the text editor, save the shell script with a .zysh filename extension. Select **All Files** as the file type.



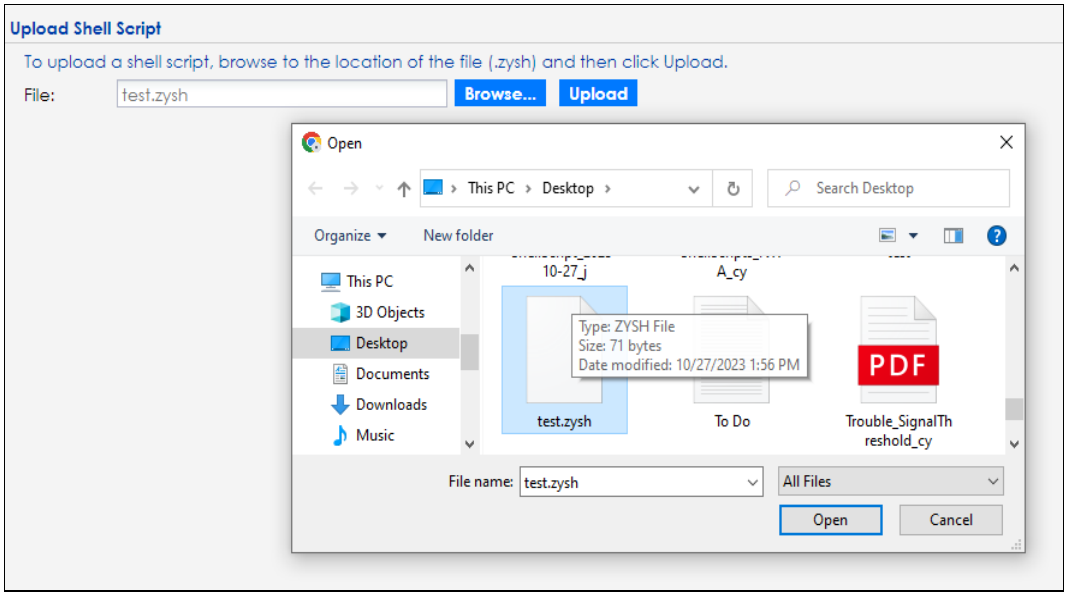
```
configure terminal
wlan-ssid-profile default
ssid Joe-AP
exit
write
```

File name: test.zysh

Save as type: All Files

Encoding: UTF-8

2 Go to the **Maintenance** > **File Manager** > **Shell Script** screen. Click **Browse...** to upload the .zysh file.



Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

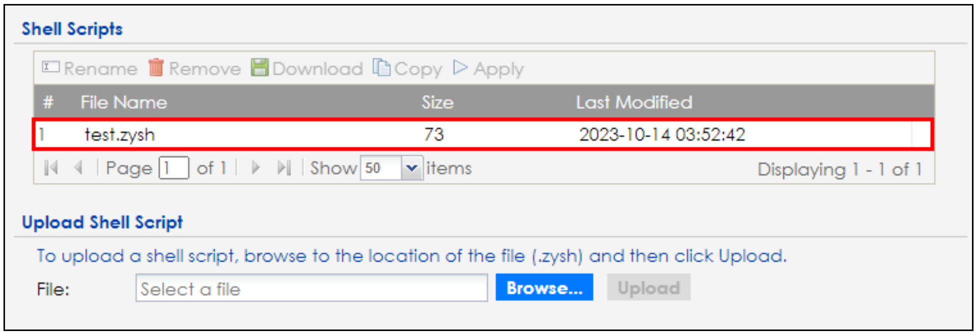
File: test.zysh

Type: ZYSH File
Size: 71 bytes
Date modified: 10/27/2023 1:56 PM

File name: test.zysh

All Files

3 Click **Upload**. The uploaded shell script will be shown in the **Shell Scripts** field.



#	File Name	Size	Last Modified
1	test.zysh	73	2023-10-14 03:52:42

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

File: Select a file

Each field is described in the following table.

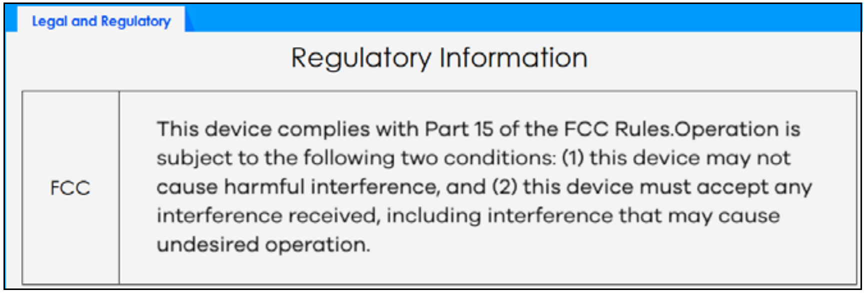
Table 13 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Shell Scripts	
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 the following characters inside the square brackets [a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-)]. Click **OK** to save the renamed file or click **Cancel** to close the screen without saving a renamed file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters, including the following characters inside the square brackets [a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-)]. 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	
File	Enter 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.

7.4 Legal and Regulatory

Use this screen to view the information on legal and regulatory. This screen may not display depending on the Zyxel Device model you are using.

Figure 39 Maintenance > Legal and Regulatory > Legal and Regulatory



Regulatory Information

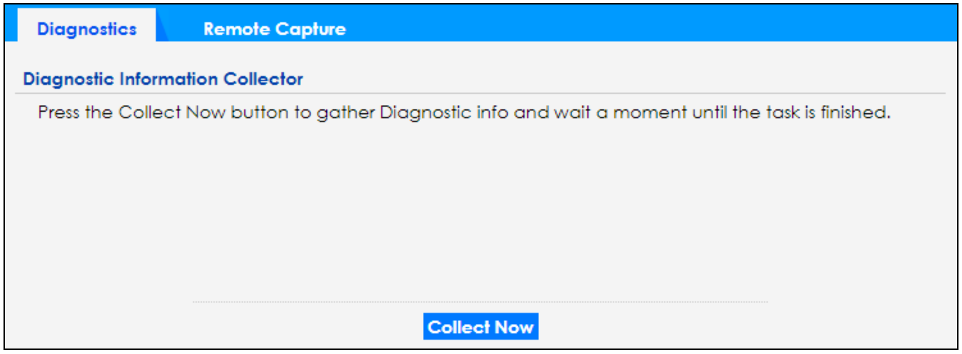
FCC	This device complies with Part 15 of the FCC Rules.Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

7.5 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.

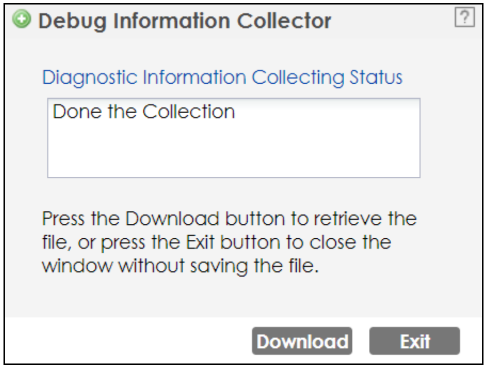
Figure 40 Maintenance > Diagnostics > Diagnostics



Press the Collect Now button to gather Diagnostic info and wait a moment until the task is finished.

The **Debug Information Collector** 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 41 Maintenance > Diagnostics > Diagnostics: Debug Information Collector



Debug Information Collector

Diagnostic Information Collecting Status

Done the Collection

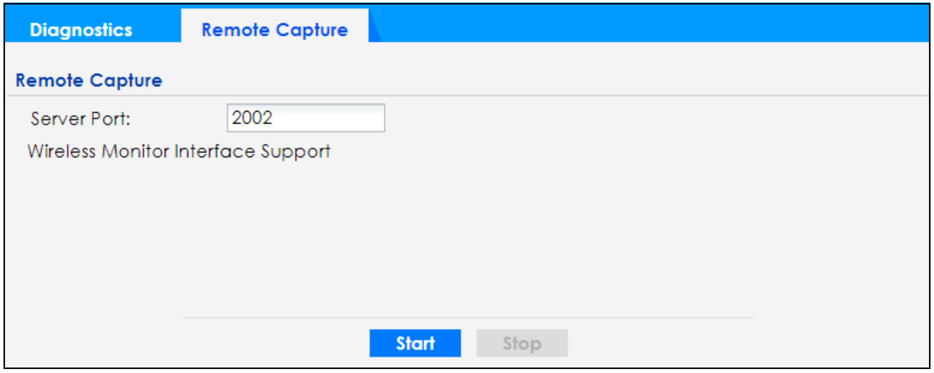
Press the Download button to retrieve the file, or press the Exit button to close the window without saving the file.

7.6 Remote Capture

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

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

Figure 42 Maintenance > Diagnostics > Remote Capture



Remote Capture

Server Port: 2002

Wireless Monitor Interface Support

The following table describes the labels in this screen.

Table 14 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.

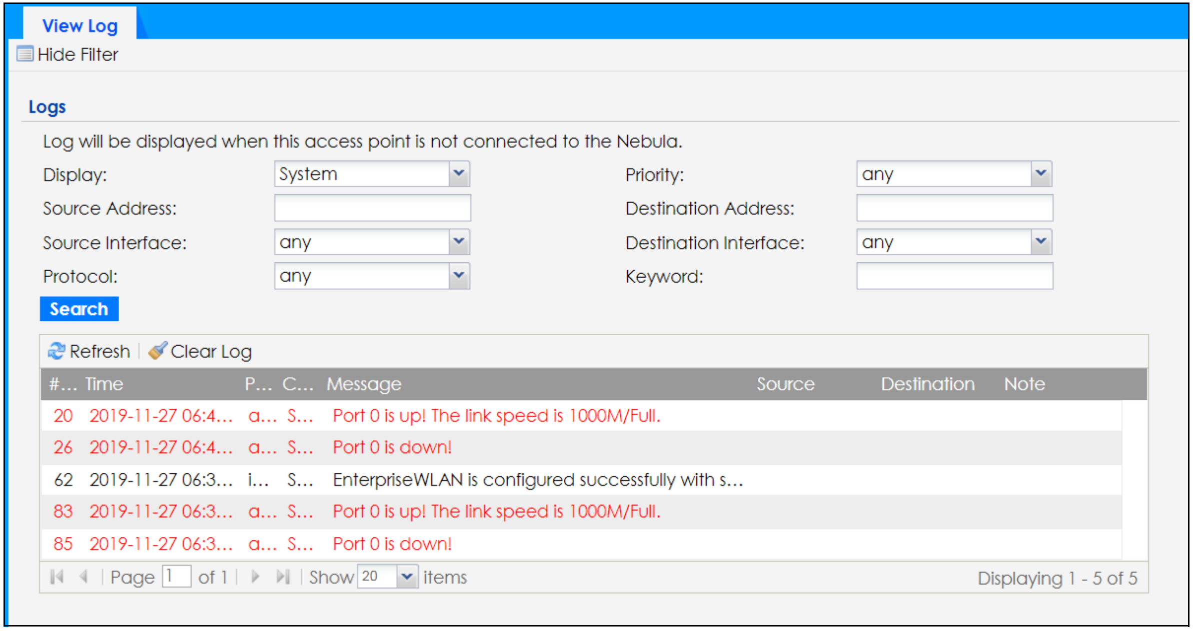
7.7 View Log

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** > **View 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 43 Maintenance > Log > View Log



Log will be displayed when this access point is not connected to the Nebula.

Display:	System	Priority:	any
Source Address:		Destination Address:	
Source Interface:	any	Destination Interface:	any
Protocol:	any	Keyword:	

#...	Time	P...	C...	Message	Source	Destination	Note
20	2019-11-27 06:4...	a...	S...	Port 0 is up! The link speed is 1000M/Full.			
26	2019-11-27 06:4...	a...	S...	Port 0 is down!			
62	2019-11-27 06:3...	i...	S...	EnterpriseWLAN is configured successfully with s...			
83	2019-11-27 06:3...	a...	S...	Port 0 is up! The link speed is 1000M/Full.			
85	2019-11-27 06:3...	a...	S...	Port 0 is down!			

The following table describes the labels in this screen.

Table 15 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** field is 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 **Display** is **Debug Log**.
Source Address	This displays when you show the filter. Enter the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.

Table 15 Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
Destination Address	This displays when you show the filter. Enter 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. Enter 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.
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.

7.8 Reboot

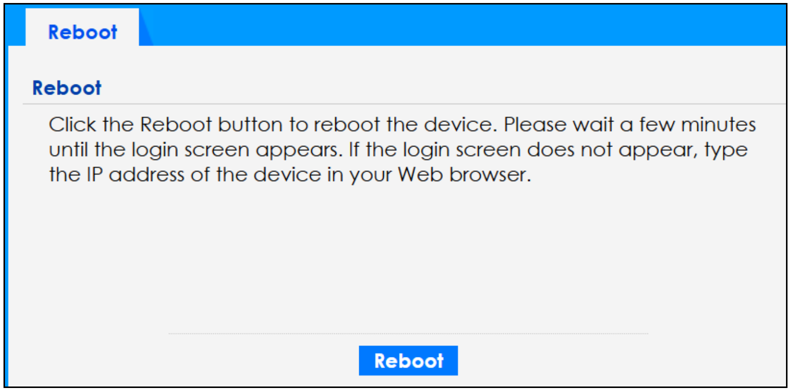
This screen allows users to restart the Zyxel Device. To access this screen, click **Maintenance** > **Reboot** > **Reboot**.

If you made changes in the CLI, you have to use the `write` command to save the configuration. They do not change when you reboot the Zyxel Device.

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

You can reboot your Zyxel Device when the Internet connection is slow or intermittent.

Figure 44 Maintenance > Reboot > Reboot



Click the Reboot button to reboot the device. Please wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

The following table describes the labels in this screen.

Table 16 Maintenance > Reboot > Reboot

LABEL	DESCRIPTION
Reboot	Click **Reboot** then click **Yes** to restart the Zyxel Device immediately.

After the Zyxel Device reboots, 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.

Part II

Appendices and Troubleshooting

CHAPTER 8 Troubleshooting

8.1 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 LEDs
- Zyxel Device Management, Access, and Login
- Internet Access
- WiFi Network
- Resetting the Zyxel Device

8.2 Power, Hardware Connections, and LEDs

The Zyxel Device does not turn on. None of the LEDs turn on.

If you are using a power adapter to power the Zyxel Device:

1. Make sure you are using a compatible power adapter.
2. Make sure the power adapter is securely connected to the Zyxel Device and plugged into an appropriate power source.
3. Make sure the power adapter is functional.
4. If the problem persists, contact Zyxel technical support.

If you are using a PSE or PoE injector to power the Zyxel Device:

1. Make sure you are using the correct PoE port on the PSE or PoE injector.
2. Make sure the PSE or PoE injector is functional.
   - Check whether the PSE or PoE injector is malfunctioning. See your PSE or PoE injector user's guide for more information.
   - If the connected PSE or PoE injector does not fully comply with the Zyxel Device's supported PoE standard, replace it with compliant PSE or PoE injector. See PoE for the Zyxel Device's supported PoE standards. Certain PSEs can adjust the power delivered to each PD based on the PoE standard supported by the PD. For detailed instructions, refer to your PSE User's Guide.

3 Make sure the Ethernet cable connected to the PSE or PoE injector is functional.

- Check whether the Ethernet cable is malfunctioning.
- Use the correct type of Ethernet cable for the PoE standard supported by the Zyxel Device. See PoE for the Zyxel Device's supported PoE standards and see PoE Standards for the compliant Ethernet cables.

4 If the problem persists, contact Zyxel technical support.

The LED does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Zyxel Device LED.

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.

8.3 Zyxel Device Management, Access, and Login

I forgot the IP address for the Zyxel Device.

1 The default in-band IP address for the local GUI Web Configurator in Nebula Cloud-managed mode is **https://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 Resetting the Zyxel Device.

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 **Site-wide** > **Devices** > **Access points** 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 (for the local GUI Web Configurator in Nebula Cloud-managed 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 Zyxel Device LED.

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. Check the DHCP IP address assigned to your Zyxel Device on the connected router.
- 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 Resetting the Zyxel Device.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Zyxel Device using another service, such as SSH. If you can access the Zyxel Device, check the remote management settings to find out why the Zyxel Device does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to the **Ethernet PoE** port.

I forgot the Web Configurator password.

1 The default password is unique to each Zyxel Device and shown on the label. 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 Resetting the Zyxel Device.

I can see the **Login** screen, but I cannot log into the Zyxel Device.

1 Clear your browser's cache.

2 Check the Zyxel Device's management mode.

- The default password is unique to each Zyxel Device and shown on the label. If you have changed the username and password, use the ones you configured to log in.
- If the Zyxel Device is in cloud managed mode, use the Nebula **Local credentials Password** to log into the cloud managed mode local GUI. The **Local credentials Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration**: **Local credentials**: **Password** in the NCC portal.

- If the Zyxel Device is managed by an APC such as the ZyWALL, then use the APC to manage the Zyxel Device.

3 Depending on your Zyxel Device's management mode, make sure you have entered the correct user name and password. These fields are case-sensitive, so check if [Caps Lock] is on or off.

Note: Steps 1 and 2 are applicable if you get an "Invalid password" error message when using some functions in the ZON utility. See Zyxel One Network (ZON) Utility for more information.

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

5 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Resetting the Zyxel Device.

I cannot upload the firmware uploaded using FTP.

Using the NCC is the recommended method for uploading firmware. Or, use the local GUI Web Configurator in Nebula Cloud-managed mode for uploading firmware. 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.

NCC is managing the Zyxel Device, but the NCC cannot access the Zyxel Device.

Connect to the Zyxel Device directly and log into the Web Configurator with the credentials configured in NCC.

I cannot register the Zyxel Device in NCC because it is already registered by the previous owner.

- If the previous owner has registered the Zyxel Device in NCC and has enabled the NCC **Override device ownership** feature in the **Organization-wide** > **Organization-wide manage** > **Organization settings** screen, use the Nebula Mobile app to scan the NCC QR code on the back label of the Zyxel Device to register with NCC.
- If the previous owner has registered it in NCC and has locked the Zyxel Device with the NCC **Override device ownership** feature in the **Organization-wide** > **Organization-wide manage** > **Organization settings** screen, inform the previous owner to unregister the Zyxel Device or contact Zyxel technical support.

The Zyxel Device is already registered with NCC, but it is still in the default non Nebula cloud-managed mode; it cannot connect to the NCC.

1 Check the Zyxel Device LED and make sure the Zyxel Device is on and ready for use.

2 Check your network's firewall/security settings. Make sure the following ports are allowed:

- TCP: 443, 4335, and 6667
- UDP: 123 is allowed.

3 Make sure your Zyxel Device has obtained an IP address and can access the Internet. Check the **Cloud Control Status** on the **Dashboard** screen for your Internet connection.

4 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.

6 Make sure your DNS server can resolve d.nebula.zyxel.com. Open the **Command Prompt** on your computer, enter *nslookup d.nebula.zyxel.com*, see if the DNS server can return the resolved IP address. If not, you can try set your gateway to use the Google Public DNS server 8.8.8.8.

Some features I set using the NCC do not work as expected.

1 Make sure your Zyxel Device can access the Internet.

2 Make sure the NCC can access the Zyxel Device. 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 to 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, 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.

8.4 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 Zyxel Device LED). See the Quick Start Guide.
2. Make sure the Zyxel Device is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
3. If clients are trying to access the Internet wirelessly, make sure the WiFi settings on the WiFi clients are the same as the settings on the Zyxel Device.
4. Make sure the Zyxel Device has the same VLAN settings configured as the gateway connected to the Zyxel Device. Traffic tagged with a specific VLAN ID tag can only go to the WiFi clients of the WiFi network that uses the same VLAN ID. Devices connected to the Zyxel Device need to have the same VLAN ID configured to receive traffic from the Zyxel Device.
5. Disconnect all the cables from your Zyxel Device, and follow the directions in the Quick Start Guide again.
6. Reboot the client and reconnect to the Zyxel Device.
7. 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 Zyxel Device LED. 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, or the 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 APC.

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.

8.5 WiFi Network

The WiFi connection is slow or intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your WiFi device closer to the Zyxel Device if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the wireless client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

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 over the setting in the Zyxel Device. 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.

8.6 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 using the local GUI Web Configurator's default settings.

8.7 Getting More Troubleshooting Help

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

Appendix A
Importing a Certificate

When you connect to the Zyxel Device Web Configurator using HTTPS, a warning page “Your connection is not private” may show up. If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the website.

This appendix shows you how to import a public key certificate into your web browser including Google Chrome, Microsoft Edge, and Mozilla Firefox.

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).

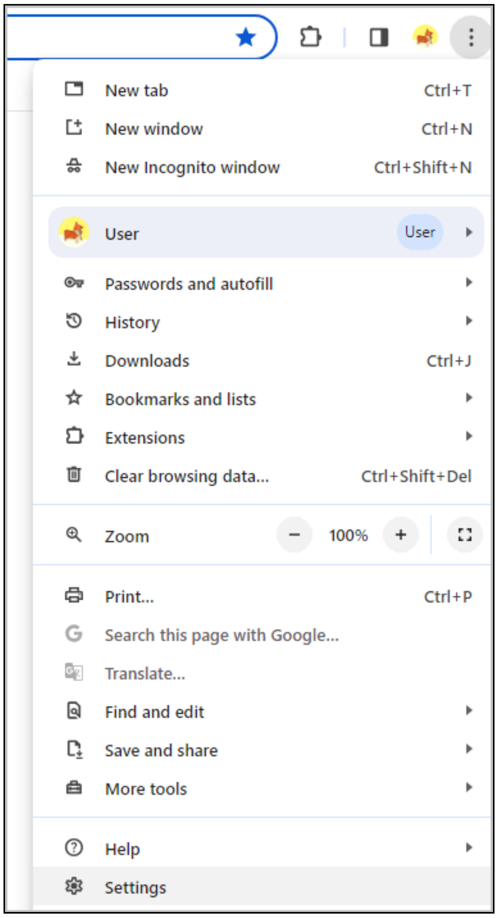
Note: You need a certificate from a trusted Certification Authority (CA) for this Zyxel Device.

Importing a Certificate to Google Chrome and Microsoft Edge

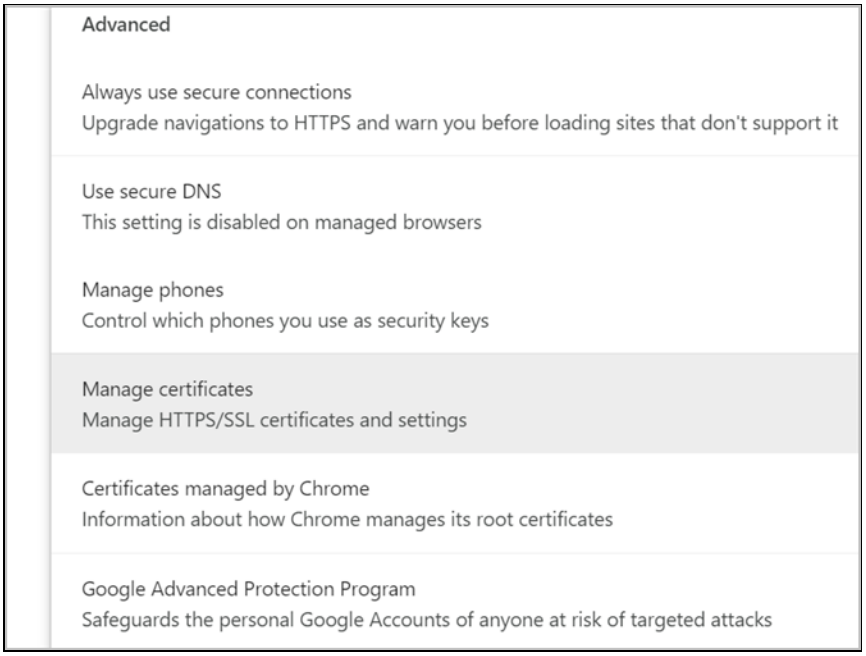
The following example uses Google Chrome on Windows 10 Pro. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

The Importing process is quite similar between Google Chrome and Microsoft Edge. The following procedures in Google Chrome can apply the same way in Microsoft Edge.

1 Open Google Chrome browser. Click the three dots on the upper right corner. Choose **Settings**.



2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates**. In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.



Advanced

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

Use secure DNS
This setting is disabled on managed browsers

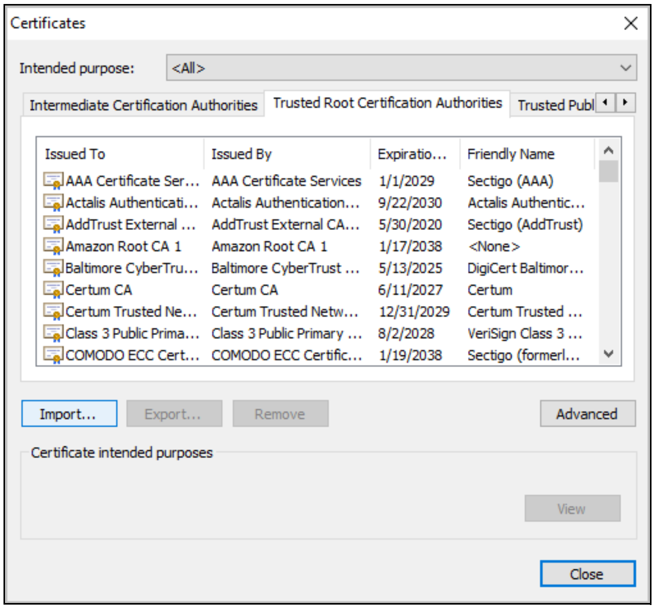
Manage phones
Control which phones you use as security keys

Manage certificates
Manage HTTPS/SSL certificates and settings

Certificates managed by Chrome
Information about how Chrome manages its root certificates

Google Advanced Protection Program
Safeguards the personal Google Accounts of anyone at risk of targeted attacks

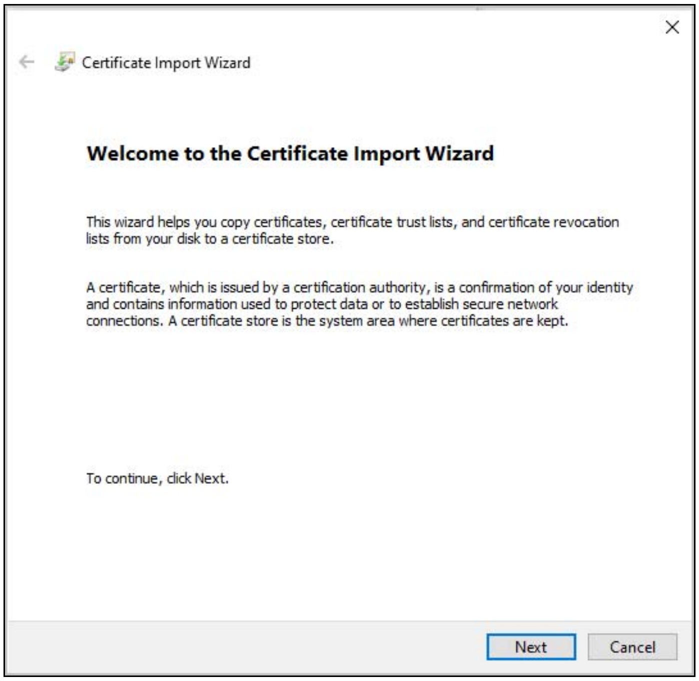
3 Select the **Trusted Root Certification Authorities** tab and click **Import**.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	1/1/2029	Sectigo (AAA)
Actalis Authenticati...	Actalis Authentication...	9/22/2030	Actalis Authentic...
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
Amazon Root CA 1	Amazon Root CA 1	1/17/2038	<None>
Baltimore CyberTru...	Baltimore CyberTrust ...	5/13/2025	DigiCert Baltimor...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
COMODO ECC Cert...	COMODO ECC Certific...	1/19/2038	Sectigo (formerl...

4 Click **Next** to proceed to the **Certificate Import Wizard**.



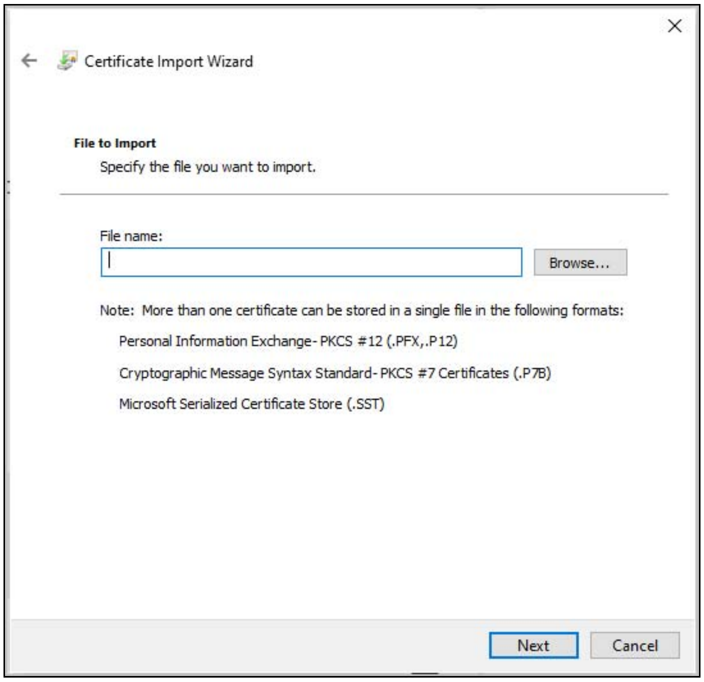
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5 Click **Browse** to select a certificate already saved in your computer and click **Next** to continue.



File to Import

Specify the file you want to import.

File name:

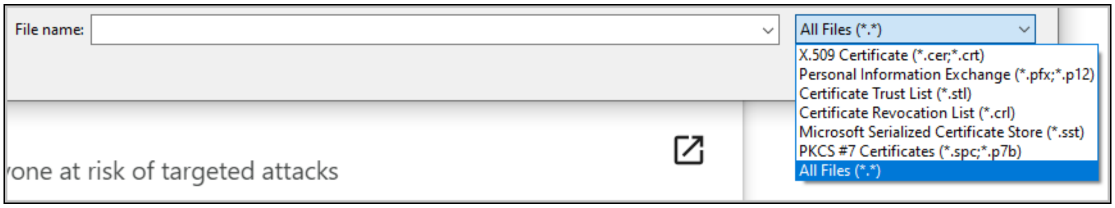
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

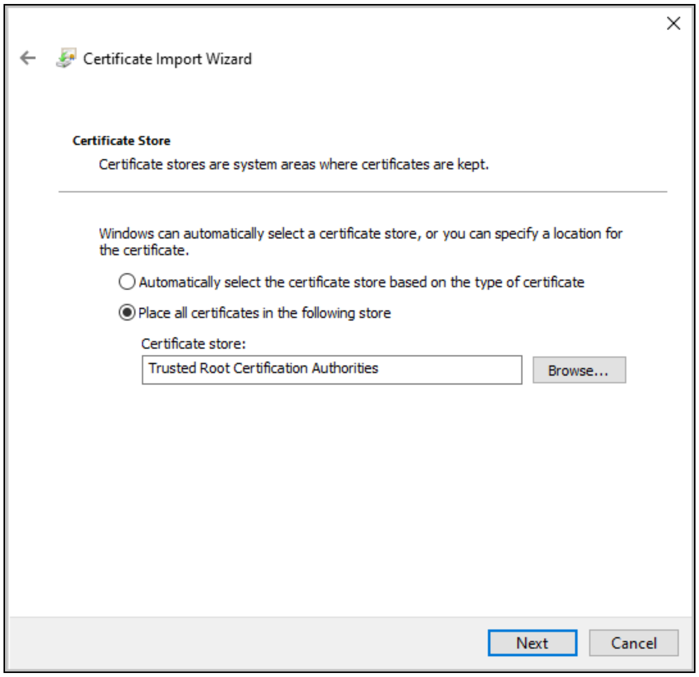
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **All Files** to find the certificate in your computer.


File name:
All Files (*.*)
X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p12)
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.sst)
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)
one at risk of targeted attacks

6 Two options are available for certificate stores. One is **Automatically select the certificate store based on the type of certificate**. This means the certificate import wizard can identify from the certificate whether it is a CA certificate or a personal certificate, and install it into the appropriate certificate store. The other option is **Place all certificates in the following store.** With this option, you can choose the desired folder for the certificate store. After selection, click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

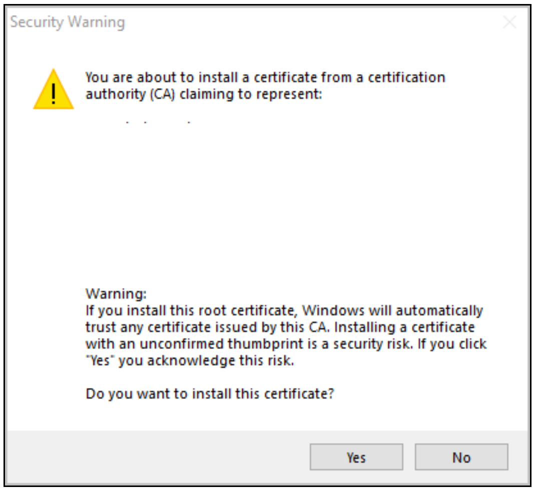
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

7 The security warning message shows up and click **Yes**.



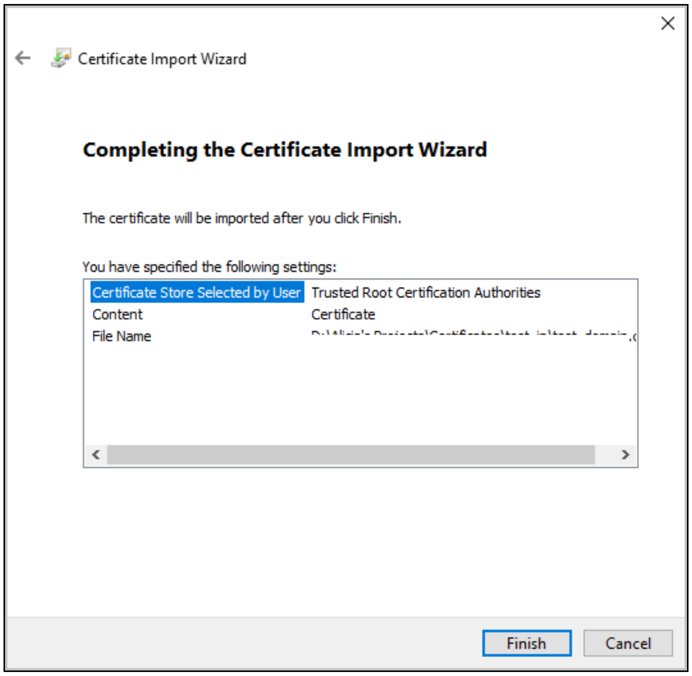
Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

8 Click **Finish**.



Certificate Import Wizard

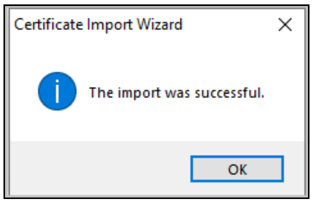
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	D:\Alicia's Projects\Certificates\test_in\test_domain.c

When you click **Finish,** a pop-up screen informs you about import completion.



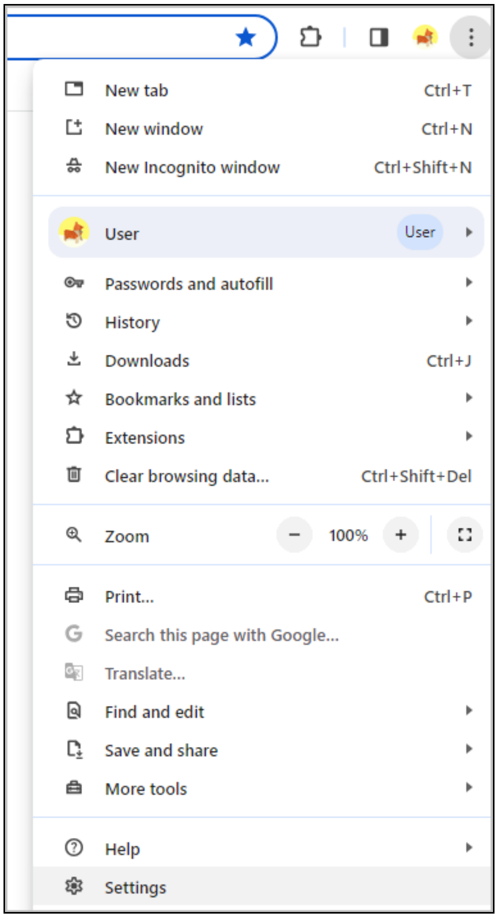
Certificate Import Wizard

The import was successful.

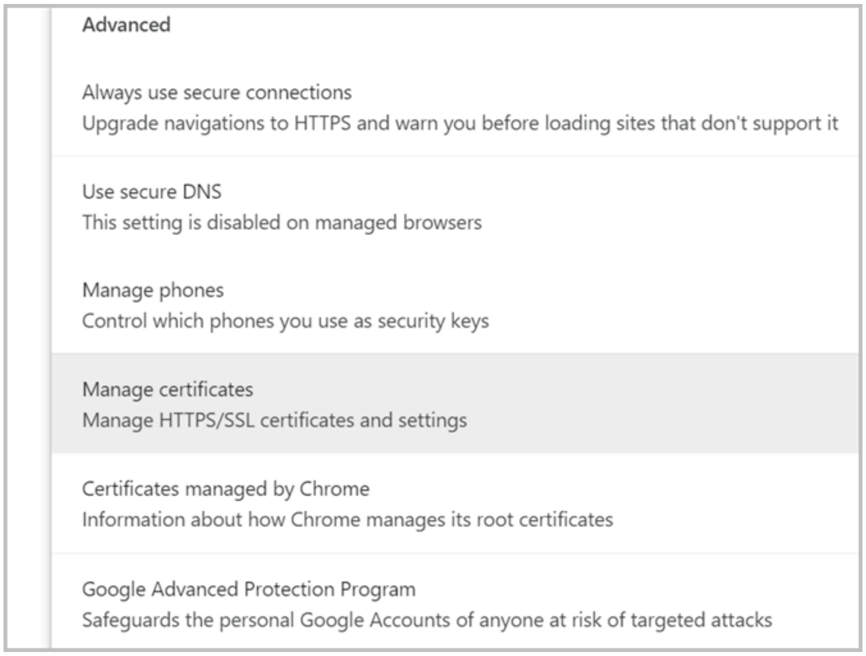
Remove a Certificate in Google Chrome and Microsoft Edge

This section shows you how to remove a public key certificate in Google Chrome and Microsoft Edge on Windows 10 Pro.

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



2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates.** In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates.**


Advanced

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

Use secure DNS
This setting is disabled on managed browsers

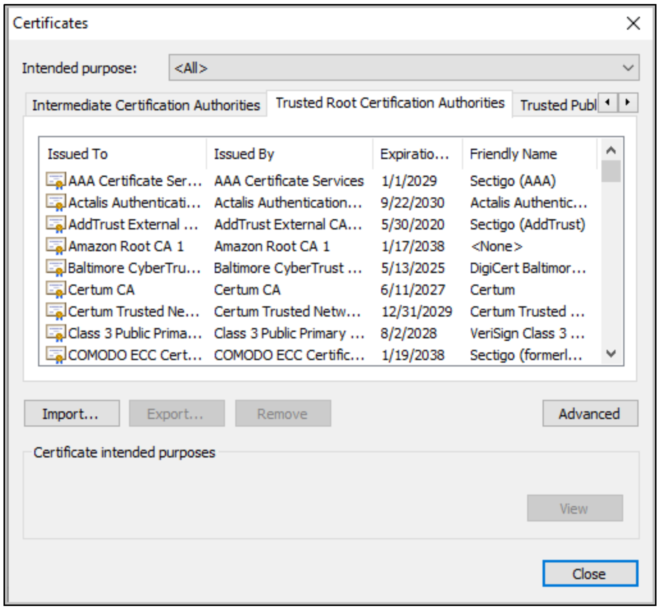
Manage phones
Control which phones you use as security keys

Manage certificates
Manage HTTPS/SSL certificates and settings

Certificates managed by Chrome
Information about how Chrome manages its root certificates

Google Advanced Protection Program
Safeguards the personal Google Accounts of anyone at risk of targeted attacks

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

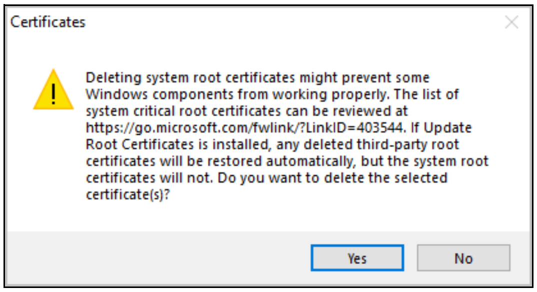

Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	1/1/2029	Sectigo (AAA)
Actalis Authenticati...	Actalis Authentication...	9/22/2030	Actalis Authentic...
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
Amazon Root CA 1	Amazon Root CA 1	1/17/2038	<None>
Baltimore CyberTru...	Baltimore CyberTrust ...	5/13/2025	DigiCert Baltimor...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
COMODO ECC Cert...	COMODO ECC Certific...	1/19/2038	Sectigo (formerl...

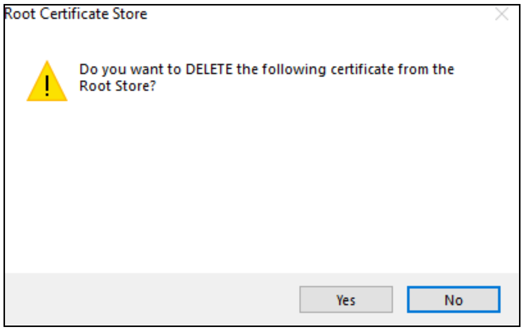
4 Select the certificate you want to remove and click **Remove**.

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



Deleting system root certificates might prevent some Windows components from working properly. The list of system critical root certificates can be reviewed at https://go.microsoft.com/fwlink/?LinkID=403544. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?

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

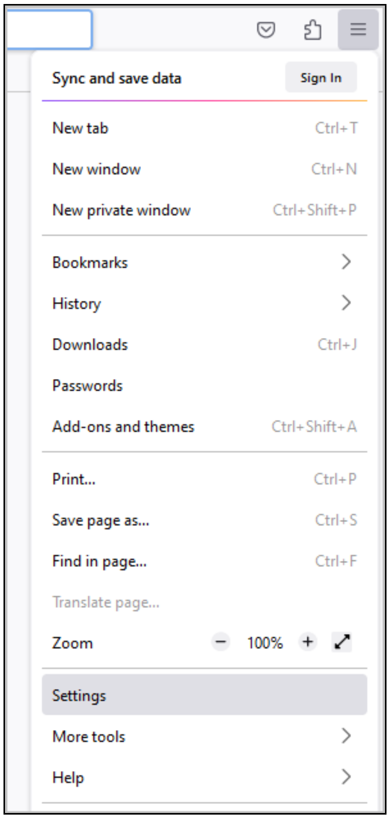


Do you want to DELETE the following certificate from the Root Store?

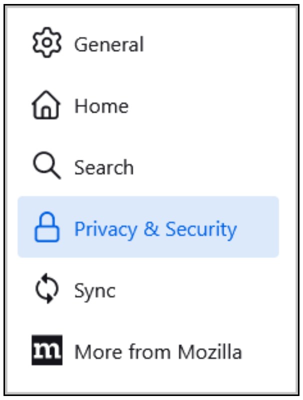
Import a Certificate to Mozilla Firefox

The following example uses Mozilla Firefox on Windows 10 Pro. You first have to store the certificate in your computer and then install it as a Trusted Root CA. To import a certificate to the Firefox browser, please follow the steps below.

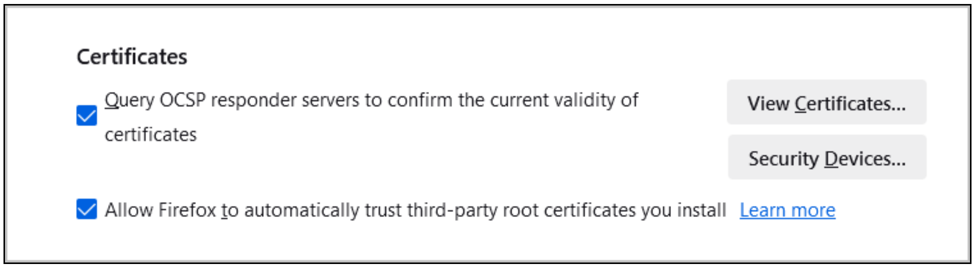
1 Open Firefox browser and click **Option** bar with three horizontal lines on the upper right corner. Click **Settings**.



2 Click **Privacy & Security**.



3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.



Certificates

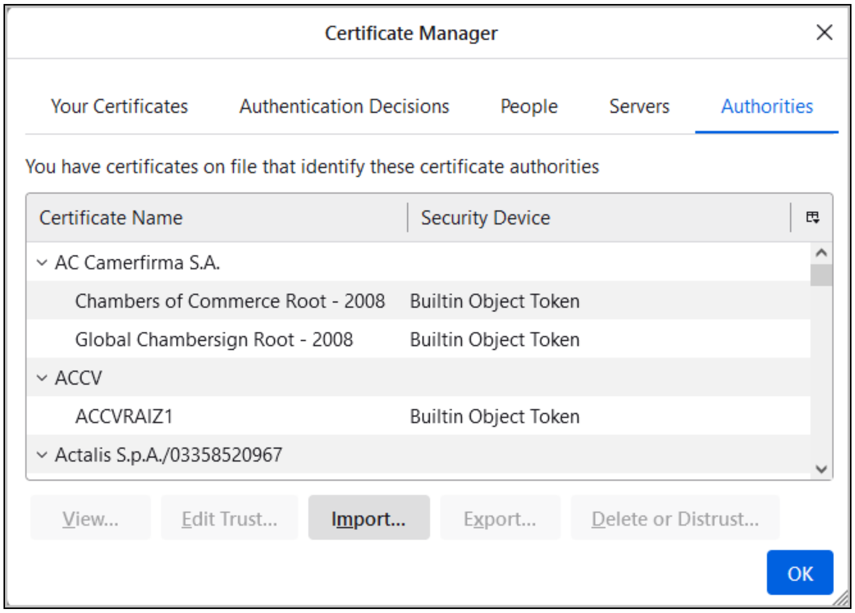
☑ Query OCSP responder servers to confirm the current validity of certificates

View Certificates...

Security Devices...

☑ Allow Firefox to automatically trust third-party root certificates you install Learn more

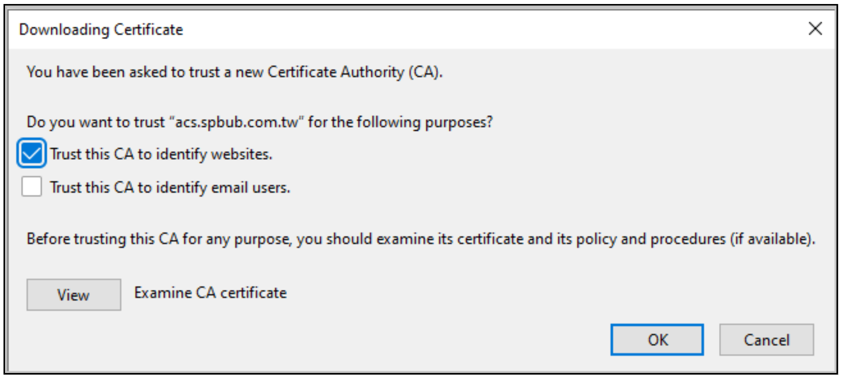
4 After the **Certificate Manager** displays, select the **Authorities** tab and click **Import**.



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

5 Open the certificate file in your computer and the **Downloading Certificate** screen shows up. Click **Trust this CA to identify websites**. Click **View** to examine the imported CA certificate.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "acs.spbub.com.tw" for the following purposes?

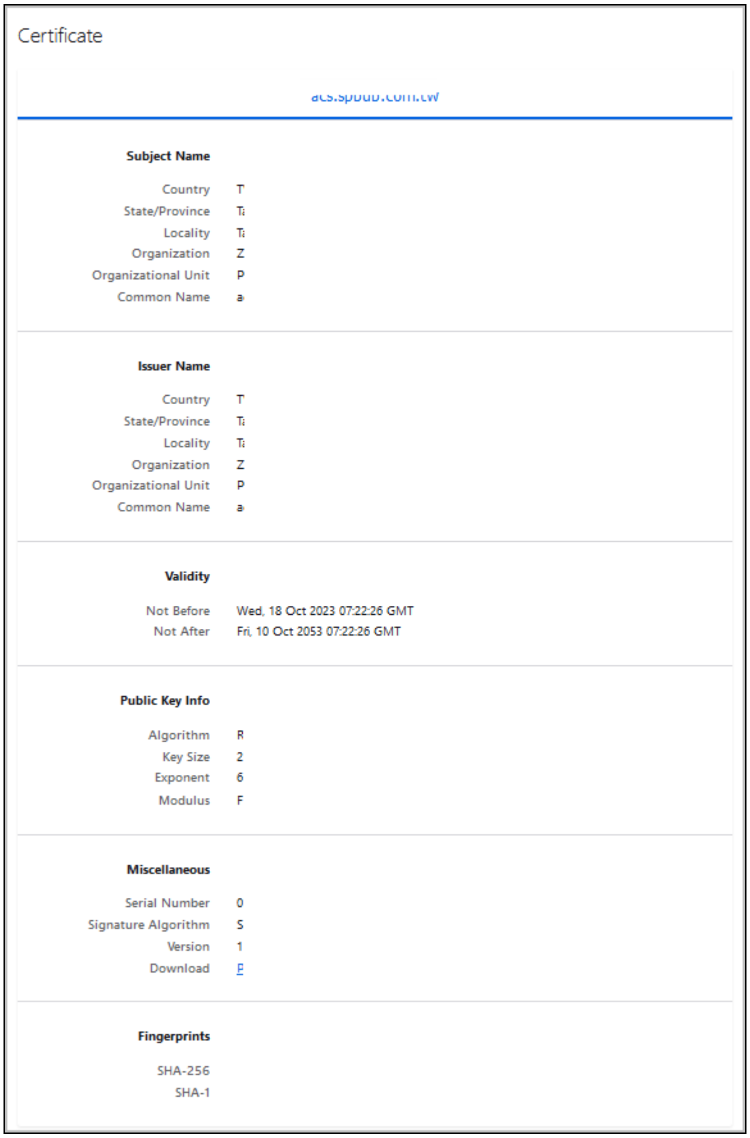
☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

6 After clicking **View**, the certificate details appear. Examine the content, ensuring the correct organization name. Verify that the validity period has the accurate start and end dates. The common name can be either an IP or domain name. Confirm that the client's used IP or domain name aligns with the Common Name on the certificate. If all the information on the certificate is correct, close the certificate screen and click **OK**.



Certificate

acs.spbub.com.tw

Subject Name

Country	T
State/Province	Ta
Locality	Ta
Organization	Z
Organizational Unit	P
Common Name	a

Issuer Name

Country	T
State/Province	Ta
Locality	Ta
Organization	Z
Organizational Unit	P
Common Name	a

Validity

Not Before	Wed, 18 Oct 2023 07:22:26 GMT
Not After	Fri, 10 Oct 2053 07:22:26 GMT

Public Key Info

Algorithm	R
Key Size	2
Exponent	6
Modulus	F

Miscellaneous

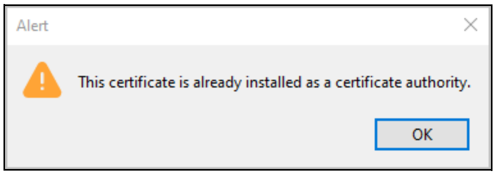
Serial Number	0
Signature Algorithm	S
Version	1
Download	P

Fingerprints

SHA-256	
SHA-1	

The certificate file is installed in Firefox now.

To check if the import is successful, click **Import** to select the same certificate again to see if the alert "**This certificate is already installed as a certificate authority**" pops out.



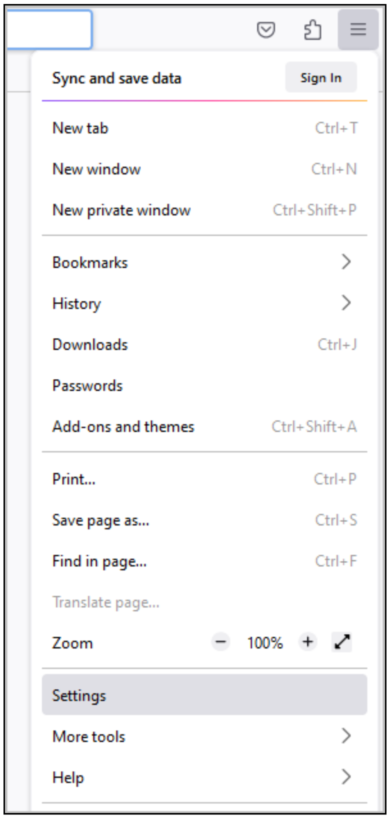
Alert

This certificate is already installed as a certificate authority.

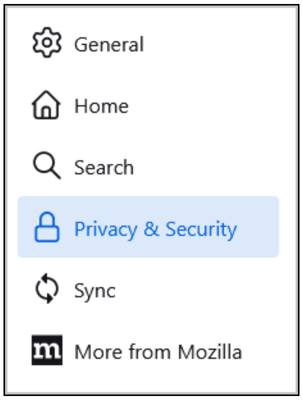
Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox.

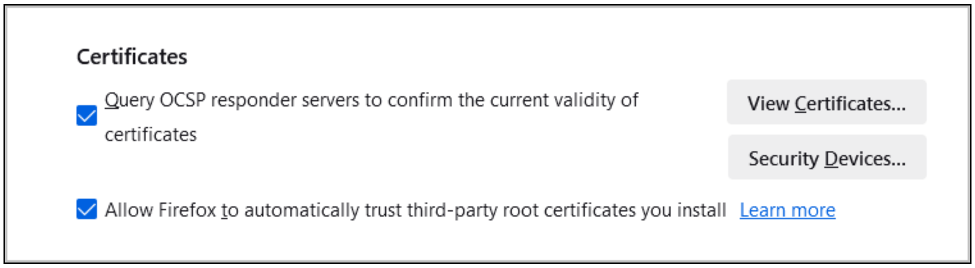
1 Open Firefox browser and click **Option** bar with three horizontal lines on the upper right corner. Click **Settings**.



2 Click **Privacy & Security**.



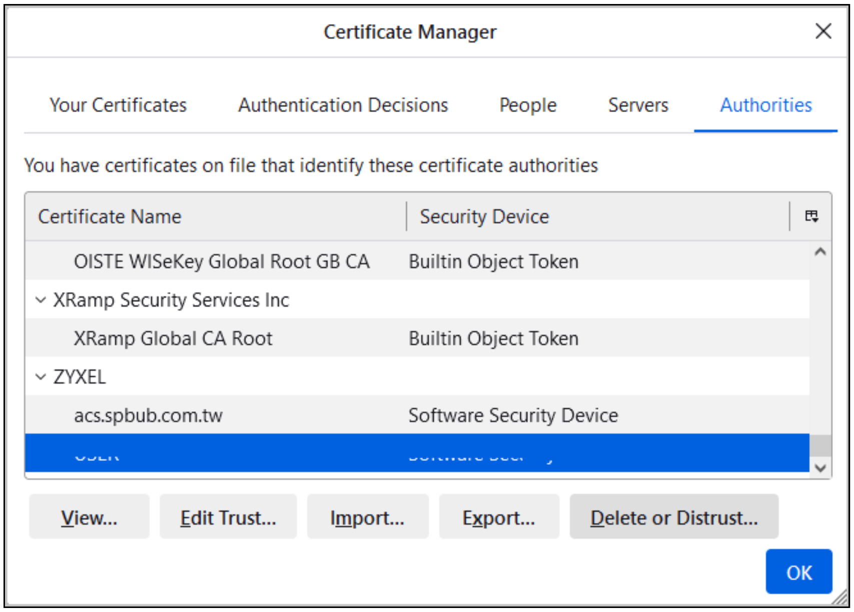
3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.


Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

☑ Allow Firefox to automatically trust third-party root certificates you install Learn more

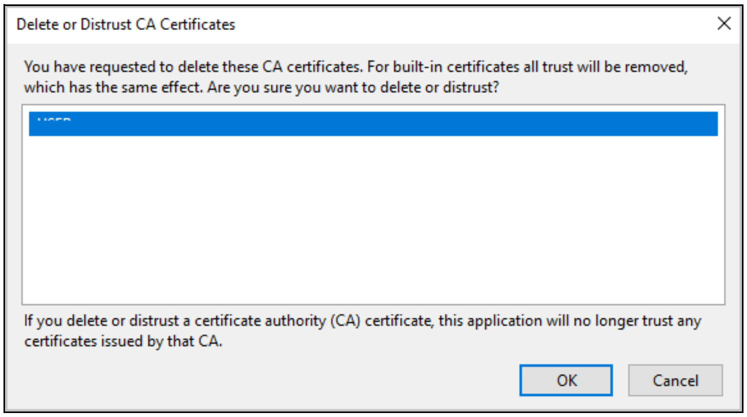
4 In the **Certificate Manager**, click **Authorities** and select the certificate you want to remove. Click **Delete or Distrust**.



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
OISTE WISeKey Global Root GB CA	Builtin Object Token
XRamp Security Services Inc	
XRamp Global CA Root	Builtin Object Token
ZYXEL	
acs.spbub.com.tw	Software Security Device

5 In the following dialog box, click **OK**.



You have requested to delete these CA certificates. For built-in certificates all trust will be removed, which has the same effect. Are you sure you want to delete or distrust?

If you delete or distrust a certificate authority (CA) certificate, this application will no longer trust any certificates issued by that CA.

6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

APPENDIX B IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 17 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 18 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 19 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0

Table 19 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 to 10, A to F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00	:	13	:	49 : 12	:	34	:	56

EUI-64	02	:	13	:	49	:	FF	:	FE	: 12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Zyxel Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

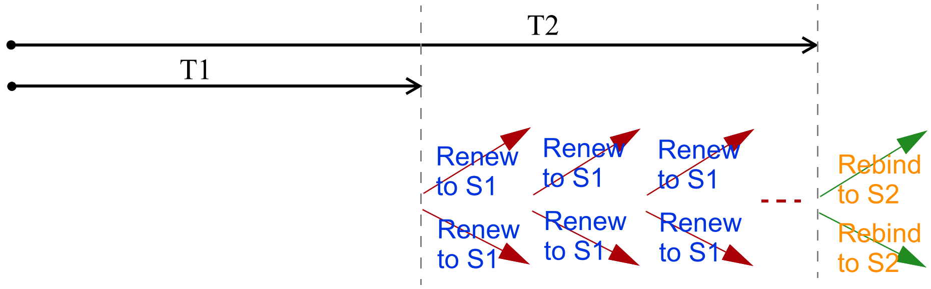
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the

[1] In IPv6, all network interfaces can be associated with several addresses.

system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor’s link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router’s information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 10

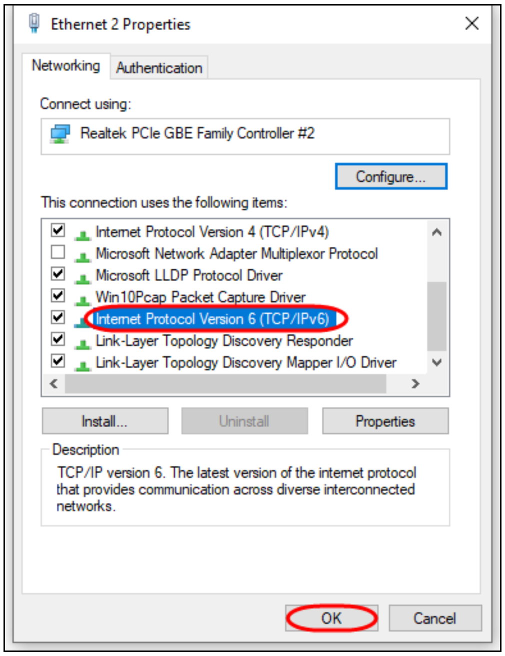
Windows 10 supports IPv6 by default. DHCPv6 is enabled when you enable IPv6 on a Windows 10 PC.

To enable IPv6 in Windows 10:

1. Select **Control Panel** > **Network and Sharing Center**.
2. On the left side of the **Network and Sharing Center**, select **Change adapter settings**.
3. Right-click your network connection and select **Properties**.

4 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.

5 Click **OK** to save the changes for the selected network adapter.



Connect using:

Realtek PCIe GBE Family Controller #2

This connection uses the following items:

☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Win10Pcap Packet Capture Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Link-Layer Topology Discovery Responder
☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

6 Click **OK** to exit the selected network adapter **Properties** screen.

Example – Enabling DHCPv6 on Windows 10

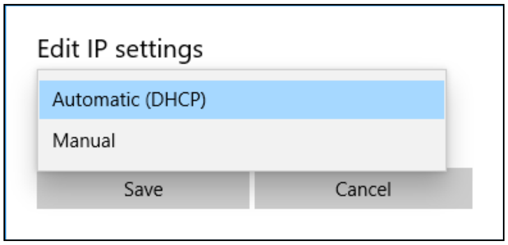
Windows 10 supports DHCPv6 by default. To enable DHCPv6 client on your computer:

1 Select **Start** > **Settings** > **Network & Internet**.

2 On the left side of the **Network & Internet**, select **Ethernet**. Then select the Ethernet network you are connected to.

3 Under **IP assignment**, select **Edit**.

4 Under **Edit IP settings**, select **Automatic (DHCP)** or **Manual**. Then click **Save**.



- When you select **Automatic (DHCP)**, the IP address settings and DNS server address setting are set automatically by your router.
- When you select **Manual**, you can manually set your IP address settings and DNS server address.

Now your computer can obtain an IPv6 address from a DHCPv6 server.

APPENDIX C
Customer Support

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

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan

- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria
- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania

- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.
- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX D
Legal Information

Copyright

Disclaimers

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

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

Trademarks

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

Regulatory Notice and Statement (Class B)

United States of America

The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) this device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the equipment and receiver
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
  - Consult the dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter. Refer to the list below for the models whose transmitters require a minimum distance of over 20 cm from the user, along with the required distances.
- Root Plus: 26 cm
- Leaf Plus: 42 cm
- Country Code selection feature to be disabled for products marketed to the US / CANADA.

Caution (For device with 6 GHz function)

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Operation of transmitters in the 5.925 to 7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Brazil

The following applies if you use the product within Brazil.

For WiFi 6 products,

- Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

- Este produto não é apropriado para uso em ambientes domésticos, pois poderá causar interferências eletromagnéticas que obrigam o usuário a tomar medidas necessárias para minimizar estas interferências.

For WiFi 6E and WiFi 7 products,

- Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.
- Este produto não é apropriado para uso em ambientes domésticos, pois poderá causar interferências eletromagnéticas que obrigam o usuário a tomar medidas necessárias para minimizar estas interferências.
- O uso deste equipamento é restrito a ambientes fechados é proibido em plataformas petrolíferas, carros, trens, embarcações e no interior de aeronaves abaixo de 3.048 m (10.000 pés).
- Para maiores informações, consulte o site da Anatel: *www.gov.br/pt-br/search?origem=form&SearchableText=anatel*

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES(B)/NMB(B)

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement

The following information applies to products with wireless functions.

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- The radio transmitter 25830-04369 (Root Plus) and 25830-04371 (Leaf Plus) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed, are strictly prohibited for use with this device.

Antenna Information

MODEL NAME	NO.	TYPE	GAIN (dBi)	IMPEDANCE
Leaf Plus	1	Patch	11.1 dBi (5150 MHz) 11.6 dBi (5350 MHz) 10.7 dBi (5550 MHz) 11.3 dBi (5750 MHz) 10.4 dBi (5850 MHz)	50 Ω
Leaf Plus	2	Patch	11.0 dBi (5150 MHz) 10.9 dBi (5350 MHz) 10.8 dBi (5550 MHz) 10.5 dBi (5750 MHz) 10.8 dBi (5850 MHz)	50 Ω
Leaf Plus	3	Patch	10.0 dBi (5925 MHz) 11.4 dBi (6325 MHz) 11.1 dBi (6725 MHz) 11.4 dBi (6925 MHz) 11.8 dBi (7125 MHz)	50 Ω
Leaf Plus	4	Patch	10.3 dBi (5925 MHz) 11.3 dBi (6325 MHz) 11.6 dBi (6725 MHz) 10.8 dBi (6925 MHz) 12.0 dBi (7125 MHz)	50 Ω

If the product with 5G wireless function operating in 5150 to 5250 MHz and 5725 to 5850 MHz, the following attention must be paid,

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725 to 5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250 to 5350 MHz and 5470 to 5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250 to 5350 MHz and 5470 to 5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.

Innovation, Sciences et Développement économique Canada RSS-GEN & RSS-247

- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio 25830-04369 (Root Plus) and 25830-04371 (Leaf Plus) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Informations Antenne

NOM DU MODÈLE	NB.	TYPE	GAIN (dBi)	IMPÉDANCE
Leaf Plus	1	Patch	11.1 dBi (5150 MHz) 11.6 dBi (5350 MHz) 10.7 dBi (5550 MHz) 11.3 dBi (5750 MHz) 10.4 dBi (5850 MHz)	50 ohm
Leaf Plus	2	Patch	11.0 dBi (5150 MHz) 10.9 dBi (5350 MHz) 10.8 dBi (5550 MHz) 10.5 dBi (5750 MHz) 10.8 dBi (5850 MHz)	50 ohm
Leaf Plus	3	Patch	10.0 dBi (5925 MHz) 11.4 dBi (6325 MHz) 11.1 dBi (6725 MHz) 11.4 dBi (6925 MHz) 11.8 dBi (7125 MHz)	50 ohm
Leaf Plus	4	Patch	10.3 dBi (5925 MHz) 11.3 dBi (6325 MHz) 11.6 dBi (6725 MHz) 10.8 dBi (6925 MHz) 12.0 dBi (7125 MHz)	50 ohm

Lorsque la fonction sans fil 5G fonctionnant en 5150 to 5250 MHz and 5725 to 5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;

- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5 250 à 5 350 MHz et 5 470 à 5 725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d’antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

For the models whose radiators require a minimum distance of over 20 cm from your body, along with the required distances.

- Root Plus: 26 cm
- Leaf Plus: 43 cm

Déclaration d’exposition aux radiations:

Cet équipement est conforme aux limites d’exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps. Veuillez vous référer à la liste ci-dessous pour connaître les modèles dont les radiateurs nécessitent une distance minimale de plus de 20 cm par rapport à votre corps, ainsi que les distances requises.

- Root Plus: 26 cm
- Leaf Plus: 43 cm

Caution:

- The maximum antenna gain permitted for devices in the bands 5250 to 5350 MHz and 5470 to 5725 MHz shall comply with the e.i.r.p. limit; and
- the maximum antenna gain permitted for devices in the band 5725 to 5825 MHz shall comply with the e.i.r.p. limits specified for point to point and non point to point operation as appropriate.
- Outdoor device: Root Plus and Leaf Plus

Caution (For device with 6 GHz function):

- Devices shall not be used for control of or communications with unmanned aircraft systems.
- Devices shall not be used on oil platforms.
- Devices shall not be used on aircraft, except for the low-power indoor access points, indoor subordinate devices, low-power client devices, and very low-power devices operating in the 5925 to 6425 MHz band, that may be used on large aircraft as defined in the Canadian Aviation Regulations, while flying above 3,048 meters (10,000 feet).
- Devices shall not be used on automobiles.
- Devices shall not be used on trains.

- Devices shall not be used on maritime vessels.

Antenna Information
Regulatory Statement
The antenna height shall be determined by the installer or operator of the standard-power access point or fixed client device, or by automatic means. This information shall be stored internally in the device. Provision of accurate device information is mandatory.

Device Specifications
This product uses an integrated internal antenna, permanently installed and not user replaceable.

- **Antenna type**: Metal Array (Internal antenna)
- **Antenna model**: OLA25B-127160-A
- **Antenna peak gain**: 5 GHz: 14.4 dBi; 6 GHz: 15.1 dBi

Avertissement:

- le gain maximal d’antenne permis pour les dispositifs utilisant les bandes 5 250 à 5 350 MHz et 5 470 à 5 725 MHz doit se conformer à la limite de p.i.r.e.;
- le gain maximal d’antenne permis (pour les dispositifs utilisant la bande 5725 à 5825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l’exploitation point à point et n on point à point, selon le cas.
- Appareil extérieur: Root Plus and Leaf Plus

Avertissement (Pour modèle avec fonction 6 GHz)

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d’aéronef sans pilote ni pour communiquer avec de tels systèmes.
- Les dispositifs ne doivent pas être utilisés sur les plateformes de forage pétrolier.
- Les dispositifs ne doivent pas être utilisés dans les aéronefs, à l'exception des points d'accès intérieurs de faible puissance, des dispositifs subordonnés intérieurs, des dispositifs clients de faible puissance et des dispositifs de très faible puissance fonctionnant dans la bande de 5 925 à 6 425 MHz, qui peuvent être utilisés dans les gros aéronefs tel qu'il est défini dans le Règlement de l'aviation canadien, et ce, lorsqu'ils volent à une altitude supérieure à 3 048 mètres (10 000 pieds).
- Les dispositifs ne doivent pas être utilisés dans les automobiles.
- Les dispositifs ne doivent pas être utilisés dans les trains.
- Les dispositifs ne doivent pas être utilisés sur les navires maritimes.

Informations sur l'antenne
Déclaration réglementaire
La hauteur de l'antenne doit être déterminée par l'installateur ou l'opérateur du point d'accès de puissance normale ou du dispositif client fixe, ou par des dispositifs automatiques. Cette information doit être enregistrée dans le dispositif. La fourniture d'information précise sur le dispositif est obligatoire.

Spécifications de l'appareil
Ce produit utilise une antenne interne intégrée, installée de manière permanente et non remplaçable par l'utilisateur.

- **Type d'antenne**: Réseau métallique (antenne interne)
- **Modèle d'antenne**: OLA25B-127160-A
- **Gain de crête de l'antenne**: 5 GHz: 14,4 dBi; 6 GHz: 15,1 dBi

Europe and the United Kingdom

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK regulation

- Compliance information for wireless products relevant to the EU, United Kingdom and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation 2017 SI 2017-1206. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device operates in the 5150 to 5350 MHz or 5945 to 6425 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:

FREQUENCY	**MAXIMUM POWER**
2,400 MHz to 2,483.5 MHz	< 100 mW
5,150 MHz to 5,350 MHz	< 200 mW
5,470 MHz to 5,725 MHz	< 1000 mW
5,945 MHz to 6,425 MHz (For device with 6 GHz function)	< 200 mW

Belgium (English) België (Flemish) Belgique (French)	**National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check *http://www.bipt.be* for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.ibpt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.

Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. National Restrictions • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a “general authorization.” Please check *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of National Codes

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

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (For indoor devices only) (2) Do not install or service this device during a thunderstorm.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.

- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120 V AC in North America or 230 V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Do not try to repair the power adaptor or cord by yourself. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- This device must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. (For devices that require grounding)

  – If your device has an earthing screw (frame ground), connect the screw to a ground terminal using an appropriate AWG ground wire. Do this before you make other connections.

  – If your device has no earthing screw, but has a 3-prong power plug, make sure to connect the plug to a 3-hole earthed socket.
- For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- Do not use a power adapter that has a power cable longer than 3 meters.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating. (For devices with a fuse)
- To avoid possible eye injury, do not look into an operating fiber-optic module's connector. (For devices with fiber)
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019. (For devices with fiber)
- Conforme à 21 CFR 1040.10 et 1040.11 sauf pour la conformité à la norme CEI 60825-1 Ed. 3., comme décrit dans la notice laser Numéro 56 du 8 mai 2019. (For devices with fiber)
- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014" (For devices with fiber)
- APPAREIL À LASER DE CLASS 1 (For devices with fiber)

- CLASS 1 CONSUMER LASER PRODUCT & “EN 50689:2021” (For devices with fiber)
- The antenna must be installed completely perpendicular to the horizon.
- **Installation Angle Requirement**
  The device shall be installed such that the main radiation direction of the internal antenna does not exceed 30 degrees above the horizontal plane (horizon).
  Installation angles greater than 30 degrees upward tilt are not permitted.
  Failure to comply with this installation requirement may result in operation outside authorization.
- **Installation Angle Definition**
  Horizon (0 degree): Horizontal plane parallel to the ground.
  Elevation Angle: The angle between the antenna main radiation direction and the horizontal plane.

Environment statement

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示 :

- 請勿將此產品接近水、火焰或放置在高溫的環境。
  避免設備接觸
  – 任何液體 – 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  – 灰塵及污物 – 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如 : 台灣供應電壓 110 伏特) 。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。(僅限於室內產品)

- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  — 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  — 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
∿	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
⎓	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
⏚	Earth; ground: A wiring terminal intended for connection of a Functional Earthing Conductor.
⧈	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *https://www.zyxel.com/global/en/support/warranty-information*.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: *https://www.zyxel.com/form/gpl_oss_software_notice.shtml*.