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

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

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

⊙ Automatically select the certificate store based on the type of certificate
○ Place all certificates in the following store

Certificate store:

[   ] Browse...

< Back   Next >   Cancel

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

Certificate Import Wizard

Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	D:\Projects_2003-10\CPE2\cp

< Back   Finish   Cancel

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

Certificate Import Wizard

ⓘ The import was successful.

OK

17.5.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device through HTTPS:

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

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

3 You next see the Web Configurator login screen.

17.6 SSH

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

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

Figure 141 SSH Communication Over the WAN Example

17.6.1 How SSH Works

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

Figure 142 How SSH v1 Works Example
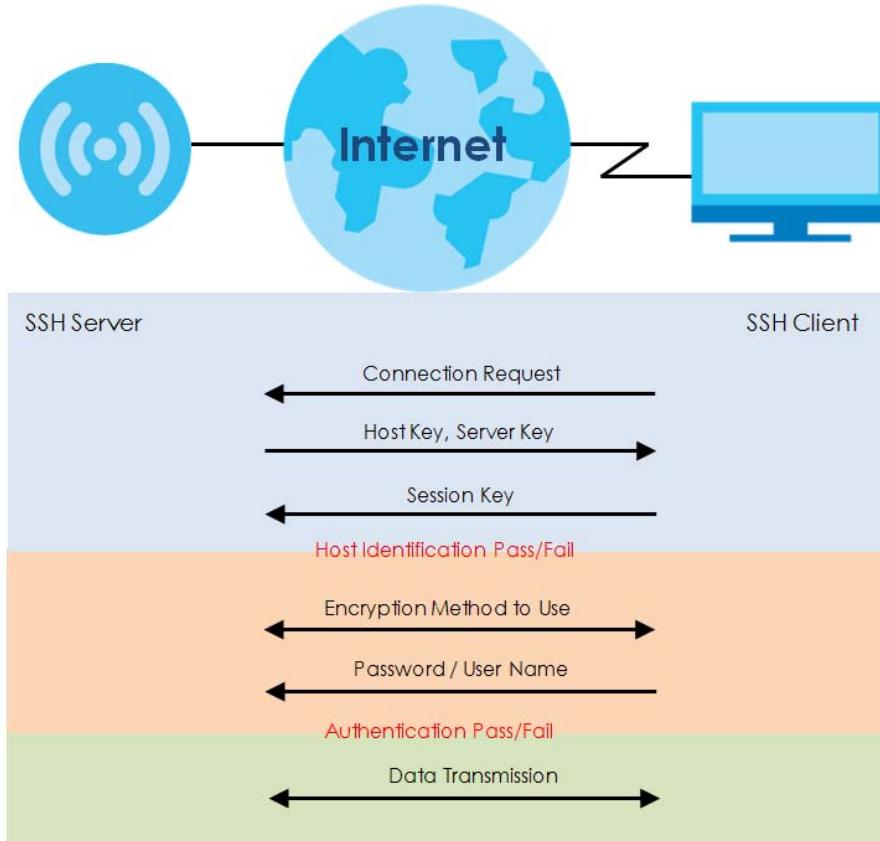
1 Host Identification

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

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

2 Encryption Method

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

3 Authentication and Data Transmission

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

17.6.2 SSH Implementation on the Zyxel Device

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

17.6.3 Requirements for Using SSH

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

17.6.4 Configuring SSH

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

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

Figure 143 Configuration > System > SSH

The following table describes the labels in this screen.

Table 91 Configuration > System > SSH

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

17.6.5 Examples of Secure Telnet Using SSH

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

17.6.5.1 Example 1: Microsoft Windows

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

1 Launch the SSH client and specify the connection information (IP address, port number) for the Zyxel Device.

2 Configure the SSH client to accept connection using SSH version 2.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 144   SSH Example 1: Store Host Key
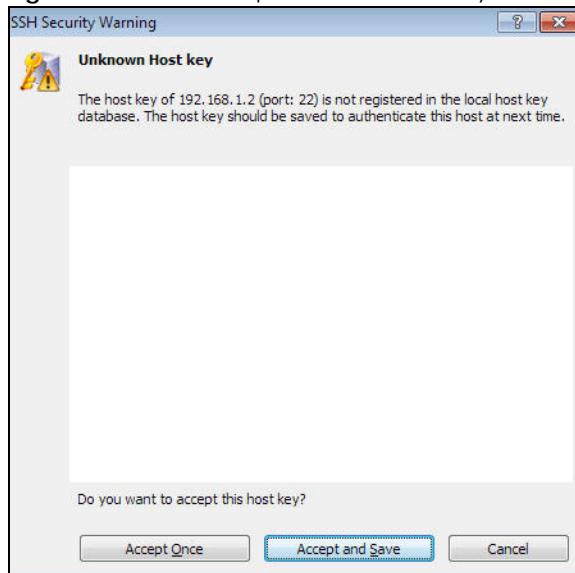
Enter the password to log in to the Zyxel Device. The CLI screen displays next.

17.6.5.2 Example 2: Linux

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

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

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

Figure 145 SSH Example 2: Log in

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

2 The CLI screen displays next.

17.7 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. See Chapter 19 on page 256 for more information about firmware and configuration files. To change your Zyxel Device's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify FTP settings.

Figure 146 Configuration > System > FTP

The following table describes the labels in this screen.

Table 92 Configuration > System > FTP

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

17.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1), version two (SNMPv2c), and version three (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 147   SNMP Management Model
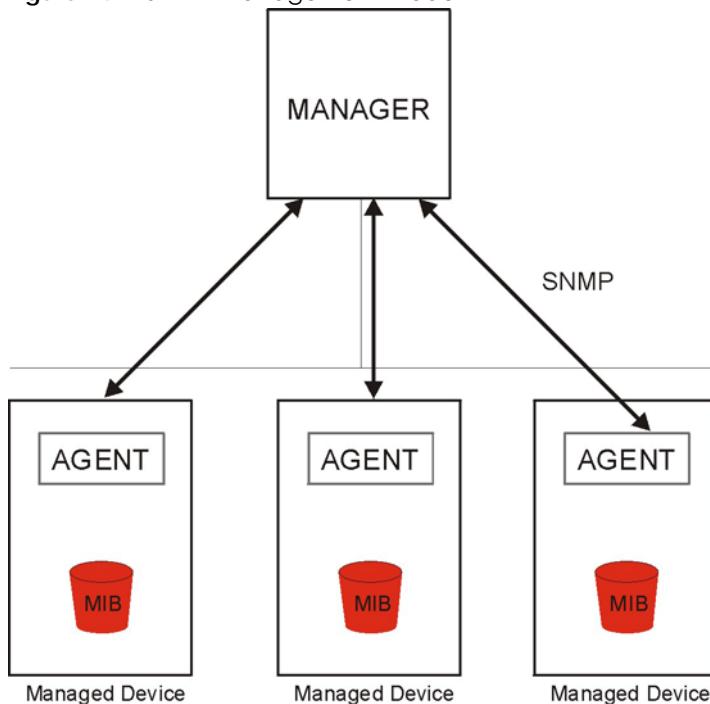
An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Zyxel Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.

• Trap - Used by the agent to inform the manager of some events.

17.8.1 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs (ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB, ZYXEL-ES-ZyXELAPMgmt.MIB, ZYXEL-ES-PROWLAN.MIB, ZYXEL-ES-RFMGMT.MIB, ZYXEL-ES-SMI.MIB, and ZYXEL-ES-WIRELESS.MIB) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

17.8.2 SNMP Traps

The Zyxel Device will send traps to the SNMP manager when any one of the following events occurs.

Table 93   SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

17.8.3 Configuring SNMP

To change your Zyxel Device's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings. You can also configure user profiles that define allowed SNMPv3 access.

Note: Not all Zyxel Device models support the SNMP feature. See the comparison table in

Figure 148   Configuration > System > SNMP

The following table describes the labels in this screen.

Table 94   Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow users to access the Zyxel Device using SNMP.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. You can use up to 63 alphanumeric(0-9, a-z, A-Z) characters, underscores (_), dots (·). The first character cannot be a dot.
Destination	Type the IP address of the station to send your SNMP traps to.
Trap Wireless Event	Select this to have the Zyxel Device send a trap to the SNMP manager when a WiFi client is connected to or disconnected from the Zyxel Device.
SNMPv2c	Select this to allow SNMP managers using SNMPv2c to access the Zyxel Device.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. You can use up to 63 alphanumeric(0-9, a-z, A-Z) characters, underscores (_), dots (·). The first character cannot be a dot.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests. You can use up to 63 alphanumeric(0-9, a-z, A-Z) characters, underscores (_), dots (·). The first character cannot be a dot.
SNMPv3	Select this to allow SNMP managers using SNMPv3 to access the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This the index number of an SNMPv3 user profile.
User Name	This is the name of the user for which this SNMPv3 user profile is configured.
Authentication	This field displays the type of authentication the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
Privacy	This field displays the type of encryption the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
Privilege	This field displays whether the SNMPv3 user can have read-only or read and write access to the Zyxel Device using this SNMPv3 user profile.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.8.4 Adding or Editing an SNMPv3 User Profile

This screen allows you to add or edit an SNMPv3 user profile. To access this screen, click the **Configuration > System > SNMP** screen's **Add** button or select a SNMPv3 user profile from the list and click the **Edit** button.

Figure 149 Configuration > System > SNMP > Add

The following table describes the labels in this screen.

Table 95   Configuration > System > SNMP > Add

LABEL	DESCRIPTION
User Name	Select the user name of the user account for which this SNMPv3 user profile is configured.
Authentication	Select the type of authentication the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
	Select **MD5** to require the SNMPv3 user's password be encrypted by MD5 for authentication.
	Select **SHA** to require the SNMPv3 user's password be encrypted by SHA for authentication.
Privacy	Select the type of encryption the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
	Select **NONE** to not encrypt the SNMPv3 communications.
	Select **DES** to use DES to encrypt the SNMPv3 communications.
	Select **AES** to use AES to encrypt the SNMPv3 communications.
Privilege	Select whether the SNMPv3 user can have read-only or read and write access to the Zyxel Device using this SNMPv3 user profile.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 18
Log and Report

18.1 Overview

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

18.1.1 What You Can Do In this Chapter

- The **Email Daily Report** screen (Section 18.2 on page 244) configures how and where to send daily reports and what reports to send.
- The **Log Setting** screens (Section 18.3 on page 246) specify which logs are emailed, where they are emailed, and how often they are emailed.

18.2 Email Daily Report

Use this screen to start or stop data collection and view various statistics about traffic passing through your Zyxel Device.

Note: This screen will not appear if your Zyxel Device does not support email daily report.

Note: Data collection may decrease the Zyxel Device's traffic throughput rate.

Click **Configuration** > **Log & Report** > **Email Daily Report** to display the following screen. Configure this screen to have the Zyxel Device email you system statistics every day.

Figure 150 Configuration > Log & Report > Email Daily Report

The following table describes the labels in this screen.

Table 96   Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
General Settings	
Enable Email Daily Report	Select this to send reports by email every day.

Table 96   Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
Email Settings	
Mail Server	Type the name or IP address of the outgoing SMTP server.
SSL/TLS Encryption	Select **SSL/TLS** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **No** to not encrypt the communications.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing email. Select **Append system name** to add the Zyxel Device's system name to the subject. Select **Append date time** to add the Zyxel Device's system date and time to the subject.
Mail From	Type the email address from which the outgoing email is delivered. This address is used in replies.
Mail To	Type the email address (or addresses) to which the outgoing email is delivered.
SMTP Authentication	Select this checkbox if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** checkbox. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the **SMTP Authentication** checkbox. Type the password to provide to the SMTP server when the log is emailed.
Send Report Now	Click this button to have the Zyxel Device send the daily email report immediately.
Schedule	
Time for sending report	Select the time of day (hours and minutes) when the log is emailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

18.3 Log Setting

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

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

18.3.1 Log Setting Screen

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

Figure 151 Configuration > Log & Report > Log Setting

The following table describes the labels in this screen.

Table 97 Configuration > Log & Report > Log Setting

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

18.3.2 Edit System Log Settings

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

Note: The **E-mail Server** fields will not appear if your Zyxel Device does not support email daily report.

Figure 152 Configuration > Log & Report > Log Setting > Edit System Log Setting

The following table describes the labels in this screen.

Table 98   Configuration > Log & Report > Log Setting > Edit System Log Setting

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

Table 98   Configuration > Log & Report > Log Setting > Edit System Log Setting (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for emailing logs to email server 1 for all log categories.
	Using the **System Log** drop-down list to disable all logs overrides your email server 1 settings.
	enable normal logs (green check mark) - email log messages for all categories to email server 1.
	enable alert logs (red exclamation point) - email alerts for all categories to email server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for emailing logs to email server 2 for all log categories.
	Using the **System Log** drop-down list to disable all logs overrides your email server 2 settings.
	enable normal logs (green check mark) - email log messages for all categories to email server 2.
	enable alert logs (red exclamation point) - email alerts for all categories to email server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices:
	disable all logs (red X) - do not log any information from this category
	enable normal logs (green check mark) - create log messages and alerts from this category
	enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in **E-Mail Server 1**. The Zyxel Device does not email debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in **E-Mail Server 2**. The Zyxel Device does not email debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=x]", where x is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=x]", where x is the number of original log messages, appended at the end of the **Message** field. The range is 1-600 seconds.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

18.3.3 Edit Remote Server

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

Figure 153 Configuration > Log & Report > Log Setting > Edit Remote Server
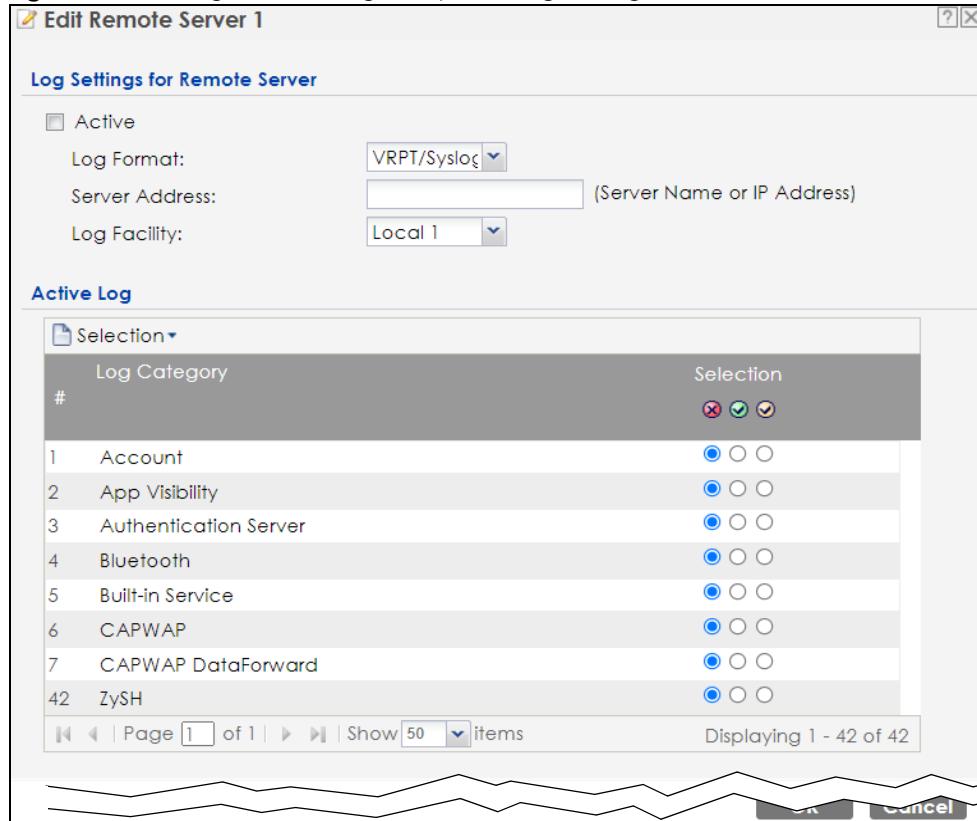
The following table describes the labels in this screen.

Table 99   Configuration > Log & Report > Log Setting > Edit Remote Server

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

Table 99   Configuration > Log & Report > Log Setting > Edit Remote Server (continued)

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

18.3.4 Active Log Summary

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

Note: The **E-mail Server** fields will not appear if your Zyxel Device does not support email daily report.

Figure 154   Active Log Summary

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

The following table describes the fields in this screen.

Table 100   Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	If the Zyxel Device is set to controller mode, the AC section controls logs generated by the controller and the AP section controls logs generated by the managed APs.
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories.
	disable all logs (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2.
	enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them.
	enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for emailing logs to email server 1 for all log categories.
	Using the **System Log** drop-down list to disable all logs overrides your email server 1 settings.
	enable normal logs (green check mark) - email log messages for all categories to email server 1.
	enable alert logs (red exclamation point) - email alerts for all categories to email server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for emailing logs to email server 2 for all log categories.
	Using the **System Log** drop-down list to disable all logs overrides your email server 2 settings.
	enable normal logs (green check mark) - email log messages for all categories to email server 2.
	enable alert logs (red exclamation point) - email alerts for all categories to email server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories.
	disable all logs (red X) - do not send the remote server logs for any log category.
	enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories.
	enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices:
	disable all logs (red X) - do not log any information from this category
	enable normal logs (green checkmark) - create log messages and alerts from this category
	enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in **E-Mail Server 1**. The Zyxel Device does not email debugging information, even if it is recorded in the **System log**.

Table 100   Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in **E-Mail Server 2**. The Zyxel Device does not email debugging information, even if it is recorded in the **System log**.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

19.1 Overview

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

19.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 19.2 on page 259) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen (Section 19.3 on page 264) checks your current firmware version and uploads firmware to the Zyxel Device.
- The **Shell Script** screen (Section 19.4 on page 268) stores, names, downloads, uploads and runs shell script files.

19.1.2 What you Need to Know

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

Configuration Files and Shell Scripts

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

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

Figure 155 Configuration File / Shell Script: Example

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

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

Table 101   Configuration Files and Shell Scripts in the Zyxel Device

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

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

Errors in Configuration Files or Shell Scripts

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

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

Sub commands in Configuration Files or Shell Scripts

In a configuration file or shell script, sub commands are used to further define commands.

In the following example, the commands change the SSID name to "Alice-AP" on the Zyxel Device:

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

- Line 1: Enter **Configuration** mode: `configure terminal`
- Line 2: Enter SSID profile (and enter sub command mode): `wlan-ssid-profile default`
- Line 3: Configure the SSID name: `ssid Joe-AP`
- Line 4: Exit sub command mode: `exit`
- Line 5: Save the configuration: `write`

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

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

Sensitive Data Protection

The Zyxel Device by default encrypts local admin and user account passwords for web configurator and CLI.

Enable **Sensitive Data Protection** to have the Zyxel Device use a private key to encrypt local admin and user account passwords for web configurator and CLI.

Note: You can only upload configuration files using FTP that are using the current private key of the Zyxel Device.

The following examples describe the situations you might come across using **Sensitive Data Protection**.

Example 1:

1 Download a configuration file (file1).

2 Enable **Sensitive Data Protection**.

3 Create a private key (key1).

4 When you upload file1 to the Zyxel Device through the Zyxel Device web configurator, you do not need to enter the private key (key1). Configuration file1 is not encrypted by the private key (key1).

Example2:

1 Enable **Sensitive Data Protection**.

2 Create an private key (key1).

3 Download a configuration file (file2).

4 You must use key1 to upload file2 to the Zyxel Device because file2 is encrypted by key1.

Example 3:

1 Change the private key from key1 to key2.

2 Download another configuration file (file3).

3 You must use key2 to upload file3 to the Zyxel Device.

Note: You must still use key1 to upload file2 to the Zyxel Device. Make a note of the key to use when you change the private key and then download a configuration file.

Example 4:

1 Enable **Sensitive Data Protection** on Zyxel Device1 and create a private key.

2 Download a configuration file from Zyxel Device1.

3 You must upload this configuration file using the private key you created on Zyxel Device1 to Zyxel Device2 even if **Sensitive Data Protection** is not enabled on Zyxel Device2.

19.2 Configuration File

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

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

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings.

- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.

- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Figure 156 Maintenance > File Manager > Configuration File

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

The following table describes the labels in this screen.

Table 102   Maintenance > File Manager > Configuration File
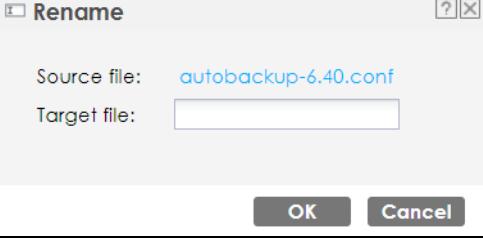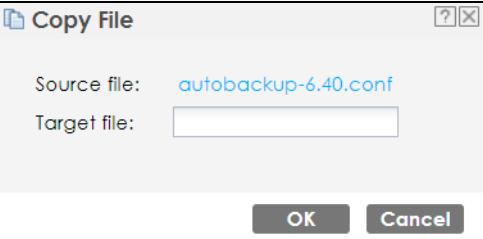
LABEL	DESCRIPTION
Configuration Files	
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files.
	You cannot rename a configuration file to the name of another configuration file in the Zyxel Device.
	Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.
	Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).
	Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files.
	A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device.
	Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.
	Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).
	Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 102   Maintenance > File Manager > Configuration File (continued)
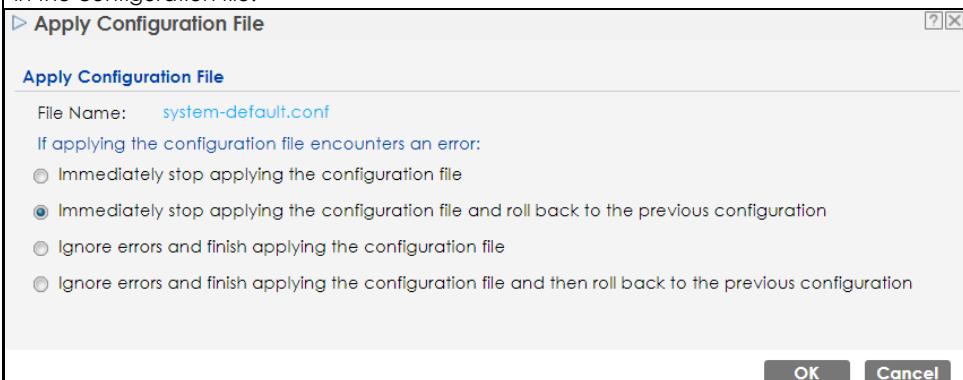
LABEL	DESCRIPTION
Apply	Use this button to have the Zyxel Device use a specific configuration file.
	Click a configuration file's row to select it and click **Apply** to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.
	The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file.
	Immediately stop applying the configuration file - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the Zyxel Device.
	Immediately stop applying the configuration file and roll back to the previous configuration - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible.
	Ignore errors and finish applying the configuration file - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix.
	Ignore errors and finish applying the configuration file and then roll back to the previous configuration - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the Zyxel Device with a fully valid configuration file.
	Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen.
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	This column displays the label that identifies a configuration file.
	You cannot delete the following configuration files or change their file names.
	The **system-default.conf** file contains the Zyxel Device's default settings. Select this file and click **Apply** to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package.
	The **startup-config.conf** file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made through CLI commands when you use the `write` command.
	The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the Zyxel Device last restarted. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.

Table 102   Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Sensitive Data Protection	
Enable	Select this to enable Sensitive Data Protection; see Section 19.1 on page 256 for more information.
	You need this key to upload configuration files. Write down the key you set and keep it in a safe place.
	Figure 157 Upload Configuration File
Enter Private Encryption Key	Enter the encryption key in this field. The encryption key should be 4-8 single byte printable characters, including 0-9a-zA-Z`~!@#$%^&*()_-+={}|\;:'<,>./]|.
Re-enter Private Encryption Key	Enter the encryption key again in this field.
Upload Configuration File	
The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device.	
You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**.	
If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.	
File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

19.2.1 Example of Configuration File Download Using FTP

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

1   Connect your computer to the Zyxel Device.

2   The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Enter your user name when prompted.

5 Enter your password as requested.

6 Use "cd" to change to the directory that contains the files you want to download.

7 Use "dir" or "ls" if you need to display a list of the files in the directory.

8 Use "get" to download files. Transfer the configuration file on the Zyxel Device to your computer. Type `get` followed by the name of the configuration file. This examples uses `get startup-config.conf`.

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

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

19.3 Firmware Package

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

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

You can manually download the new firmware from the Zyxel website, or you can click **Check Now** to automatically find the latest firmware for your Zyxel Device (recommended).

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 158 Maintenance > File Manager > Firmware Package
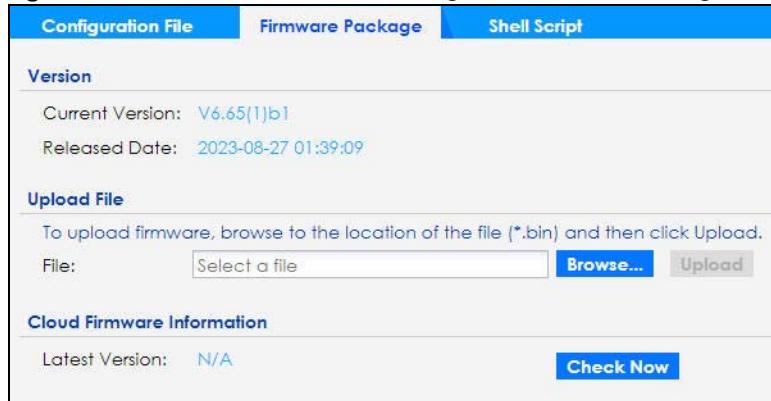
Figure 159 Maintenance > File Manager > Firmware Package > Check now
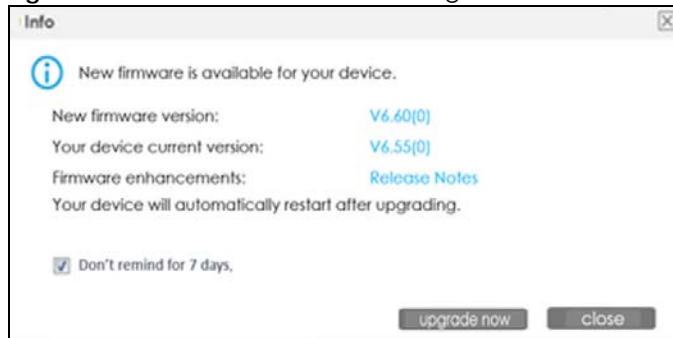
The following table describes the labels in this screen.

Table 103   Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **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.
Check now	Click **Check now** to view the firmware information. The following message appears when there is a new firmware version available for your Zyxel Device.

Table 103   Maintenance > File Manager > Firmware Package (continued)

LABEL	DESCRIPTION
New firmware version	This is the new firmware version available for your Zyxel Device. V6.60 is the firmware trunk version and the number in brackets is the release number. 0 is the first release of this version firmware. 1 is the next update release of this version firmware.
Your device current version	This is the current firmware version of your Zyxel Device.
Firmware enhancements	Click **Release Notes** to view the firmware release information of the new firmware, including new features, enhancements and bug fix.
Don't remind for 7 days	Select this to stop receiving this notification for the next 7 days.
upgrade now	Click this to start upgrading your Zyxel Device to the new firmware version.
close	Click this to exit this screen without upgrading your Zyxel Device to the new firmware version.
	The following message appears when the Zyxel Device is checking the latest firmware version available on the cloud server. If it is later than your current firmware version on the Zyxel Device, you will be prompted to download it. Checking the latest firmware version available on the cloud server...

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 for more information.

Figure 160   Firmware Download Failed. Check Internet Access.
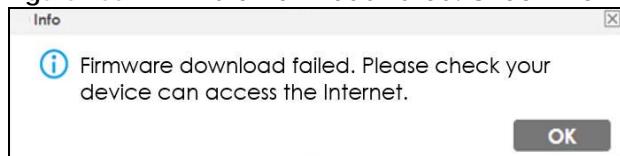

Firmware download failed due to a DNS problem. Please check your device's DNS settings.

Figure 161   Firmware Download failed. Check DNS Settings.
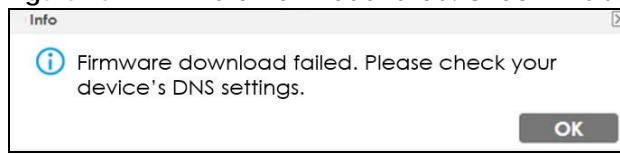
Firmware download failed. Download the new firmware manually from the Zyxel website. Then, go to the **Maintenance** > **File Manager** > **Firmware Package** screen to upload the new firmware.

Figure 162   Firmware Download Failed. Download Manually.
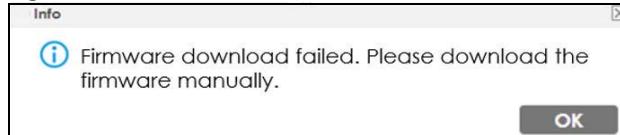
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Zyxel Device again.

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

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

Figure 163 Network Temporarily Disconnected

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

19.3.1 Example of Firmware Upload Using FTP

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

1 Connect your computer to the Zyxel Device.

2 The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 - 192.168.1.254.

3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Enter your user name when prompted.

5 Enter your password as requested.

6 Enter "hash" for FTP to print a `#' character for every 1024 bytes of data you upload so that you can watch the file transfer progress.

7 Enter "bin" to set the transfer mode to binary.

8 Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This examples uses `put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin`.

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

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

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

19.4 Shell Script

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

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

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

Figure 164 Maintenance > File Manager > Shell Script
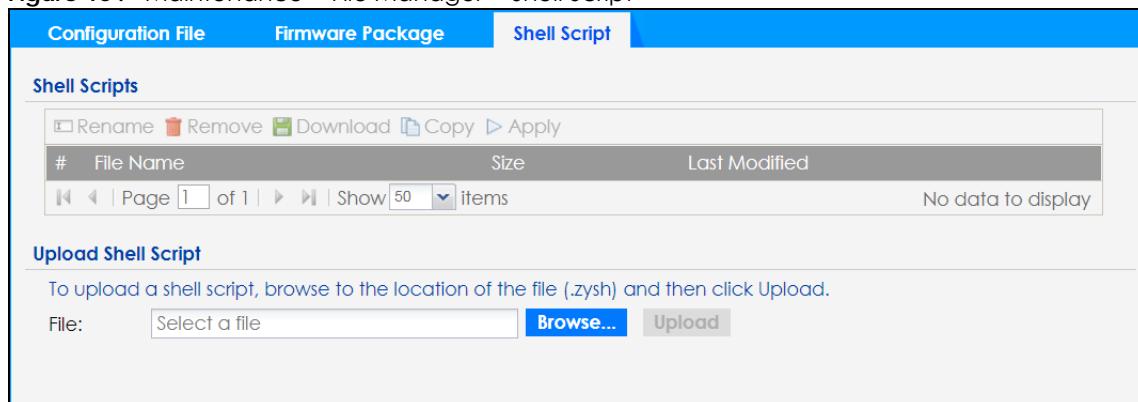
Each field is described in the following table.

Table 104 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 a-zA-Z0-9;`~!@#$%^&()_+[]{}',.=-).
	Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 104   Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device.
	A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device.
	Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen.
	Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).
	Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file.
	Click a shell script file's row to select it and click **Apply** to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	
The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.	
File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

CHAPTER 20
Diagnostics

20.1 Overview

Use the diagnostics screen for troubleshooting.

20.1.1 What You Can Do in this Chapter

- The **Diagnostics** screen (Section 20.2 on page 270) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Remote Capture** screen (Section 20.3 on page 271) enables remote packet captures on wired or wireless interfaces through an external packet analyzer.

20.2 Diagnostics

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

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

Figure 165 Maintenance > Diagnostics> Diagnostics
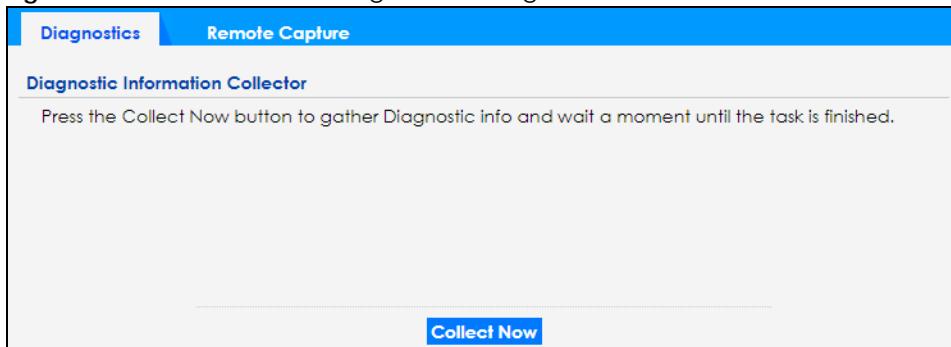
The **Debug Information Collector** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 166   Maintenance > Diagnostics: Debug Information Collector
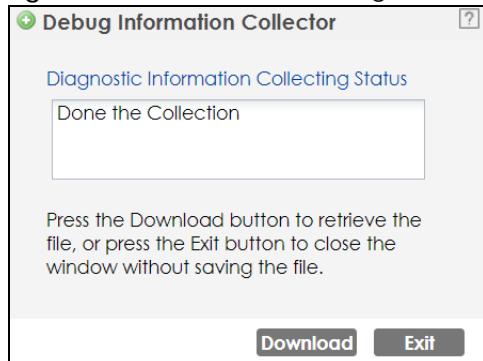
20.3 Remote Capture

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

Not all models support wireless remote capture. See for models that support remote capture on wireless interfaces.

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

Figure 167   Maintenance > Diagnostics > Remote Capture (Zyxel Device that supports Wireless Remote Capture)
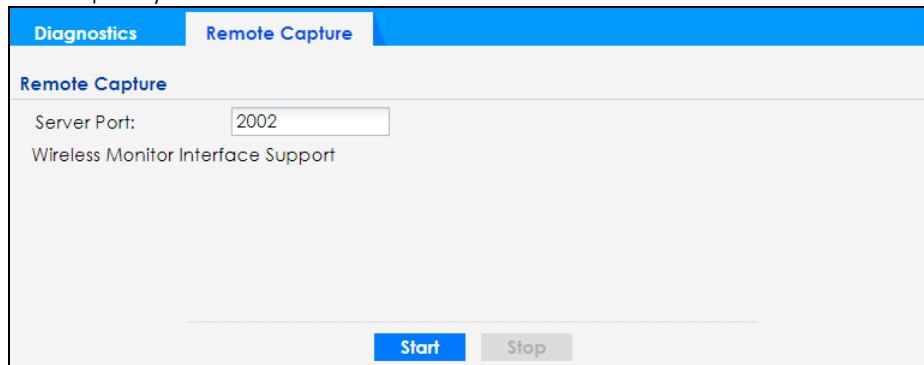
The following table describes the labels in this screen.

Table 105   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.

21.1 Overview

The LEDs of your Zyxel Device can be controlled such that they stay lit (ON) or OFF after the Zyxel Device is ready. There are two features that control the LEDs of your Zyxel Device – **Locator** and **Suppression**.

21.1.1 What You Can Do in this Chapter

- The **Suppression** screen (Section 21.2 on page 272) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The **Locator** screen (Section 21.3 on page 273) allows users to see the actual location of the Zyxel Device between several devices in the network.

21.2 Suppression Screen

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

You can go to the **Maintenance** > **LEDs** > **Suppression** screen to see the default LED behavior and change the LED suppression setting. After you make changes in the suppression screen, it will be stored as the default when the Zyxel Device is restarted. See (Section 1.2 on page 14) for information on default values for different models.

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

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

Figure 168   Maintenance > LEDs > Suppression
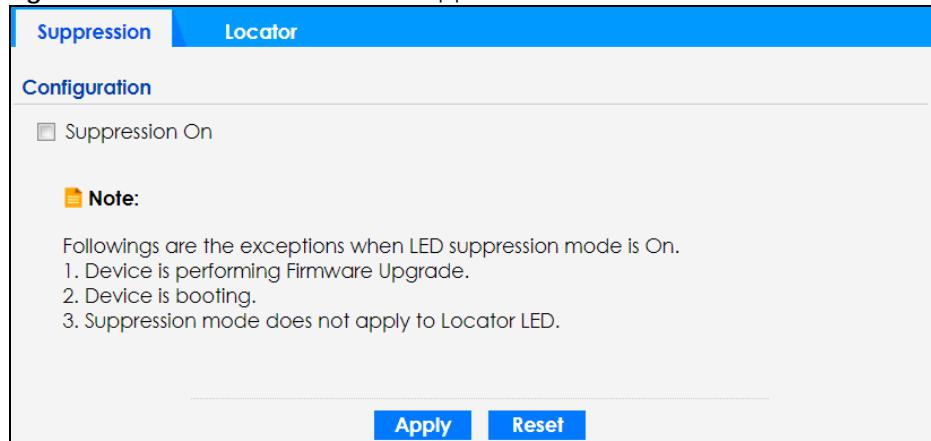
The following table describes fields in the above screen.

Table 106   Maintenance > LED > Suppression

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

21.3 Locator Screen

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

To run the locator feature, enter a number of minutes and click **Turn On** button to have the Zyxel Device find its location. The Locator LED will start to blink for the number of minutes set in the **Locator** screen. The default setting is 10 minutes. While the locator is running, the turn on button will gray out and return after it's finished. If you make changes to the time default setting, it will be stored as the default when the Zyxel Device restarts.

Note: The Locator feature is not affected by the Suppression setting.

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

Figure 169   Maintenance > LEDs > Locator
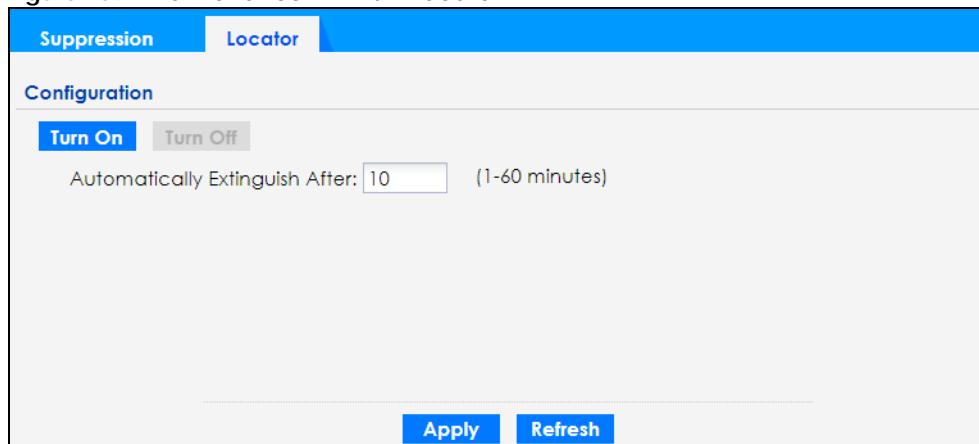
The following table describes fields in the above screen.

Table 107   Maintenance > LED > Locator

LABEL	DESCRIPTION
Turn On / Turn Off	Click **Turn On** button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network. Otherwise, click **Turn Off** to disable the locator feature.
Automatically Extinguish After	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. Default is 10 minutes.

Table 107   Maintenance > LED > Locator

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

CHAPTER 22
Antenna Switch

22.1 Overview

Use this screen to adjust coverage depending on the orientation of the antenna.

22.1.1 What You Need To Know

Positioning the antennas properly increases the range and coverage area of WiFi.

On the Zyxel Device that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the antenna orientation for the Zyxel Device radios using the Web Configurator, the command line interface (CLI) or a physical switch. See Section 1.2 on page 14 to see if your Zyxel Device comes with internal antennas and has an antenna switch. Check Section 1.2 on page 14 to see if your Zyxel Device has an antenna switch.

Figure 170   WAC Physical Antenna Switch
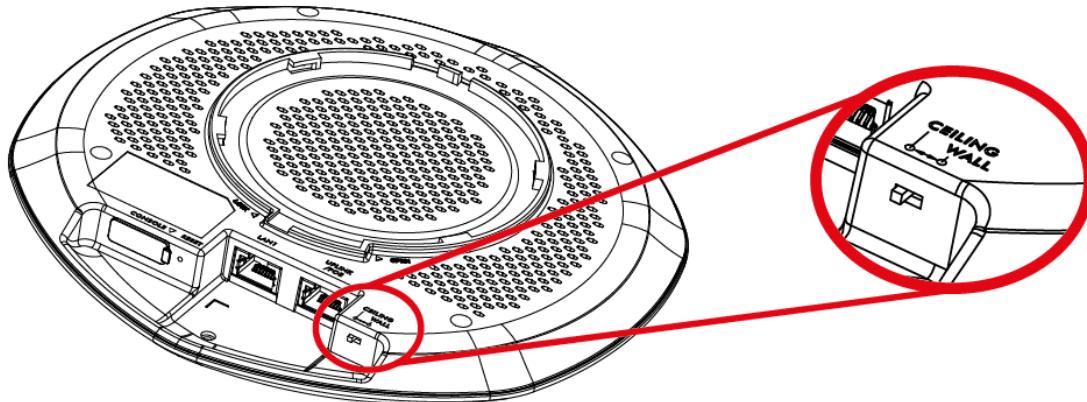
Note: With the physical antenna switch, you apply the same antenna orientation settings to both radios. You can set the radios to have different settings while using the Web Configurator or the command line interface.

Note: The antenna switch in the Web Configurator has priority over the physical antenna switch after you **Enable Software Control** in the **Maintenance > Antenna** screen. By default, software control is disabled.

22.2 Antenna Switch Screen

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

The screen varies depending on whether the Zyxel Device has a physical antenna switch or allows you to change antenna orientation settings on a per-radio basis or on a per-AP basis.

Figure 171   Maintenance > Antenna > Antenna Switch (Per Radio)

Figure 172   Maintenance > Antenna > Antenna Switch (Per AP)

If the Zyxel Device has a physical antenna switch, select the **Enable Software Control** option to use the Web Configurator to adjust coverage depending on each radio's antenna orientation for better coverage.

Select **Wall** if you mount the Zyxel Device to a wall. Select **Ceiling** if the Zyxel Device is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still wireless dead zones, and vice versa.

Click **Apply** to save your changes or click **Reset** to return the screen to its last-saved settings.

CHAPTER 23
Reboot

23.1 Overview

Use this screen to restart the Zyxel Device.

23.1.1 What You Need To Know

If you made changes in the Web Configurator, they were saved when you click **Apply**. They do not change when you reboot the Zyxel Device.

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 to reset; reset returns the Zyxel Device to its default configuration.

23.2 Reboot

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

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

Figure 173 Maintenance > Reboot

Each field is described in the following table.

Table 108   Maintenance > Reboot

LABEL	DESCRIPTION
Maintenance	
Enable the schedule	Select this checkbox to have your Zyxel Device restart at a specific time on selected days of the week. By scheduling a reboot, you can have the Zyxel Device refresh the network connections at a specified time, allowing automatic reconnection with WiFi clients in case of a connection failure.
Start time	Specify the time of the day (in 24-hour format) to have the Zyxel Device automatically restart. For example, 23:00 is 11:00 PM.
Week Days	Select each day of the week to have the automatically restart.
Apply	Click **Apply** to save your changes to the Zyxel Device.
Reboot Now	Click **Reboot Now** 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
# Local Configuration in Cloud Mode

CHAPTER 24
Cloud Mode

24.1 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 Cloud Mode Web Configurator screens by connecting directly to the LAN port of the Zyxel Device, and check if the Zyxel Device's VLAN setting or (manual) 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 174 Cloud Mode Application
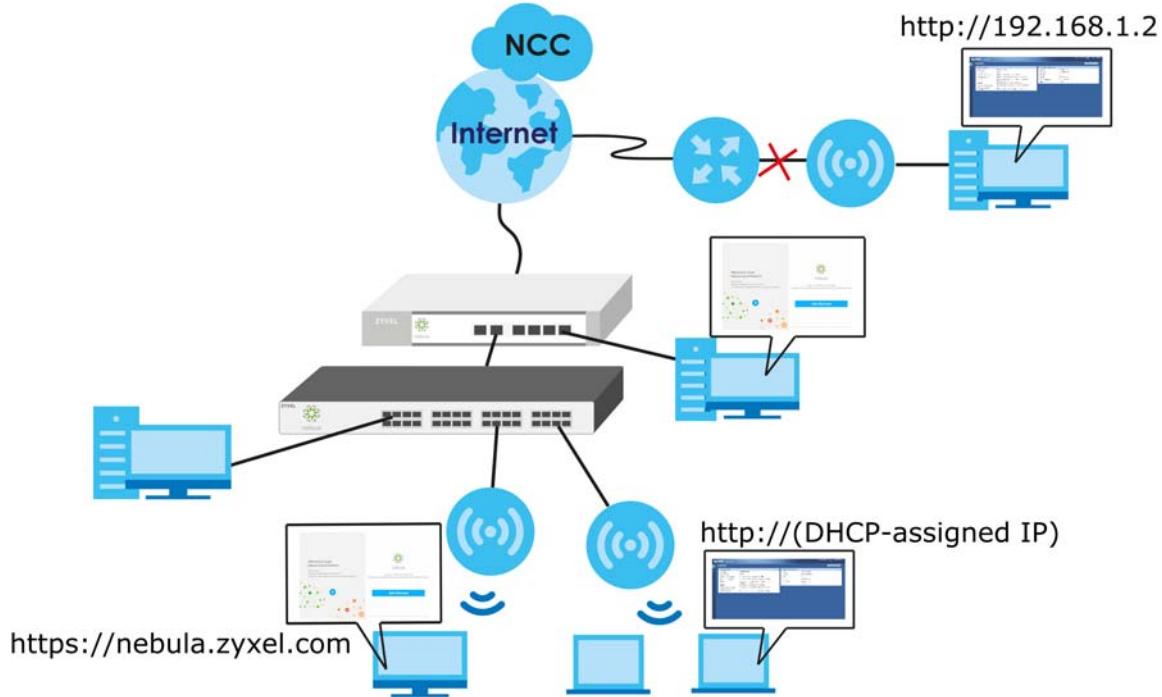
24.2 Cloud Mode Web Configurator Screens

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

- **Dashboard**
- **Configuration** > **Network** > **IP Setting**
- **Configuration** > **Network** > **VLAN**
- **Maintenance** > **Shell Script**
- **Maintenance** > **Diagnostics** > **Diagnostics**
- **Maintenance** > **Diagnostics** > **Remote Capture**
- **Maintenance** > **Log**

These screens also have fewer options than those in standalone Zyxel Devices. The rest of the Zyxel Device's features must be configured through the NCC.

24.3 Dashboard

This screen displays general AP information, and client information in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 175 Dashboard
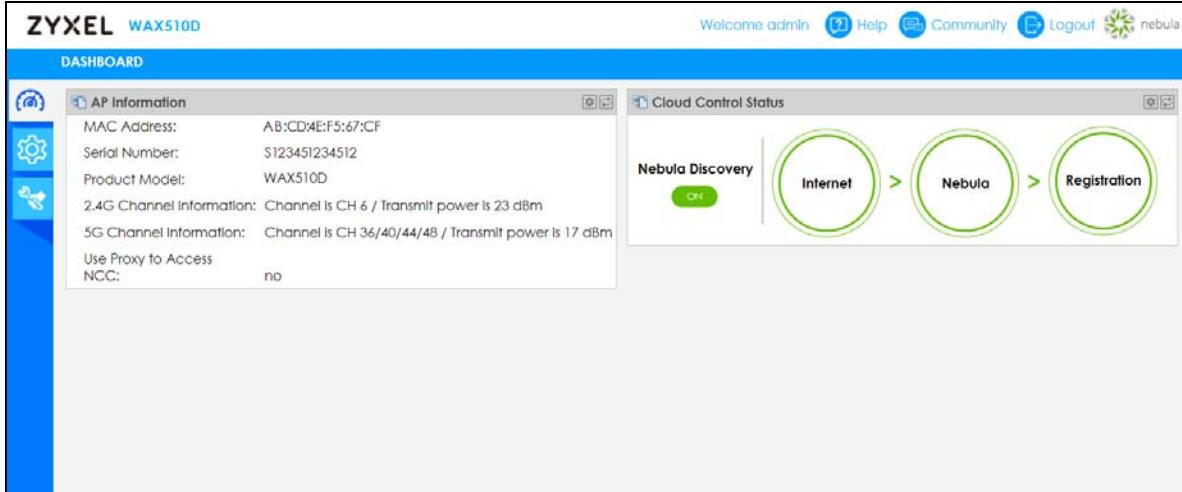
The following table describes the labels in this screen.

Table 109   Dashboard

LABEL	DESCRIPTION
AP Information	
MAC Address	This field displays the MAC address of the Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Product Model	This field displays the model name of the Zyxel Device.
2.4G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 2.4 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
5G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 5 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
Use Proxy to Access NCC	This displays whether the NAP uses a proxy server to access the NCC (Nebula Control Center).

Table 109   Dashboard (continued)

LABEL	DESCRIPTION
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.
Nebula Discovery	Slide the switch to the right to enable NCC discovery on the Zyxel Device. The Zyxel Device will connect to NCC and change to the NCC management mode if it: • is connected to the Internet. • has been registered on NCC. Note: The switch is always on and cannot be disabled when the Zyxel Device is in Cloud mode.

If the Zyxel Device cannot connect to the Internet or to NCC, move the mouse over the status circle to check the error message.
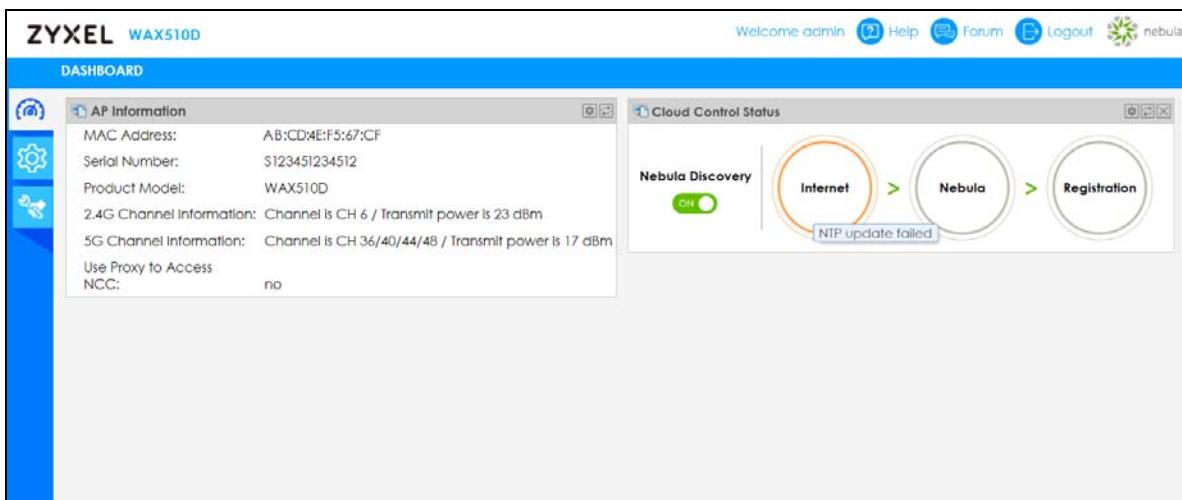
CHAPTER 25
Network

25.1 Overview

You can configure the management IP address and VLAN settings of your Zyxel Device in cloud mode in the **Network** screens.

See Section 10.1 on page 124 for information about IP addresses.

Note: Make sure your VLAN settings allow the Zyxel Device to connect to the Internet so you could manage it with NCC.

25.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 25.2 on page 283) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 25.3 on page 285) configures the Zyxel Device's VLAN settings.

25.2 IP Setting

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

Figure 176 Configuration > Network > IP Setting

Each field is described in the following table.

Table 110 Configuration > Network > IP Setting

LABEL	DESCRIPTION
IP Address Assignment	
IP Type	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.
Use Proxy to Access Internet	If the Zyxel Device is behind a proxy server, you need to select this option and configure the proxy server settings so that the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter service port number used by the proxy server.
Authentication	Select this option if the proxy server requires authentication before it grants access to the Internet.
User Name	Enter your proxy user name.
Password	Enter your proxy password.

Table 110   Configuration > Network > IP Setting (continued)

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

25.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings. See Section 10.3 on page 128 for more information about VLAN.

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

Figure 177 Configuration > Network > VLAN

Each field is described in the following table.

Table 111   Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device. If you change the default management VLAN ID, you need to use the new ID to access the Zyxel Device.
Untagged/ Tagged	Set whether the Zyxel Device adds the VLAN ID to outbound traffic transmitted through its Ethernet port.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 26
Maintenance

26.1 Overview

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

See Chapter 19 on page 256 for information about shell scripts.

26.1.1 What You Can Do in this Chapter

- The **Shell Script** screen (Section 26.2 on page 286) stores, names, downloads, and uploads shell script files.
- The **Diagnostics** screen (Section 26.3 on page 289) generates 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 (Section 26.4 on page 289) enables remote packet captures on wired or wireless interfaces through an external packet analyzer.
- The **Log > View Log** screen (Section 26.5 on page 290) displays the Zyxel Device's current log messages when it is disconnected from the NCC.

26.2 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 > 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 178   Maintenance > Shell Script

1 In the text editor, save the shell script with a .zysh filename extension. Select **All Files** as the file type.
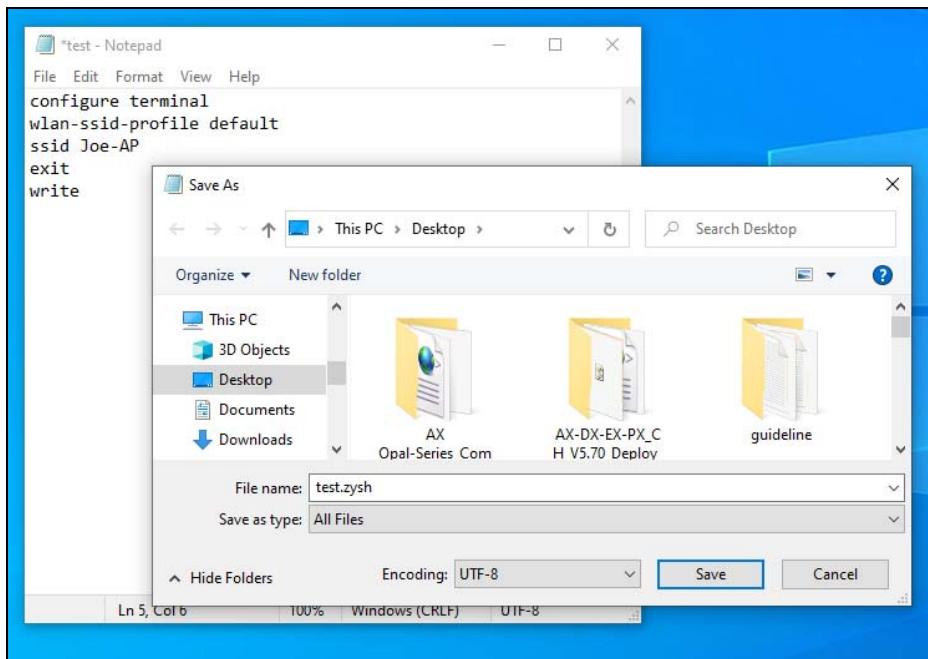
2 Go to the **Maintenance** > **Shell Script** screen. Click **Browse** to upload the .zysh file.
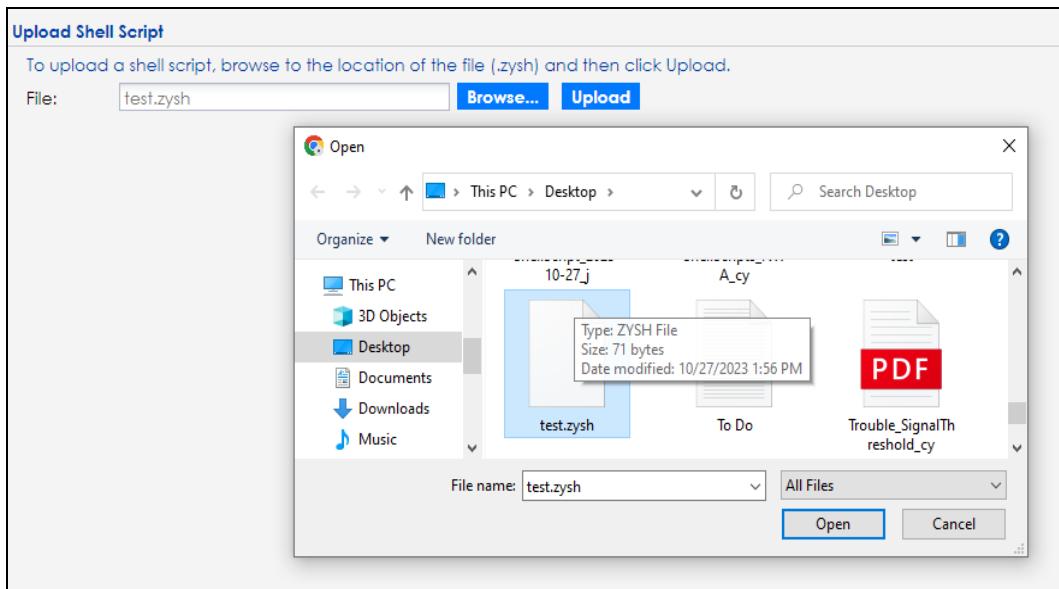
3 Click **Upload**. The uploaded shell script will be shown in the **Shell Scripts** field.

Each field is described in the following table.

Table 112   Maintenance > Shell Script

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

26.3 Diagnostics

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

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

Figure 179   Maintenance > Diagnostics
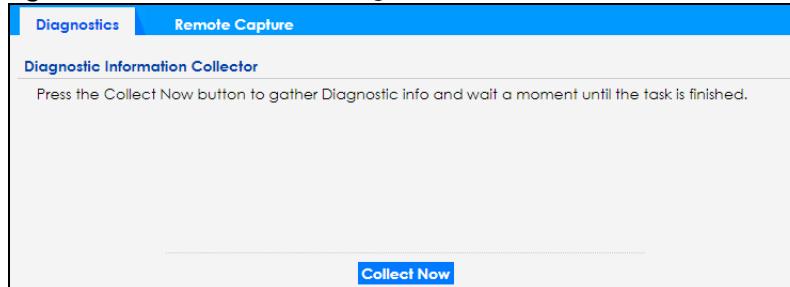
The **Debug Information Collector** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 180   Maintenance > Diagnostics: Debug Information Collector
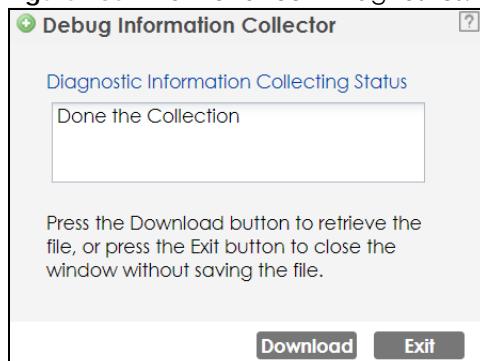
26.4 Remote Capture

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.

Note: Not all models support wireless remote capture. See Section 1.2 on page 14 for the models that support remote capture on wireless interfaces.

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

Figure 181 Maintenance > Diagnostics > Remote Capture (Zyxel Device that supports Wireless Remote Capture)
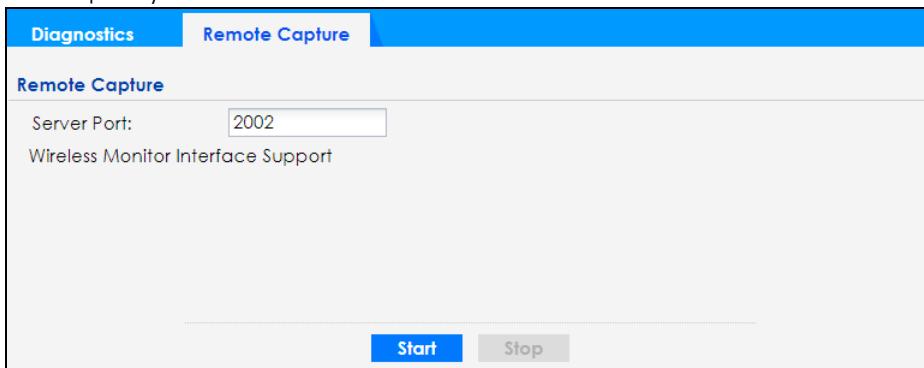
The following table describes the labels in this screen.

Table 113   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.

26.5 View Log

The NCC periodically gathers log files from the devices being managed by it. Before the NCC pulls logs from the Zyxel Device or when the Zyxel Device is disconnected from the NCC, you can use this screen to view its current log messages. To access this screen, click **Maintenance > Log**.

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

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

Figure 182 Maintenance > Log > View Log

The following table describes the labels in this screen.

Table 114   Maintenance > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Display** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.

Table 114   Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=x]", where x is a number, appears at the end of the **Message** field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.
Protocol	This field displays the service protocol in the event that generated the log message.
Note	This field displays any additional information about the log message.

PART III
Appendices and Troubleshooting

CHAPTER 27
Troubleshooting

27.1 Overview

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

- Power, Hardware Connections, and LED
- Zyxel Device Management, Access, and Login
- Internet Access
- WiFi Network
- Resetting the Zyxel Device

27.2 Power, Hardware Connections, and LED

The Zyxel Device does not turn on. The LED is not on.

1 Make sure you are using the power adapter included with the Zyxel Device or a PoE power injector/switch. If your Zyxel Device uses a type C power adapter, and you want to use your own type C adapter, ensure that the power supply is at least 45W.

2 Make sure the power adapter or PoE power injector/switch is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.

3 Disconnect and re-connect the power adapter or PoE power injector/switch. Check that you are using the correct PoE port on the PoE power injector/switch to supply power to the Zyxel Device.

4 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

5 If none of these steps work, you may have faulty hardware and should contact your Zyxel Device vendor.

The LED does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 3.3 on page 44.

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.

27.3 Zyxel Device Management, Access, and Login

I forgot the IP address for the Zyxel Device.

1 The default in-band IP address in standalone mode is **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 Section 27.6 on page 304.

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 (in standalone mode) is 192.168.1.2.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Zyxel Device.

2 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 3.3 on page 44.

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 Section 27.6 on page 304.

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

Advanced Suggestions

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

I forgot the Web Configurator password.

1 The default password is **1234**. If the Zyxel Device is connected to the NCC and registered, check the NCC for the password.

2 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 27.6 on page 304.

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.

- If the Zyxel Device is in standalone mode, the default password is **1234**. If you have changed the username and password, use the ones you configured to log in.
- If the Zyxel Device is in cloud mode, use the Nebula **Local credentials Password** to log into the cloud 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 a controller such as the NXC or ZyWALL, then use the controller 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 Section 2.3 on page 36 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 Section 27.6 on page 304.

I cannot use FTP to upload or download the configuration file.

Ensure you have enabled FTP in the **Configuration** > **System** > **FTP** screen.

I cannot upload the firmware uploaded using FTP.

The Web Configurator is the recommended method for uploading firmware in standalone mode. For managed Zyxel Devices, using the NCC or AC is recommended. You only need to use FTP if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

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 enabled **NCC Discovery**, but the Zyxel Device is still in standalone mode.

Make sure your Zyxel Device is registered to the NCC. See Section 2.2 on page 35 for more information.

I cannot register the Zyxel Device in NCC because it's 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 standalone 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   Make sure that NCC Discovery is enabled (see Section 10.6 on page 135).

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

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

4 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.

5 Check your network's VLAN settings (see Section 10.3 on page 128). 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.

6 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.

7 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. Or, set the DNS server address in the Zyxel Device Web Configurator. Go to **Configuration** > **Network** > **IP Setting**, select **Use Fixed IP Address**. Set the **DNS Server IP Address:** to 8.8.8.8. Click **Apply**.

I want to switch from NCC to AP Controller (AC) management, but I could not find the **AC Discovery** menu in the Zyxel Device Web Configurator.

---

1 Unregister the Zyxel Device from the NCC. See the NCC User's Guide for more information.

2 Reset your Zyxel Device to the factory defaults.

3 Make sure that your Zyxel Device is in the same subnet as the AC, and enable **AC Discovery** in **Configuration** > **Network** > **AC Discovery**.

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 1-2 minutes for the changes to take effect.

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

When a log reaches the maximum number of log messages (see Section 1.2 on page 14), 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.

My Zyxel Device's CPU usage is too high.

The Zyxel Device may receive too many HTTPS connection requests. Do the following to reduce the number of HTTPS connection requests:

Go to **Configuration** > **Object** > **User** > **Setting** and select **Limit the number of simultaneous logons for administration account**. Set a number in **Maximum number per administration account** to limit the number of simultaneous logins for each admin.

How do I set up multiple Access Points (APs)?

Avoid positioning APs in direct line of sight of each other, as this can cause interference and reduce the overall performance of your WiFi network.

In case, it may be necessary to position APs in direct line of sight of each other, you can:

- Adjust the transmit power of each AP in the **Configuration** > **Wireless** > **AP Management** screen, so that they are not using too much power and overlapping too much with each other.
- Configure the APs to operate on non-overlapping channels, such as channels 1, 6, and 11 in the 2.4 GHz band, 5 GHz band or 6 GHz band's channels or enabling DCS to let APs scan the best channel to use. This can help to minimize co-channel interference between the APs.

I only want certain users to access specific parts of my network.

See Section 8.4.6 on page 98 for more information on how to allow certain users to access only specific parts of your network.

I only want admins to use HTTPS or SSH to access the Zyxel Device.

See Section 8.8 on page 110 for more information on how to configure access to the Zyxel Device.

27.4 Internet Access

Clients cannot access the Internet through the Zyxel Device.

1   Check the Zyxel Device's hardware connections, and make sure the LEDs are behaving as expected (refer to Section 3.3 on page 44). See the Quick Start Guide and Section 27.1 on page 294.

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. If you select **Tagged** (**As Native VLAN**) in the **Configuration > Network > VLAN** screen, traffic going out from the Zyxel Device Ethernet port will be tagged with the **Management VLAN ID** you set. 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 Section 3.3 on page 44. 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 AC.

4   Check the settings for QoS. If it is disabled, activate it. When enabled, raise or lower the priority for some applications.

5   If the problem continues, contact the network administrator or vendor.

27.5 WiFi Network

I cannot connect to the Zyxel Device WiFi network.

1   Check the Zyxel Device LED status to make sure the Zyxel Device WiFi is on.

2   Make sure your WiFi client is within transmission range of the Zyxel Device.

3   Make sure you enter the correct SSID, password (**Pre-Shared Key**). They are case-sensitive. See the Zyxel Device back label for the default SSID and password.

4   Make sure your WiFi client is using the same WiFi security type (none, Enhanced-open, WEP, WPA, WPA2, WPA3) as the Zyxel Device. If you have previously changed the security settings, remove the SSID profile on the client device. Reconnect again using the correct SSID, password and security type.

5   Make sure the DHCP server is working properly. For example, the client may receive a private IPv4 address such as 192.168.1.x where x is a number for 2 to 254. If the client gets an address like 169.x.x.x, it means the client didn't get a valid IP address from the DHCP server.

6   Make sure the DNS server is working properly. If you can ping an IP address, but cannot ping its related URL, then it means there is a DNS server connection issue. For example, if you can ping 8.8.8.8 successfully but fail to ping google.com, there may be a DNS resolution issue.

7   Make sure the WiFi adapter on your WiFi client is working properly.

8   Make sure the wireless adapter on your WiFi client is IEEE 802.11 compatible and supports the same WiFi standard as the Zyxel Device's active radio. For example, 6 GHz WiFi networks are only available for WiFi clients that support WiFi 6E or higher standards.

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.
- To ensure the connected WiFi clients receive strong WiFi signal, adjust the minimum signal strength between the Zyxel Device and its WiFi clients by going to the **Configuration** > **Object** > **AP Profile** > **Radio** screen and selecting **Enable Signal Threshold**. To apply the settings to your Zyxel Device, go to the **Configuration** > **AP Management** > **AP Group** screenand select the **Profile Name** you just created.
- 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.

Too many people are downloading movies in my network.

Bandwidth restriction controls the amount of network traffic that WiFi clients can consume. This prevents the WiFi clients from downloading too many movies and slowing down other devices on the network. See Section 8.3 on page 90 for more information on how to restrict network bandwidth for each WiFi client.

Unauthorized users have accessed my wireless LAN.

- WEP is extremely insecure. It is recommended that you use the strongest security mechanism that all the WiFi devices in your network support. WPA2, WPA2-Mix or WPA3 are recommended. See Section 8.3 on page 90 for how to change security settings for a WiFi network.
- Rogue AP is an unauthorized access point in the network that poses a security threat. See Section 8.4.3 on page 93 for how to set up rogue AP detection.
- A MAC filter list blocks or allows a list of clients based on their MAC addresses, ensuring only authorized clients can access the network. See Section 8.4.5 on page 97 for more information about MAC filter.

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 forgot the WiFi password.

- If the Zyxel Device is connected to the NCC and registered, the WiFi password can be found in **Configure** > **Access points** > **SSID advanced settings** > **Choose the SSID** in the NCC portal.
- If the Zyxel device is in standalone mode, you can change the WiFi password by going to **Configuration** > **Edit SSID Profile** > **Edit Security Profile** in the Web Configurator, selecting **Personal**, and entering the new password in the **Pre-Shared Key** field.

I cannot import a certificate into the Zyxel Device.

1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

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

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

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

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

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

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

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

- Check that the AP profile which contains the load balancing settings is correctly assigned to the Zyxel Devices in question.
- The load balancing task may have been terminated because further load balancing on the Zyxel Devices in question is no longer required.

27.6 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following procedure to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

1 Make sure the Power LED is on and not blinking.

2 Press the **RESET** button and hold it until the Power LED begins to blink. (This usually takes about ten seconds.)

3 Release the **RESET** button, and wait for the Zyxel Device to restart.

You should be able to access the Zyxel Device in standalone mode using the default settings.

27.7 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.**
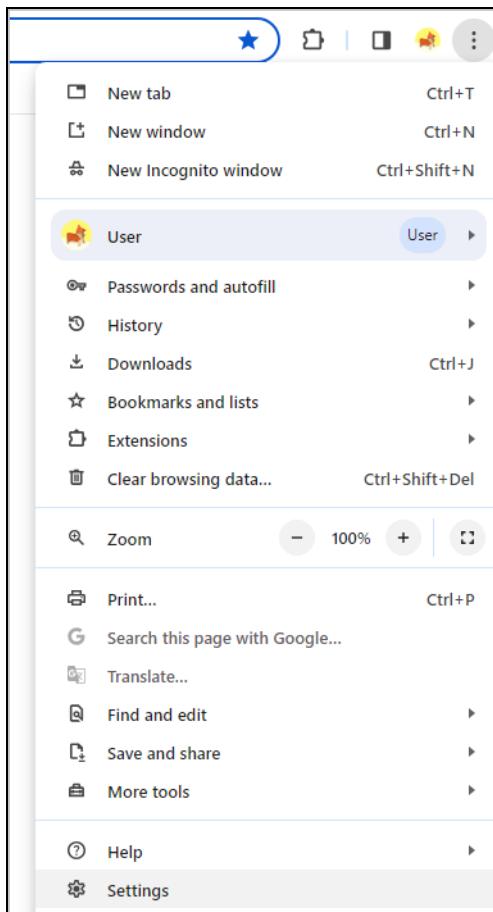

2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates.** In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates.**
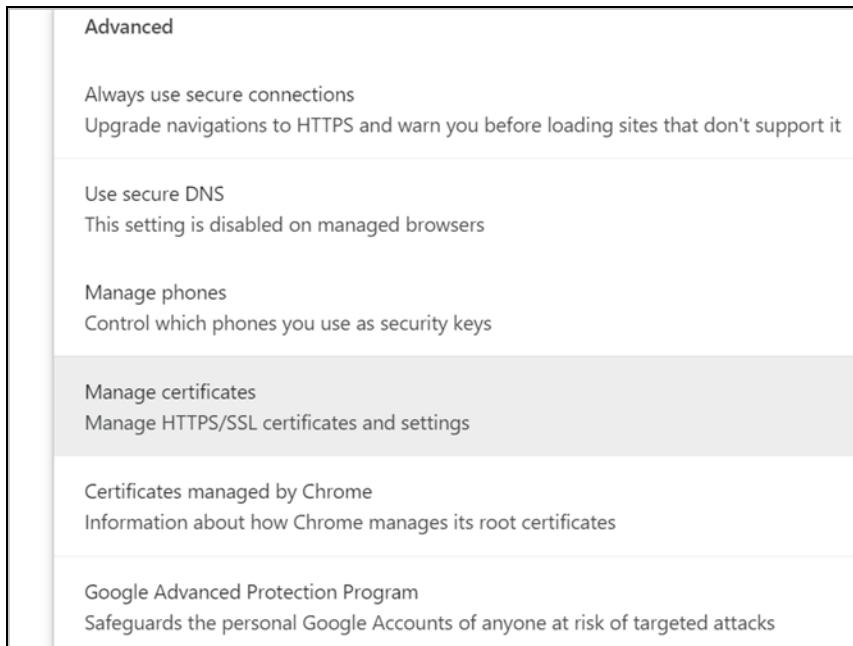
**3** Select the **Trusted Root Certification Authorities** tab and click **Import**.
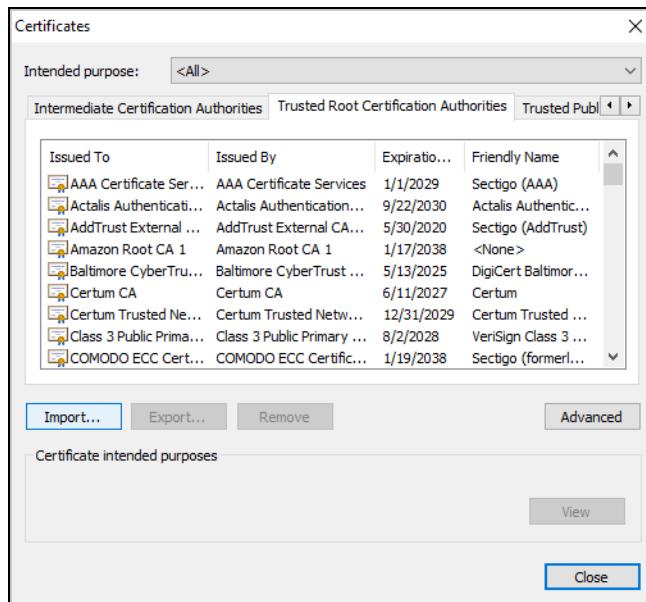
**4** Click **Next** to proceed to the **Certificate Import Wizard**.
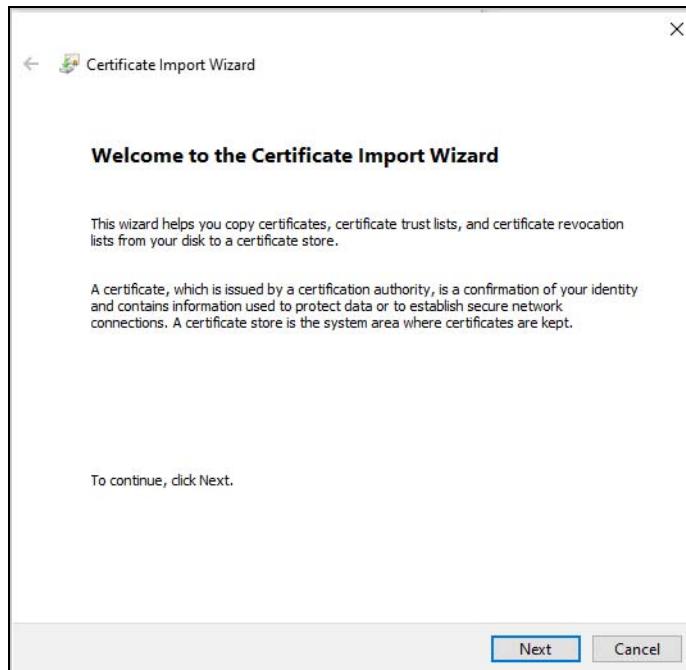
5 Click **Browse** to select a certificate already saved in your computer and click **Next** to continue.
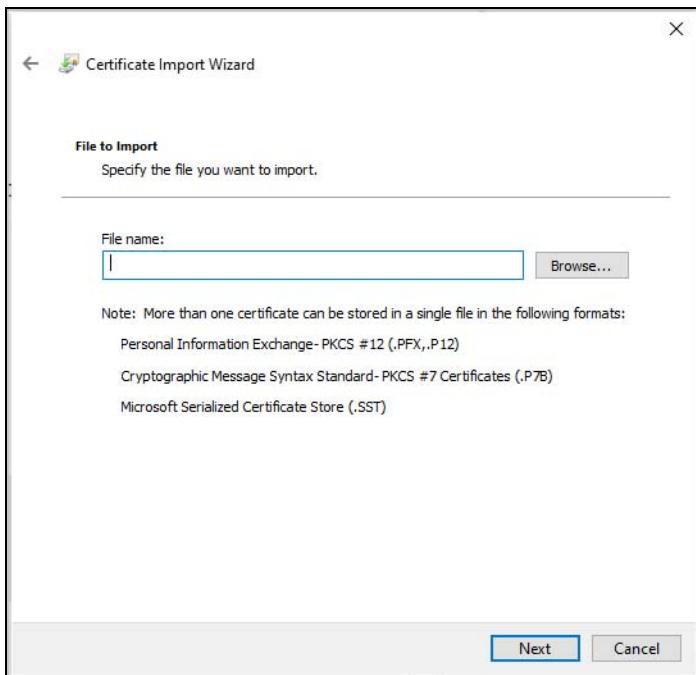
Select **All Files** to find the certificate in your computer.
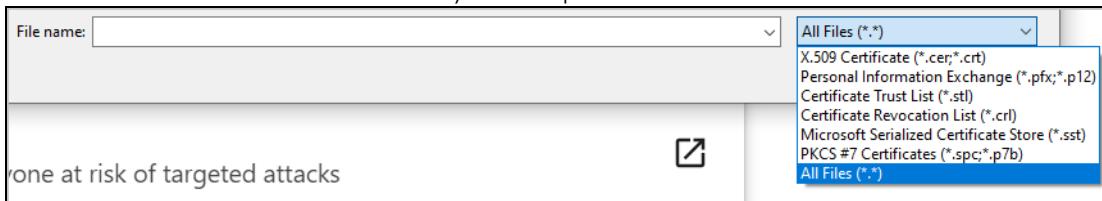
6 Two options are available for certificate stores. One is **Automatically select the certificate store based on the type of certificate**. This means the certificate import wizard can identify from the certificate whether it is a CA certificate or a personal certificate, and install it into the appropriate 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**.
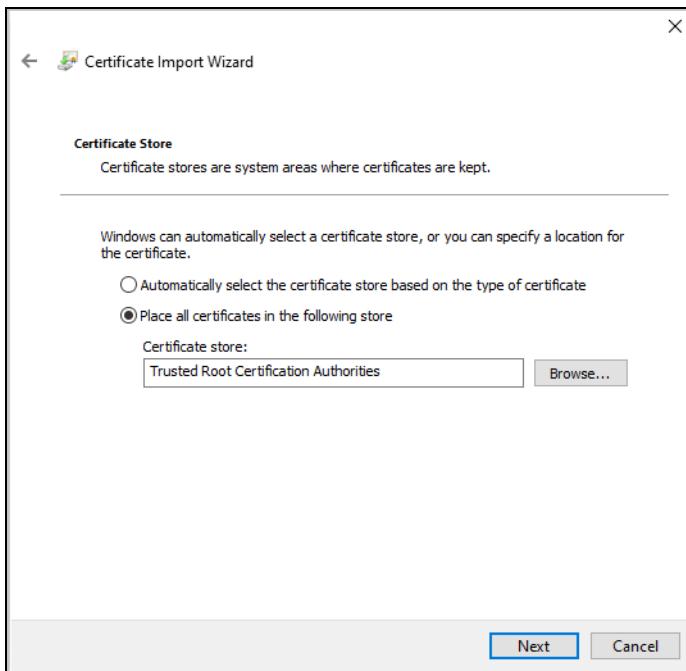
7 The security warning message shows up and click **Yes.**
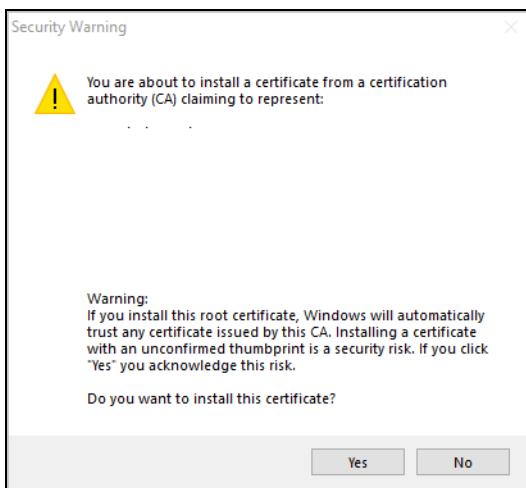
8 Click **Finish.**
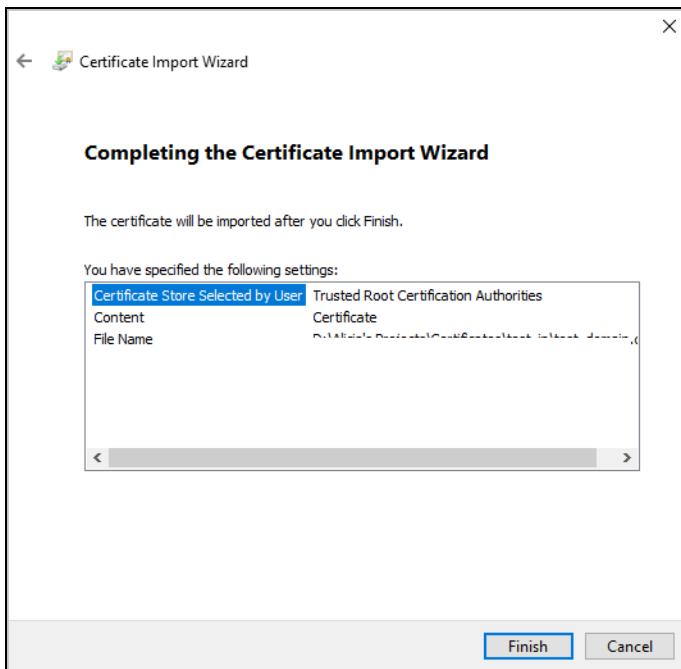
When you click **Finish**, a pop-up screen informs you about import completion.
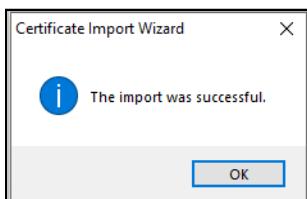
Remove a Certificate in Google Chrome and Microsoft Edge

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**.
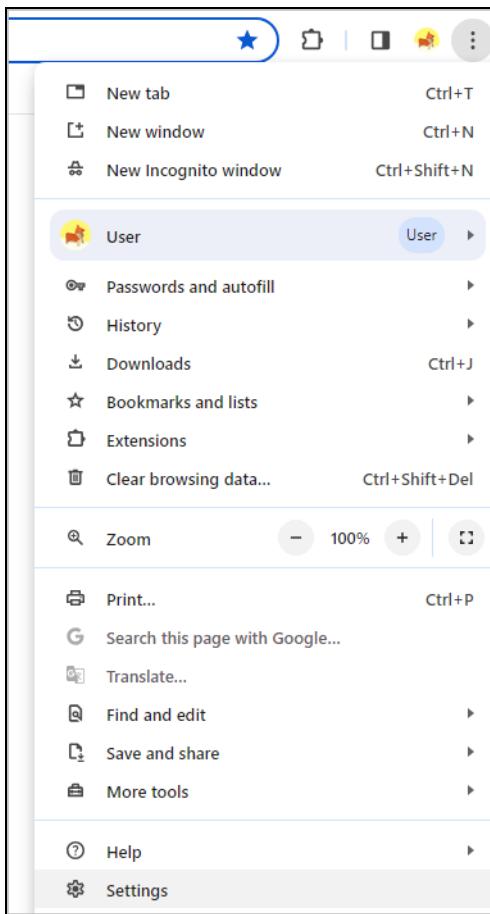
2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates.** In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.
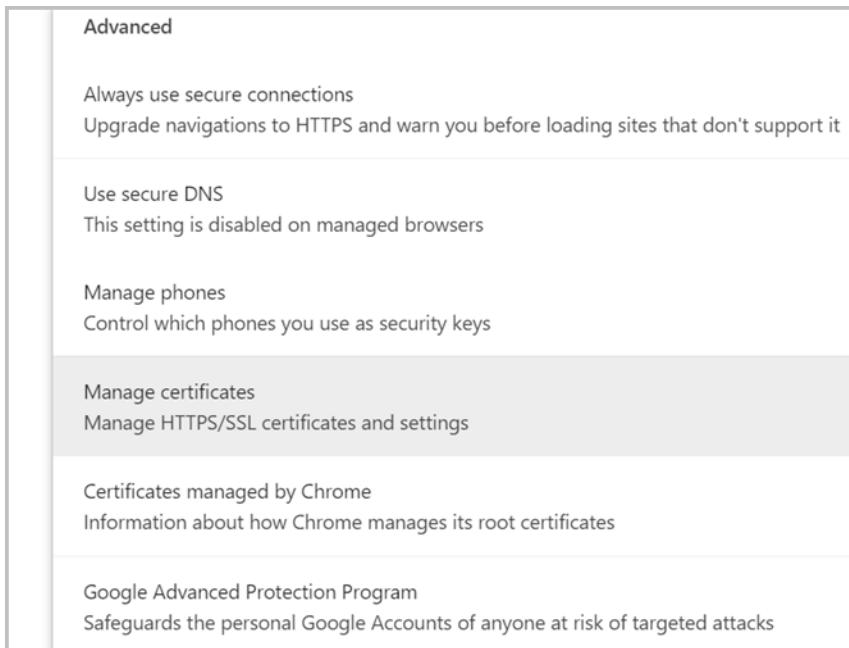
3 In the **Certificates** pop-up screen, select the **Trusted Root Certification Authorities** tab.
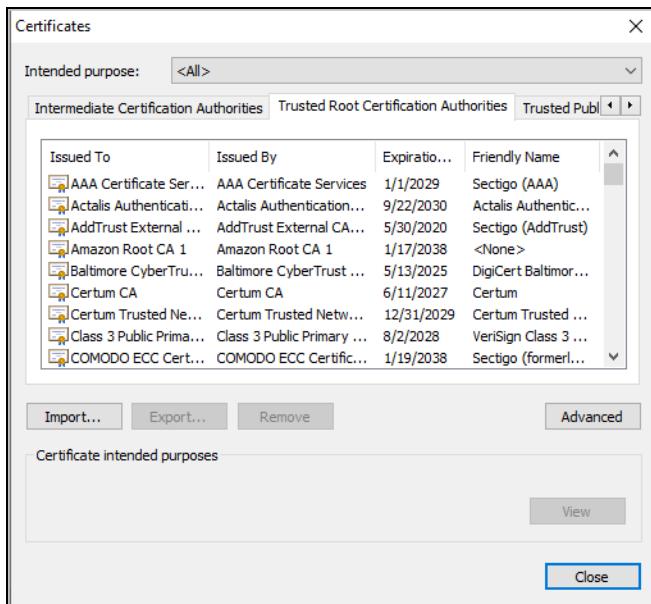
4 Select the certificate you want to remove and click **Remove**.

**5** Click **Yes** when you see the following warning message.
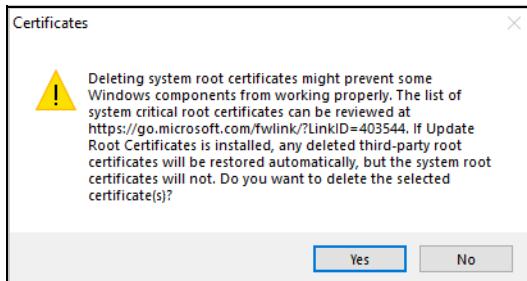
6 Confirm the details displayed in the warning message and click **Yes**.
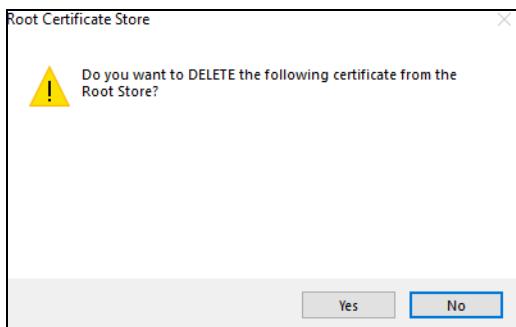
Import a Certificate to Mozilla Firefox

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**.
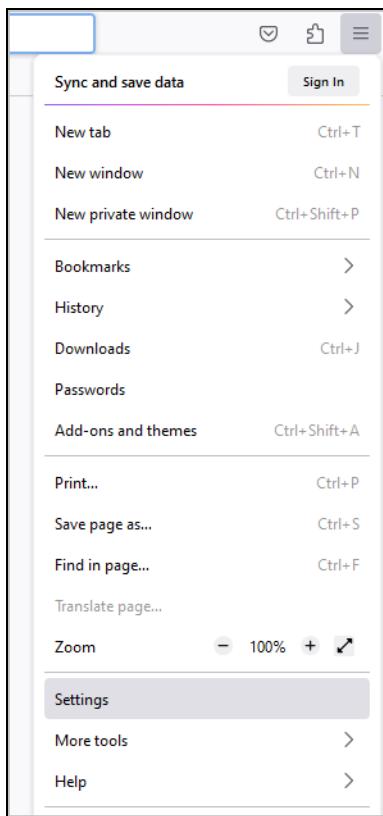

**2** Click **Privacy & Security**.
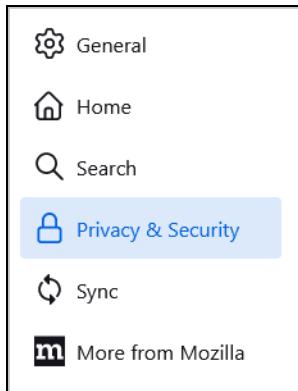
3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.
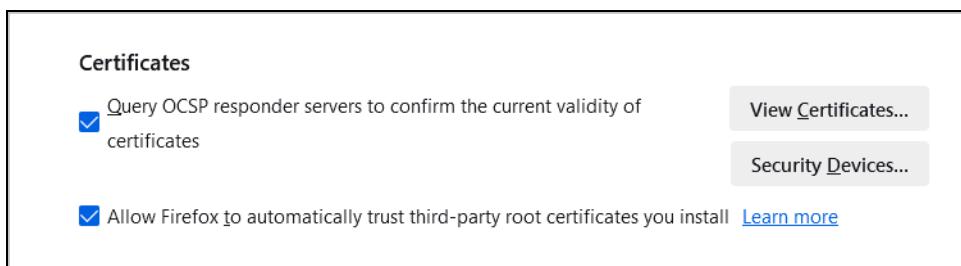
4 After the **Certificate Manager** displays, select the **Authorities** tab and click **Import**.

Certificate Manager				✕
Your Certificates	Authentication Decisions	People	Servers	Authorities

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		

View...   Edit Trust...   **Import...**   Export...   Delete or Distrust...

OK

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.

Downloading 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).

View   Examine CA certificate

OK   Cancel

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**.
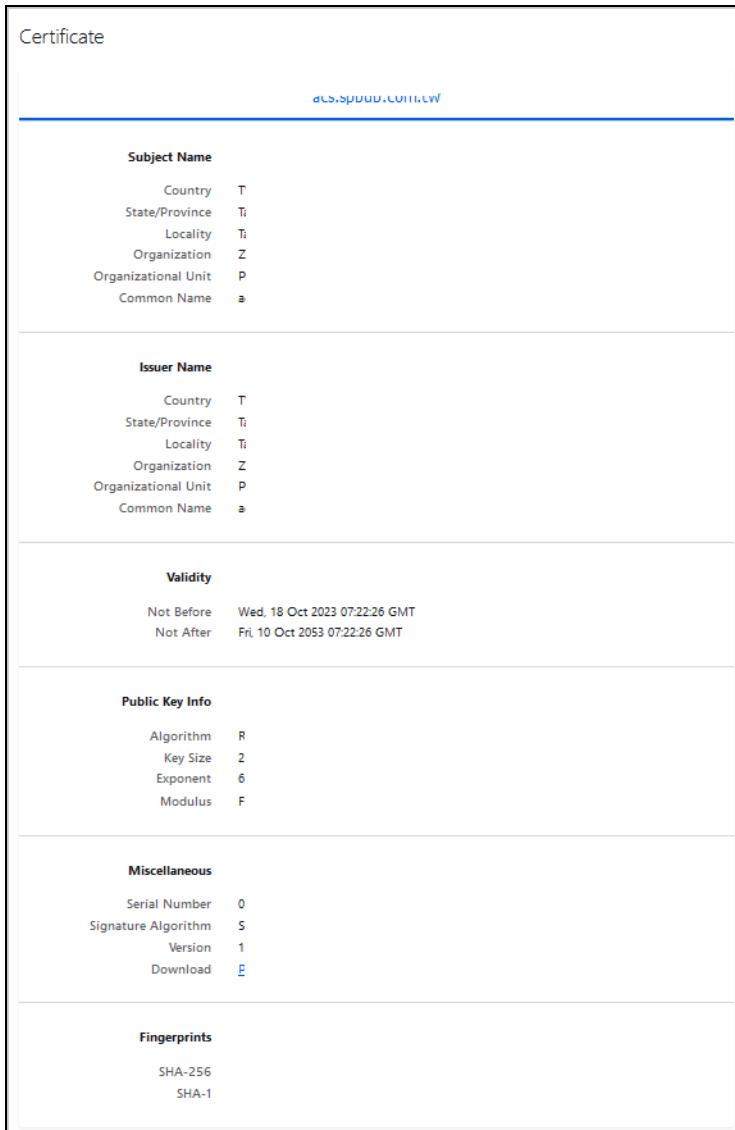
The certificate file is installed in Firefox now.

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.
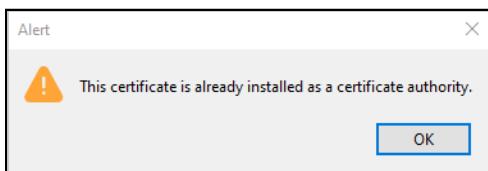

Removing a Certificate in Firefox

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**.
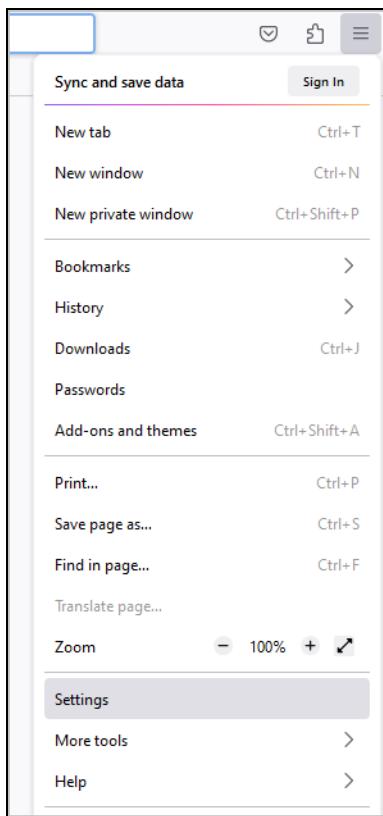
2 Click **Privacy & Security**.
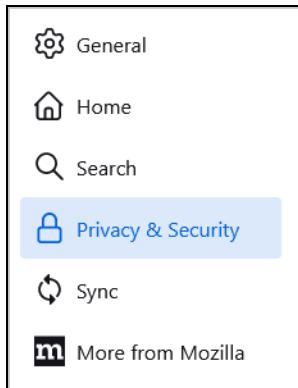
3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.
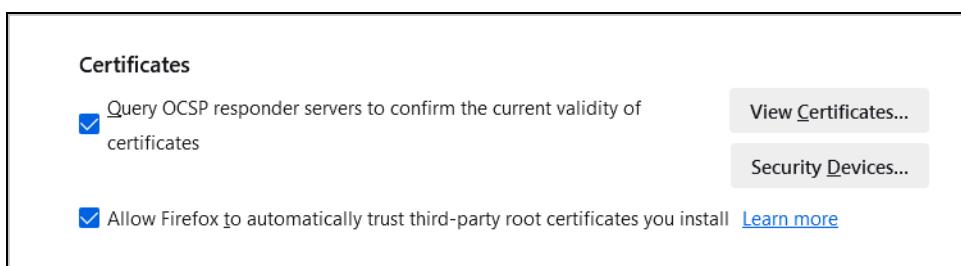
4 In the **Certificate Manager**, click **Authorities** and select the certificate you want to remove. Click **Delete or Distrust**.
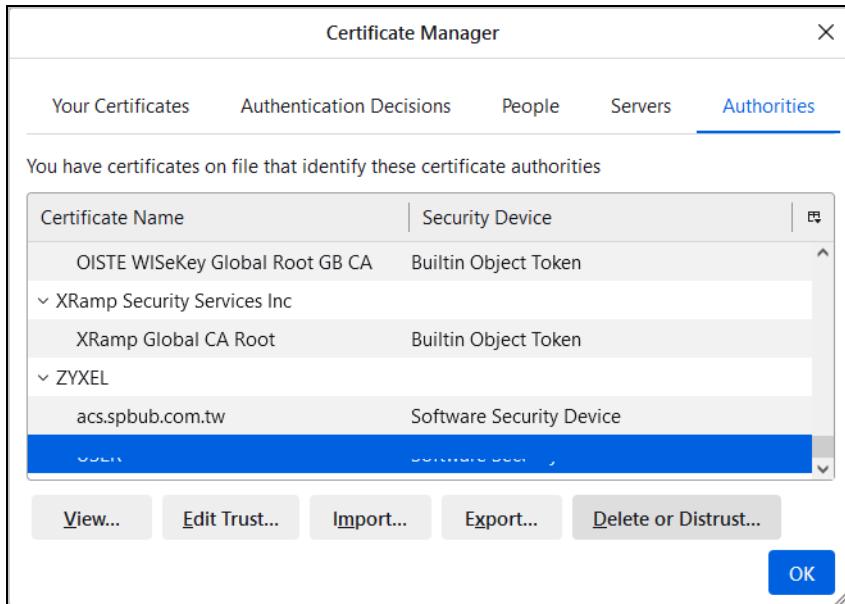
5 In the following dialog box, click **OK**.
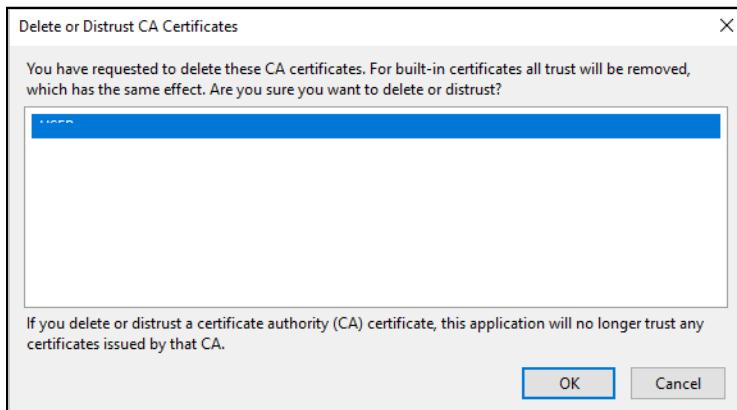
6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

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 3.4×10^{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 115   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 116   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 117   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
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

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

Interface ID

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

EUI-64

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

Table 118

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

Table 119

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.

---

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

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

Identity Association

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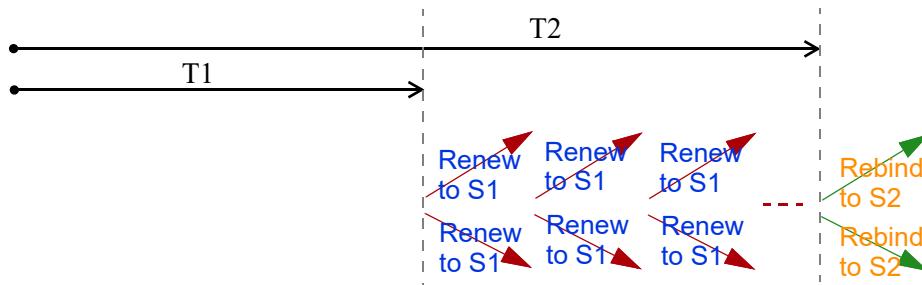
DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

• Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.

• Neighbor advertisement: A response from a node to announce its link-layer address.

• Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.

• Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

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

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

Multicast Listener Discovery

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

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive

multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

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

MLD filtering controls which multicast groups a port can join.

MLD Messages

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

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

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.
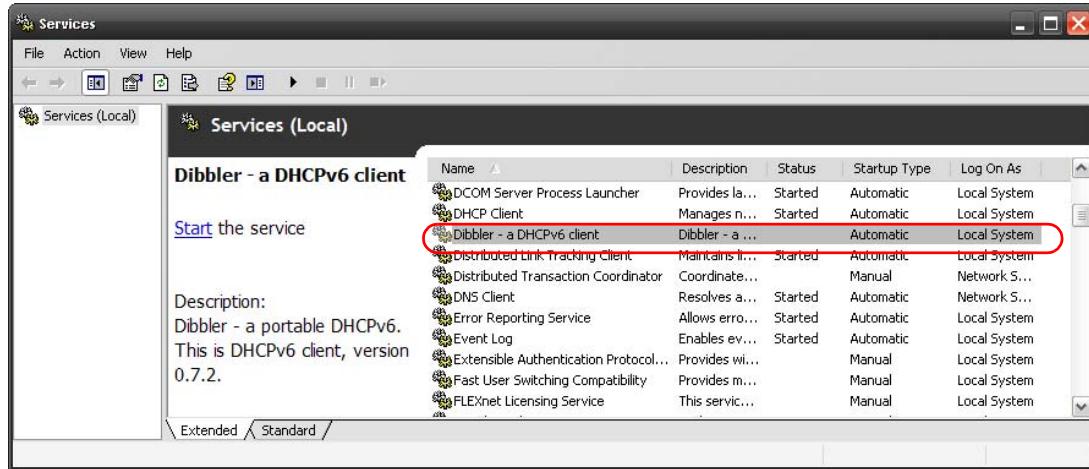

5 Click **Start** and then **OK**.
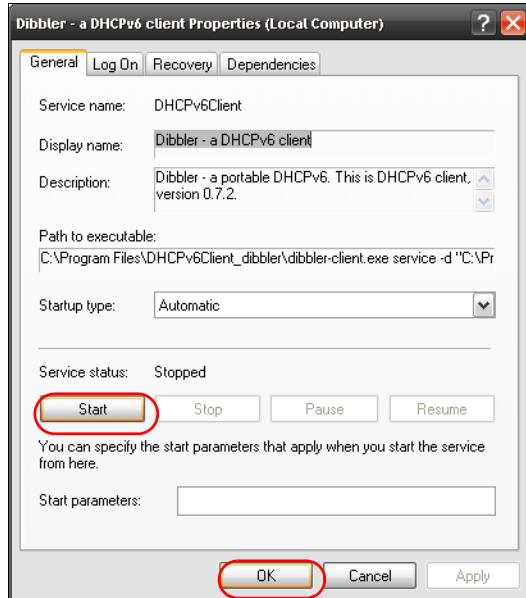
6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.
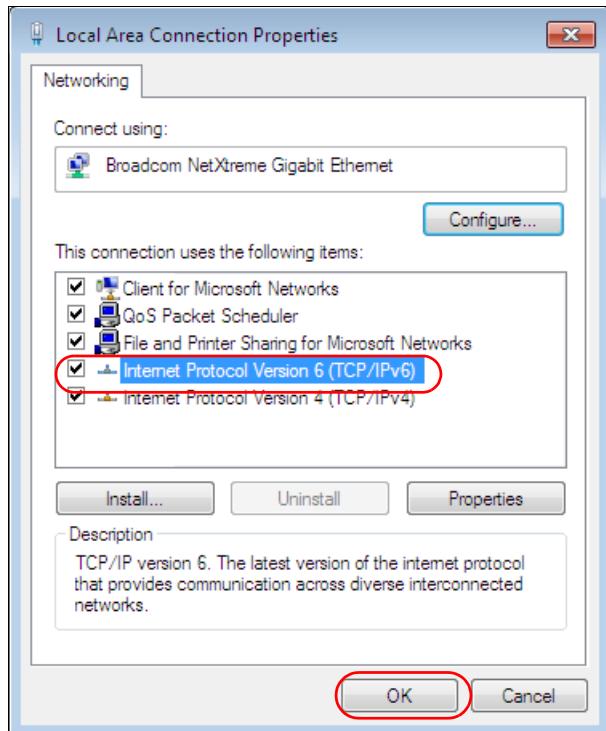
4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX C
Customer Support

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

For Zyxel 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

Copyright © 2024 by Zyxel and/or its affiliates

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

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimers

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

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

Trademarks

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

Regulatory Notice and Statement

United States of America

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

FCC 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 according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this 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. This transmitter must be at least 25 cm (WBE660S) from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.

Caution (for model – WAX620D-6E/NWA220AX-6E/WAX640S-6E/WBE660S/NWA130BE/WBE530)

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Brazil

The following applies if you use the product within Brazil.

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Canada

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

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-003 (B)/NMB-003(B)

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

- 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 2468C-11ACAP22W (WAC500H), 2468C-11ACAP22 (WAC500 and NWA1123ACv3), 2468C-WAX650S (WAX650S), 2486C-11AXAP24 (NWA210AX, WAX610D and WAX630S), 2468C-11AXAP22 (NWA110AX and WAX510D), 2468C-11AXAP2246E (WAX640S-6E), 2468C-11AXAP246E (WAX620D-6E, NWA220AX-6E), 2468C-03785 (WAX655E), 2468C-03973 (WAX300H), 25830-04011 (NWA130BE and WBE530), and 25830-04157 (WBE630S,WBE510D, NWA210BE and NWA110BE) 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

ANTENNA MODEL	NO.	TYPE	CONNECTOR	2.4 G GAIN (dBi)	5G/6G GAIN (dBi)	REMARK
WAX630S		PIFA	U.FL	0.92	1.32 (5150-5250 MHz) 1.39 (5250-5350 MHz) 0.44 (5470-5725 MHz) 1.63 (5725-5850 MHz)	
WAX650S		Direction	U.FL	0 (2400-2483.5 MHz)	3.51 (5150-5250 MHz) 4.22 (5250-5350 MHz) 4.61 (5470-5725 MHz) 4.68 (5725-5850 MHz)	
WAX510D NWA110AX	1	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	2	PIFA	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	3	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	4	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
NWA210AX WAX610D	1	Dipole	I-PEX		U-NII-1:7.8 dBi U-NII-2A:7.7 dBi U-NII-2C:6.8 dBi U-NII-3:7.2 dBi	
	2	PIFA	I-PEX	5.08 dBi		
	3	PIFA	I-PEX	5.56 dBi	U-NII-1:7.5 dBi U-NII-2A:6.8 dBi U-NII-2C:6.5 dBi U-NII-3:7.6 dBi	
	4	Dipole	I-PEX	6.06 dBi	U-NII-1:8.19 dBi U-NII-2A:7.7 dBi U-NII-2C:7.14 dBi U-NII-3:7.6 dBi	Wall Mount
	5	Dipole	I-PEX		U-NII-1:6.8 dBi U-NII-2A:7.5 dBi U-NII-2C:5.81 dBi U-NII-3:6.99 dBi	Ceiling Mount
	6	Dipole	I-PEX		U-NII-1:8.3 dBi U-NII-2A:7.8 dBi U-NII-2C:7.1 dBi U-NII-3:7.98 dBi	
WAC500H	1	PIFA	N/A	0 dBi	2.5 dBi	
	2	PIFA	N/A	0 dBi	2.5 dBi	
WAC500 NWA1123ACv3	1	PIFA	N/A	0 dBi	0 dBi	
	2	PIFA	N/A	0 dBi	0 dBi	
WAX640S-6E		PIFA	U.FL	1 dBi	U-NII-1:4.86 dBi U-NII-2A:5.93 dBi U-NII-2C:4.08 dBi U-NII-3:5.21 dBi U-NII-5:3.29 dBi U-NII-6:3.34 dBi U-NII-7:2.64 dBi U-NII-8:3.35 dBi	
WAX620D-6E NWA220AX-6E		PIFA	U.FL	1 dBi	U-NII-1:3.87 dBi U-NII-2A:3.96 dBi U-NII-2C:4.54 dBi U-NII-3:3.04 dBi U-NII-5:3.87 dBi U-NII-6:4.26 dBi U-NII-7:5.34 dBi U-NII-8:3.42 dBi	
WAX655E		Dipole	N type	4 dBi	6 dBi	

ANTENNA MODEL	NO.	TYPE	CONNECTOR	2.4 G GAIN (dBi)	5G/6G GAIN (dBi)	REMARK
WAX300H	1	PIFA	N/A	1.4	4.2 (5150-5250 MHz) 4.6 (5250-5350 MHz) 5.1 (5470-5725 MHz) 5.1 (5725-5850 MHz)	
	2	PIFA	N/A	2.7	3.2 (5150-5250 MHz) 3.5 (5250-5350 MHz) 3.5 (5470-5725 MHz) 4.3 (5725-5850 MHz)	

- For indoor use only (except WAX655E).

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

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna 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 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio 2468C-11ACAP22W (WAC500H), 2468C-11ACAP22 (WAC500 and NWA1123ACv3), 2468C-WAX650S (WAX650S), 2486C-11AXAP24 (NWA210AX, WAX610D and WAX630S), 2468C-11AXAP22 (NWA110AX and WAX510D), 2468C-11AXAP2246E (WAX640S-6E), 2468C-11AXAP246E (WAX620D-6E, NWA220AX-6E), 2468C-03785 (WAX655E), 2468C-03973 (WAX300H), 25830-04011 (NWA130BE and WBE530), and 25830-04157 (WBE630S,WBE510D, NWA210BE and NWA110BE) 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

MODÈLE D'ANTENNE	NB.	TYPE	CONNECTEUR	2.4 G GAIN (dBi)	5G/6G GAIN (dBi)	REMARQUE
WAX630S		PIFA	U.FL	0.92	1.32 (5150-5250 MHz) 1.39 (5250-5350 MHz) 0.44 (5470-5725 MHz) 1.63 (5725-5850 MHz)	
WAX650S		Direction	U.FL	0 (2400-2483.5 MHz)	3.51 (5150-5250 MHz) 4.22 (5250-5350 MHz) 4.61 (5470-5725 MHz) 4.68 (5725-5850 MHz)	
WAX510D NWA110AX	1	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	2	PIFA	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	3	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
	4	Dipole	I-PEX	0 (2400-2483.5 MHz)	4.5 (5150-5350MHz) 5.2 (5470-5725MHz) 5.5 (5725-5850MHz)	
NWA210AX WAX610D	1	Dipole	I-PEX		U-NII-1:7.8 dBi U-NII-2A:7.7 dBi U-NII-2C:6.8 dBi U-NII-3:7.2 dBi	
	2	PIFA	I-PEX	5.08 dBi		
	3	PIFA	I-PEX	5.56 dBi	U-NII-1:7.5 dBi U-NII-2A:6.8 dBi U-NII-2C:6.5 dBi U-NII-3:7.6 dBi	
	4	Dipole	I-PEX	6.06 dBi	U-NII-1:8.19 dBi U-NII-2A:7.7 dBi U-NII-2C:7.14 dBi U-NII-3:7.6 dBi	Wall Mount
	5	Dipole	I-PEX		U-NII-1:6.8 dBi U-NII-2A:7.5 dBi U-NII-2C:5.81 dBi U-NII-3:6.99 dBi	Ceiling Mount
	6	Dipole	I-PEX		U-NII-1:8.3 dBi U-NII-2A:7.8 dBi U-NII-2C:7.1 dBi U-NII-3:7.98 dBi	
WAC500H	1	PIFA	N/A	0 dBi	2.5 dBi	
	2	PIFA	N/A	0 dBi	2.5 dBi	
WAC500 NWA1123ACv3	1	PIFA	N/A	0 dBi	0 dBi	
	2	PIFA	N/A	0 dBi	0 dBi	
WAX640S-6E		PIFA	U.FL	1 dBi	U-NII-1:4.86 dBi U-NII-2A:5.93 dBi U-NII-2C:4.08 dBi U-NII-3:5.21 dBi U-NII-5:3.29 dBi U-NII-6:3.34 dBi U-NII-7:2.64 dBi U-NII-8:3.35 dBi	
WAX620D-6E NWA220AX-6E		PIFA	U.FL	1 dBi	U-NII-1:3.87 dBi U-NII-2A:3.96 dBi U-NII-2C:4.54 dBi U-NII-3:3.04 dBi U-NII-5:3.87 dBi U-NII-6:4.26 dBi U-NII-7:5.34 dBi U-NII-8:3.42 dBi	
WAX655E		Dipole	N type	4 dBi	6 dBi	

MODÈLE D'ANTENNE	NB.	TYPE	CONNECTEUR	2.4 G GAIN (dBi)	5G/6G GAIN (dBi)	REMARQUE
WAX300H	1	PIFA	N/A	1.4	4.2 (5150-5250 MHz) 4.6 (5250-5350 MHz) 5.1 (5470-5725 MHz) 5.1 (5725-5850 MHz)	
	2	PIFA	N/A	2.7	3.2 (5150-5250 MHz) 3.5 (5250-5350 MHz) 3.5 (5470-5725 MHz) 4.3 (5725-5850 MHz)	

- Pour une utilisation en intérieur uniquement (à l'exception WAX655E).

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

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

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

Industry Canada radiation exposure statement

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. This equipment should be installed and operated with a minimum distance of 21 cm (WAX300H) between the radiator and your body. This equipment should be installed and operated with a minimum distance of 28 cm (WBE660S) between the radiator and your body.

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. Cet équipement doit être installé et utilisé avec un minimum de 21 cm (WAX300H) de distance entre la source de rayonnement et votre corps. Cet équipement doit être installé et utilisé avec un minimum de 28 cm (WBE660S) de distance entre la source de rayonnement et votre corps.

Caution:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and

(iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

(iv) WAX655E is an outdoor device.

For model – WAX620D-6E/NWA220AX-6E/WAX640S-6E/WBE660S/NWA130BE/WBE530/WBE630S/ WBE510D/NWA210BE/NWA110BE

(v) Operation shall be limited to indoor use only;

(vi) Operation on oil platforms, cars, trains, boats and aircraft shall be prohibited except for on large aircraft flying above 10,000 ft.

(vii) Devices shall not be used for control of or communications with unmanned aircraft systems.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

(iv) WAX655E est un appareil extérieur.

For model – WAX620D-6E/NWA220AX-6E/WAX640S-6E/WBE660S/NWA130BE/WBE530/WBE630S/ WBE510D/NWA210BE/NWA110BE

(v) Utilisation limitée à l'intérieur seulement;

(vi) Utilisation interdite à bord de plateformes de forage pétrolier, de voitures, de trains, de bateaux et d'aéronefs, sauf à bord d'un gros aéronef volant à plus de 10 000 pieds d'altitude.

(vii) Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.

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 in the below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device operates in the 5150-5350 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:

WAC500H
- The band 2,400 MHz to 2,483.5 MHz is 87.7 mW,
- The band 5,150 MHz to 5,350 MHz is 174.58 mW,
- The band 5,470 MHz to 5,725 MHz is 443.61 mW.

WAC500
- The band 2,400 MHz to 2,483.5 MHz is 88.5 mW,
- The band 5,150 MHz to 5,350 MHz is 181.55 mW,
- The band 5,470 MHz to 5,725 MHz is 195.43 mW.

NWA1123ACv3
- The band 2,400 MHz to 2,483.5 MHz is 86.5 mW,
- The band 5,150 MHz to 5,350 MHz is 181.55 mW,
- The band 5,470 MHz to 5,725 MHz is 195.43 mW.

WAX630S
- The band 2400 MHz to 2483.5 MHz is 90.36 mW,
- The band 5150 MHz to 5350 MHz is 175.39 mW,
- The band 5470 MHz to 5725 MHz is 826.04 mW.

WAX650S
- The band 2,400 MHz to 2,483.5 MHz is 91.2 mW,
- The band 5,150 MHz to 5,350 MHz is 177.01 mW,
- The band 5,470 MHz to 5,725 MHz is 871 mW.

WAX510D and NWA110AX
- The band 2,400 MHz to 2,483.5 MHz is 85.31 mW,
- The band 5,150 MHz to 5,350 MHz is 172.19 mW,
- The band 5,470 MHz to 5,725 MHz is 651.63 mW.

WAX610D and NWA210AX
- The band 2,400 MHz to 2,483.5 MHz is 92.47 mW.
- The band 5,150 MHz to 5,350 MHz is 177.01 mW.
- The band 5,470 MHz to 5,725 MHz is 889.2 mW.

WAX640S-6E
- The band 2,400 MHz to 2,483.5 MHz is 81.85 mW,
- The band 5,150 MHz to 5,350 MHz is 169.82 mW,
- The band 5,470 MHz to 5,725 MHz is 839.46 mW.
- The band 5,925 MHz to 6,425 MHz is 169.82 mW.

WAX620D-6E and NWA220AX-6E
- The band 2,400 MHz to 2,483.5 MHz is 86.30 mW,
- The band 5,150 MHz to 5,350 MHz is 164.44 mW,
- The band 5,470 MHz to 5,725 MHz is 498.88 mW.
- The band 5,925 MHz to 6,425 MHz is 168.66 mW.

WAX655E
- The band 2,400 MHz to 2,483.5 MHz is 93.76 mW,
- The band 5,150 MHz to 5,350 MHz is 174.18 mW,
- The band 5,470 MHz to 5,725 MHz is 796.16 mW.

WAX300H
- The band 2,400 MHz to 2,483.5 MHz is 89.13 mW,
- The band 5,150 MHz to 5,350 MHz is 198.15 mW,
- The band 5,470 MHz to 5,725 MHz is 485.29 mW.

WBE660S

- The band 2,400 MHz to 2,483.5 MHz is 89.54 mW,
- The band 5,150 MHz to 5,350 MHz is 178.65 mW,
- The band 5,470 MHz to 5,725 MHz is 853.10 mW.
- The band 5,925 MHz to 6,425 MHz is 176.60 mW.

NWA130BE and WBE530

- The band 2,400 MHz to 2,483.5 MHz is 90.57 mW,
- The band 5,150 MHz to 5,350 MHz is 168.66 mW,
- The band 5,470 MHz to 5,725 MHz is 835.60 mW.
- The band 5,945 MHz to 6,425 MHz is 197.70 mW.

WBE630S / WBE510D/ NWA210BE / NWA110BE

- The band 2,400 MHz to 2,483.5 MHz is 88.10 mW,
- The band 5,150 MHz to 5,350 MHz is 181.55 mW,
- The band 5,470 MHz to 5,725 MHz is 521.19 mW.
- The band 5,945 MHz to 6,425 MHz is 188.80 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 cerințele esențiale 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/EC.

Notes:

1. Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	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 or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing the device covers can expose you to dangerous high voltage 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 it to the right supply voltage (for example, 120V AC in North America or 230V 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.
- 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.
- This device (WAC6553D-E, WAC6552D-S, WAX655E) 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 qualified service personnel if you are uncertain that suitable grounding is available.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For 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.

Environment statement

ErP (Energy-related Products) (NWA1123ACv3, WAC500, WAX510D, NWA110AX, WAX610D, NWA210AX, WAX630S, WAX620D-6E, NWA220AX-6E, WBE630S, WBE510D, NWA210BE and NWA110BE)

Zyxel products put on the EU and United Kingdom markets comply with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), the so called "ErP Directive (Energy-related Products directive), as well as ecodesign requirements laid down in applicable implementation measures. Power consumption has satisfied the regulation requirements which are:

Network standby power consumption < 8W(watts), and/or

Off mode power consumption < 0.5W(watts), and/or

Standby mode power consumption < 0.5W(watts).

For wireless setting, please refer to the chapter about wireless settings for more detail.

Disposal and Recycling Information

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

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

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

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

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

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

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 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。
- 使用無線產品時,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。
- 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 if the unidirectional flow or movement of electric charge carriers.
(earth/ground symbol)	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
(class II symbol)	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*.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product contains 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*.

Index

Numbers

802.11k   **14**, **16**, **17**, **18**, **19**, **21**, **22**, **23**
802.11r   **14**, **16**, **17**, **18**, **19**, **21**, **22**, **23**
802.11v   **14**, **16**, **17**, **18**, **19**, **21**, **22**, **23**

A

AC. See AP Controller
access   **55**
access privileges   **29**
access users   **156**
  see also users   **156**
admin users   **156**
  multiple logins   **161**
  see also users   **156**
alerts   **249**, **250**, **252**, **253**, **254**
antenna switch   **275**
AP Controller   **14**, **16**, **17**, **18**, **19**, **21**, **22**, **23**, **35**
applications
  MBSSID   **29**
  Repeater   **84**
Assisted Roaming, see 802.11k/v
Assisted Roaming. See 802.11k/v

B

backing up configuration files   **259**
Basic Service Set
  see BSS
Bluetooth
  BLE, see Bluetooth Low Energy
  BLE. See Bluetooth Low Energy
  advertisements   **153**
  advertising settings   **155**
  BLE   **153**
  Bluetooth Low Energy   **15**, **16**, **17**, **18**, **19**, **21**, **22**, **24**, **153**

  Bluetooth Smart   **153**
  iBeacon   **153**
  iBeacon ID   **153**
  major   **153**
  minor   **153**
  UUID   **153**
  UUID format   **155**
BSS   **29**

C

CA
  and certificates   **207**
CA (Certificate Authority), see certificates
CAPWAP   **124**
CEF (Common Event Format)   **247**, **251**
Certificate Authority (CA)
  see certificates
Certificate Revocation List (CRL)   **207**
  vs OCSP   **221**
certificates   **206**
  advantages of   **207**
  and CA   **207**
  and FTP   **239**
  and HTTPS   **228**
  and SSH   **237**
  and WWW   **229**
  certification path   **207**, **214**, **219**
  expired   **207**
  factory-default   **207**
  file formats   **207**
  fingerprints   **215**, **220**
  importing   **210**
  not used for encryption   **207**
  revoked   **207**
  self-signed   **207**, **211**
  serial number   **214**, **219**
  storage space   **209**, **217**
  thumbprint algorithms   **208**
  thumbprints   **208**
  used for authentication   **207**

V

W

Z