Table 111 Maintenance > Remote Management > MGMT Services (continued)

LABEL	DESCRIPTION
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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

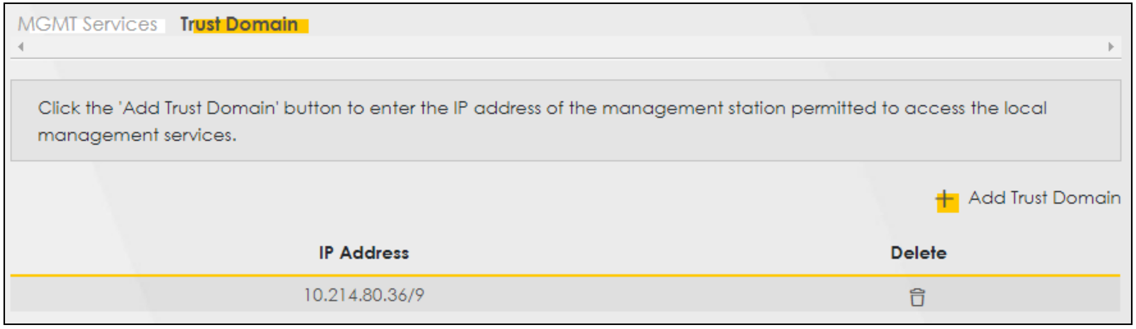
29.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance > Remote Management > MGMT Services** screen.

Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 158 Maintenance > Remote Management > Trust Domain



Click the 'Add Trust Domain' button to enter the IP address of the management station permitted to access the local management services.

IP Address	Delete
10.214.80.36/9	🗑

The following table describes the fields in this screen.

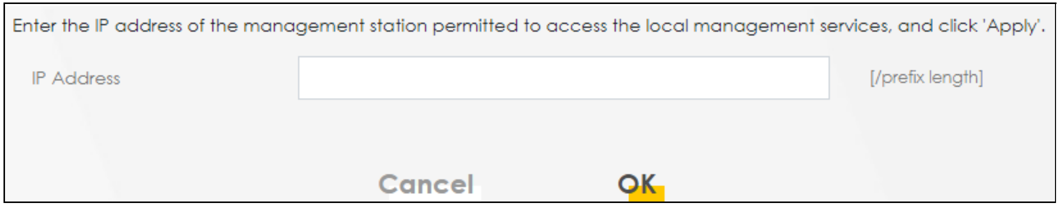
Table 112 Maintenance > Remote Management > Trust Domain

LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trust IP address.

29.3.1 Add Trust Domain

Use this screen to configure a public IP address which is allowed to access the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain** screen to open the following screen.

Figure 159 Maintenance > Remote Management > Trust Domain > Add Trust Domain



Enter the IP address of the management station permitted to access the local management services, and click 'Apply'.

The following table describes the fields in this screen.

Table 113 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IP address which is allowed to access the service on the Zyxel Device from the WAN. You can enter an IPv4 or IPv6 address and subnet mask or prefix length.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes back to the Zyxel Device.

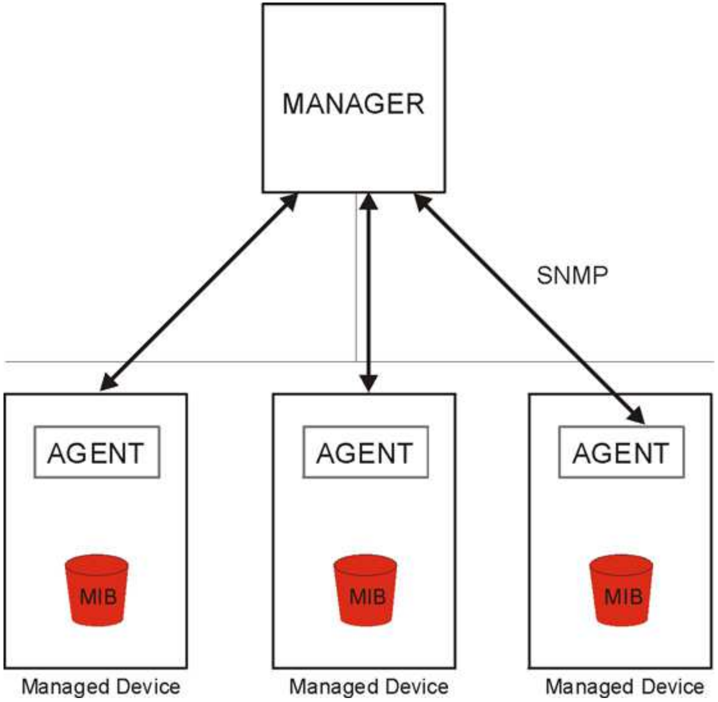
CHAPTER 30 SNMP

30.1 SNMP Overview

This screen allows you to configure the SNMP settings on the Zyxel Device.

The 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 next figure illustrates an SNMP management operation.

Figure 160 SNMP Management Model



An SNMP managed network consists of two main types of components: 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 the number of packets received, node port status, and so on. 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.

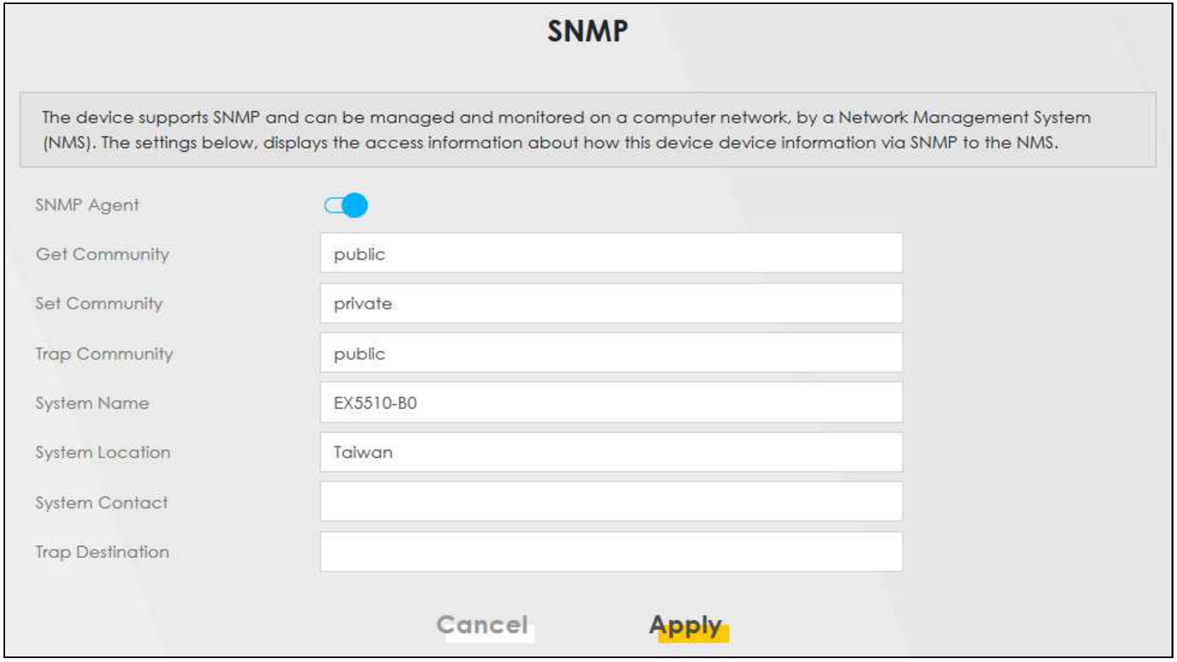
Trap - Used by the agent to inform the manager of some events.

30.2 SNMP Settings

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the Zyxel Device SNMP settings.

Configure how the Zyxel Device reports to the Network Management System (NMS) via SNMP using the screen below.

Figure 161 Maintenance > SNMP



SNMP

The device supports SNMP and can be managed and monitored on a computer network, by a Network Management System (NMS). The settings below, displays the access information about how this device device information via SNMP to the NMS.

SNMP Agent	●
Get Community	public
Set Community	private
Trap Community	public
System Name	EX5510-B0
System Location	Taiwan
System Contact	
Trap Destination	

The following table describes the fields in this screen.

Table 114 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Enable this switch to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network, Click on this switch to enable/disable it. When the switch goes to the right ●, the function is enabled.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set Community**, which is the password for the incoming Set requests from the management station.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 31 Time Settings

31.1 Time Settings Overview

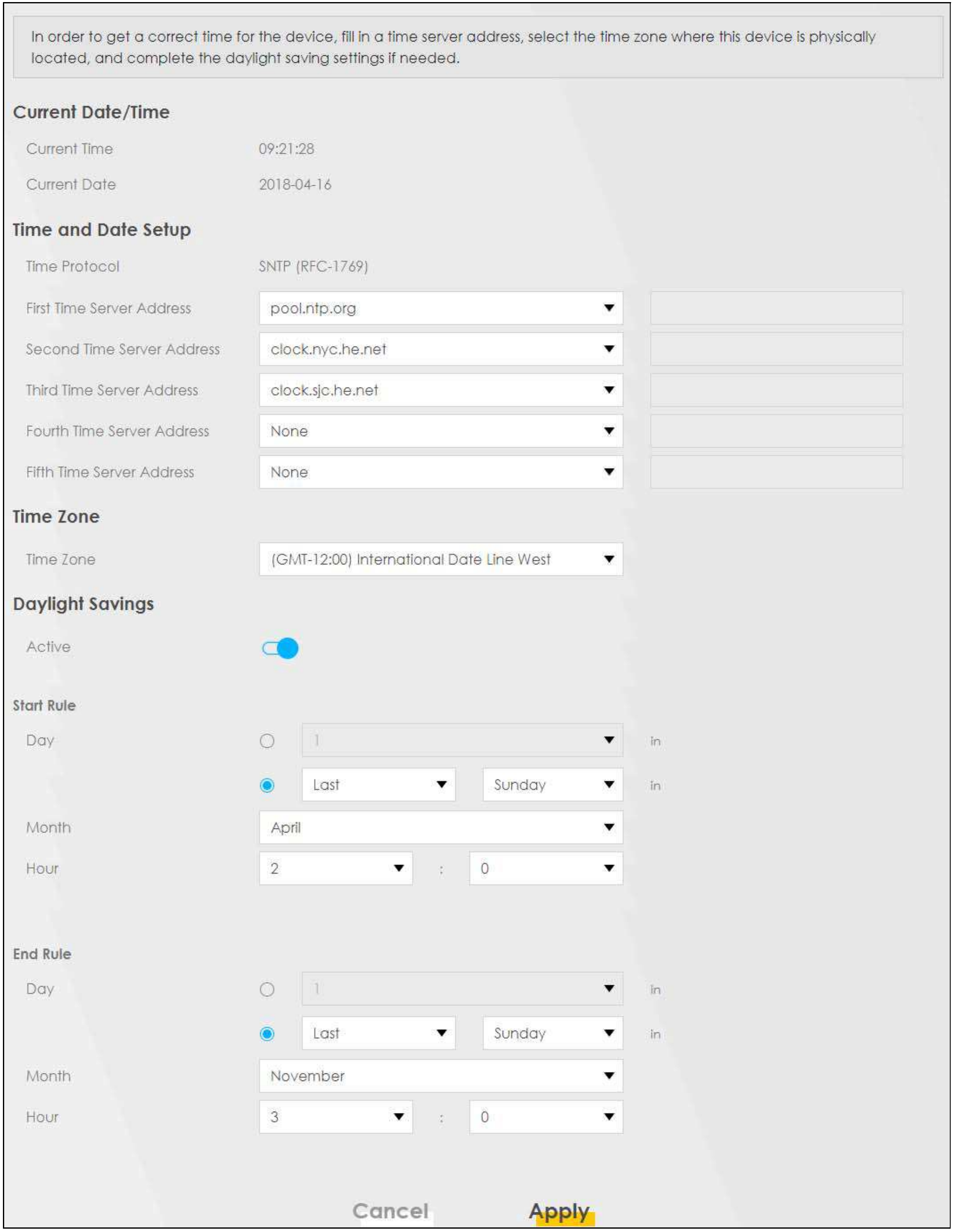
This chapter shows you how to configure the Zyxel Device's system date and time.

31.2 Time

For effective scheduling and logging, the Zyxel Device's system time must be accurate. Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings when needed.

Click **Maintenance** > **Time** to open the following screen.

Figure 162 Maintenance > Time



In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time	09:21:28
Current Date	2018-04-16

Time and Date Setup

Time Protocol	SNTP (RFC-1769)
First Time Server Address	pool.ntp.org
Second Time Server Address	clock.nyc.he.net
Third Time Server Address	clock.sjc.he.net
Fourth Time Server Address	None
Fifth Time Server Address	None

Time Zone

Time Zone	(GMT-12:00) International Date Line West

Daylight Savings

Active

Start Rule

Day	○	1		in
	●	Last	Sunday	in
Month		April		
Hour		2	: 0	

End Rule

Day	○	1		in
	●	Last	Sunday	in
Month		November		
Hour		3	: 0	

The following table describes the fields in this screen.

Table 115   Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the time with the time server.
Current Date	This field displays the date of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right ●, the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

CHAPTER 32
E-mail Notification

32.1 E-mail Notification Overview

A mail server is an application or a computer that can receive, forward and deliver e-mail messages.

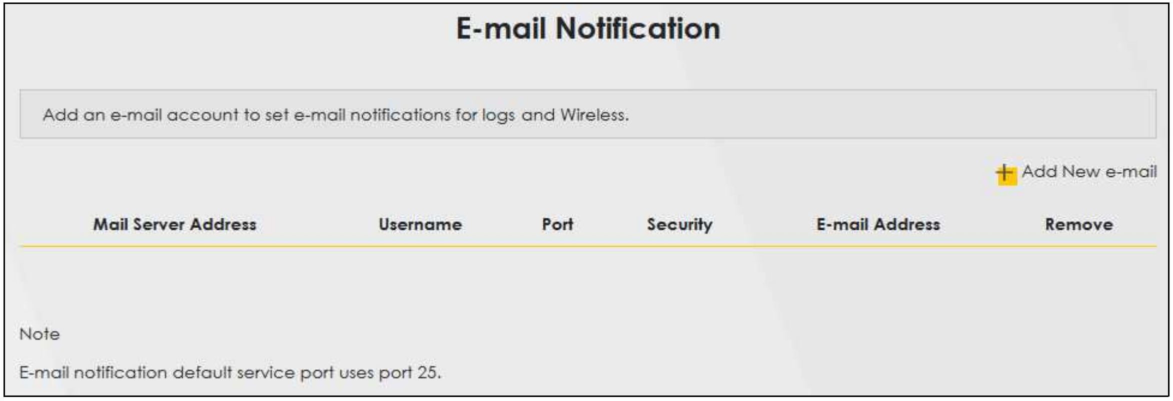
To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

32.2 E-mail Notification Settings

Click **Maintenance > E-mail Notification** to open the **E-mail Notification** screen. Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

Note: The default port number of the mail server is 25.

Figure 163 Maintenance > E-mail Notification



E-mail Notification

Add an e-mail account to set e-mail notifications for logs and Wireless.

Note

E-mail notification default service port uses port 25.

The following table describes the labels in this screen.

Table 116 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.

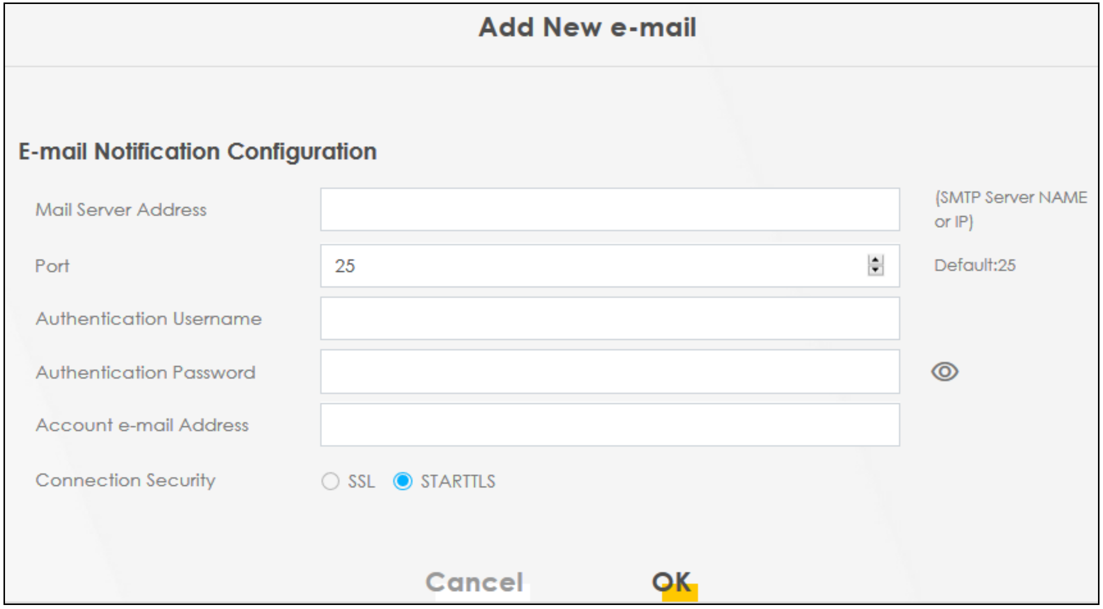
Table 116 Maintenance > E-mail Notification (continued)

LABEL	DESCRIPTION
E-mail Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Zyxel Device sends.
Remove	Click this to delete the entry.

32.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 164 E-mail Notification > Add



Add New e-mail

E-mail Notification Configuration

Mail Server Address		(SMTP Server NAME or IP)
Port	25	Default:25
Authentication Username		
Authentication Password		
Account e-mail Address		
Connection Security	○ SSL ● STARTTLS	

The following table describes the labels in this screen.

Table 117 E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account e-mail Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** 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.

Table 117 E-mail Notification > Add (continued)

LABEL	DESCRIPTION
Cancel	Click this button to exit this screen without saving any changes.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 33
Log Setting

33.1 Logs Setting Overview

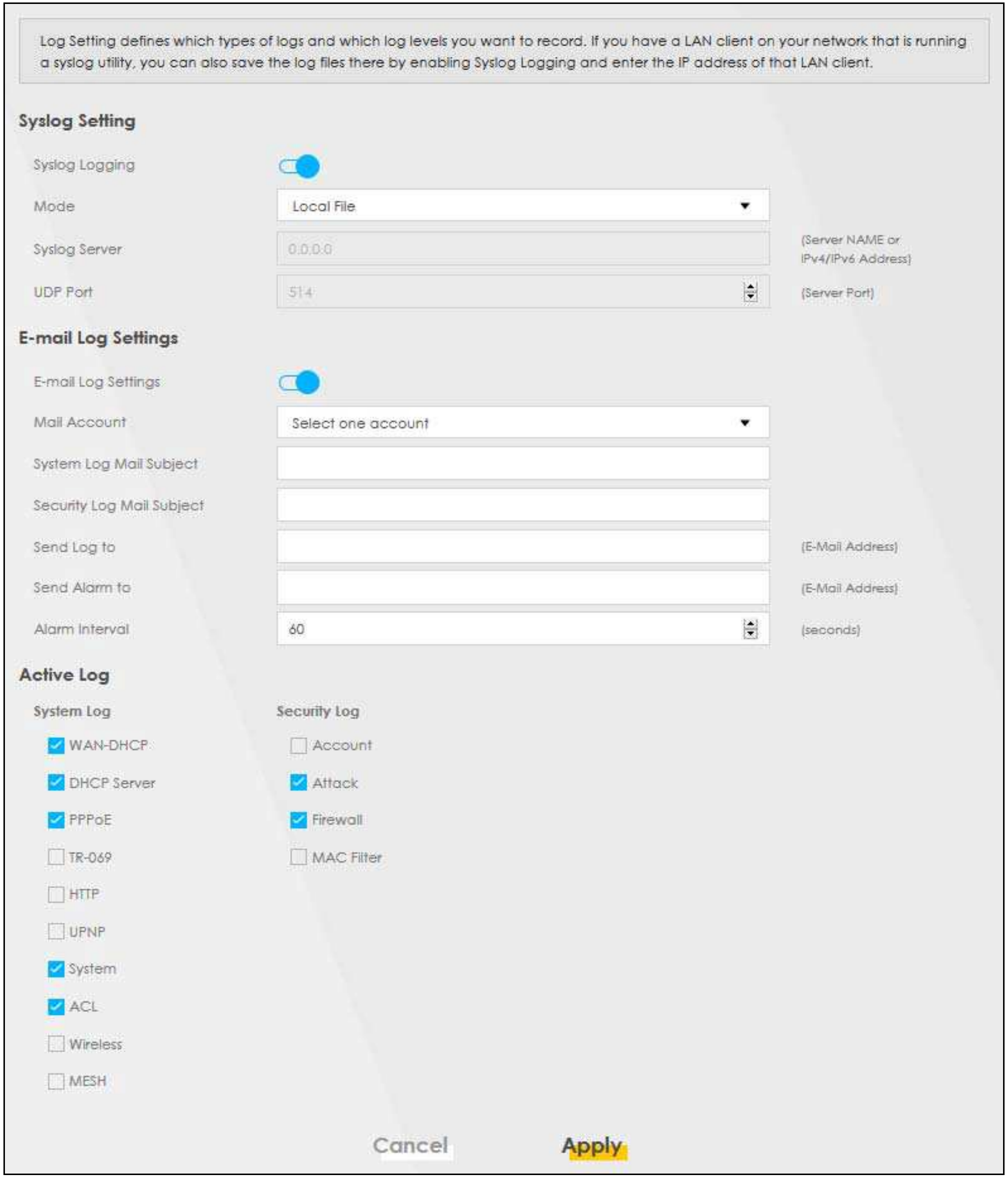
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

33.2 Log Settings

To change your Zyxel Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

If you have a LAN client on your network or a remote server that is running a syslog utility, you can also save its log files by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the LAN client in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server.

Figure 165 Maintenance > Log Setting



Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging: ●

Mode: Local File ▾

Syslog Server: 0.0.0.0 (Server NAME or IPv4/IPv6 Address)

UDP Port: 514 (Server Port)

E-mail Log Settings

E-mail Log Settings: ●

Mail Account: Select one account ▾

System Log Mail Subject:

Security Log Mail Subject:

Send Log to: (E-Mail Address)

Send Alarm to: (E-Mail Address)

Alarm Interval: 60 (seconds)

Active Log

System Log	Security Log
☑ WAN-DHCP	☐ Account
☑ DHCP Server	☑ Attack
☑ PPPoE	☑ Firewall
☐ TR-069	☐ MAC Filter
☐ HTTP	
☐ UPNP	
☑ System	
☑ ACL	
☐ Wireless	
☐ MESH	

The following table describes the fields in this screen.

Table 118 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Zyxel Device sends a log to an external syslog server. Click this switch to enable or disable to enable syslog logging. When the switch goes to the right ●, the function is enabled. Otherwise, it is not.
Mode	Select the syslog destination from the drop-down list box. If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 118 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Settings	Click this switch to have the Zyxel Device send logs and alarm messages to the configured e-mail addresses. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Mail Account	Select a mail account from which you want to send logs. You can configure mail accounts in the **Maintenance > E-mail Notification** screen.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the Zyxel Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the Zyxel Device sends.
Send Log to	The Zyxel Device sends logs to the e-mail address specified in this field. If this field is left blank, the Zyxel Device does not send logs via e-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
Alarm Interval	Specify how often the alarm should be updated.
Active Log	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

33.2.1 Example E-mail Log

An ‘End of Log’ message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- ‘`End of Log`’ message shows that a complete log has been sent.

Figure 166 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……………………………..{snip}…………………………………..
……………………………..{snip}…………………………………..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 34
Firmware Upgrade

34.1 Firmware Upgrade Overview

This screen lets you upload new firmware to your Zyxel Device. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to upgrade your device’s performance.

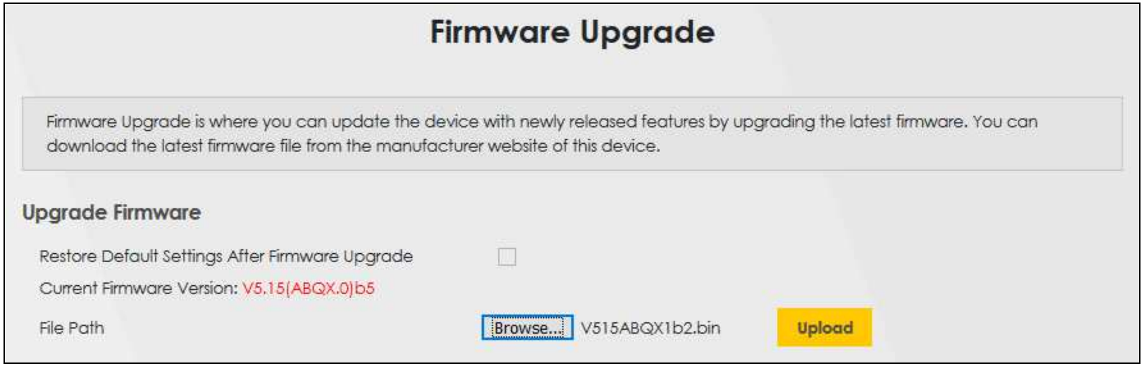
Only use firmware for your device’s specific model. Refer to the label on the bottom of your Zyxel Device.

34.2 Firmware Upgrade Settings

Click **Maintenance > Firmware Upgrade** to open the following screen. Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the Zyxel Device will reboot.

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

Figure 167 Maintenance > Firmware Upgrade



Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade □

Current Firmware Version: V5.15(ABQX.0)b5

File Path Browse... V515ABQX1b2.bin Upload

The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the Zyxel Device again.

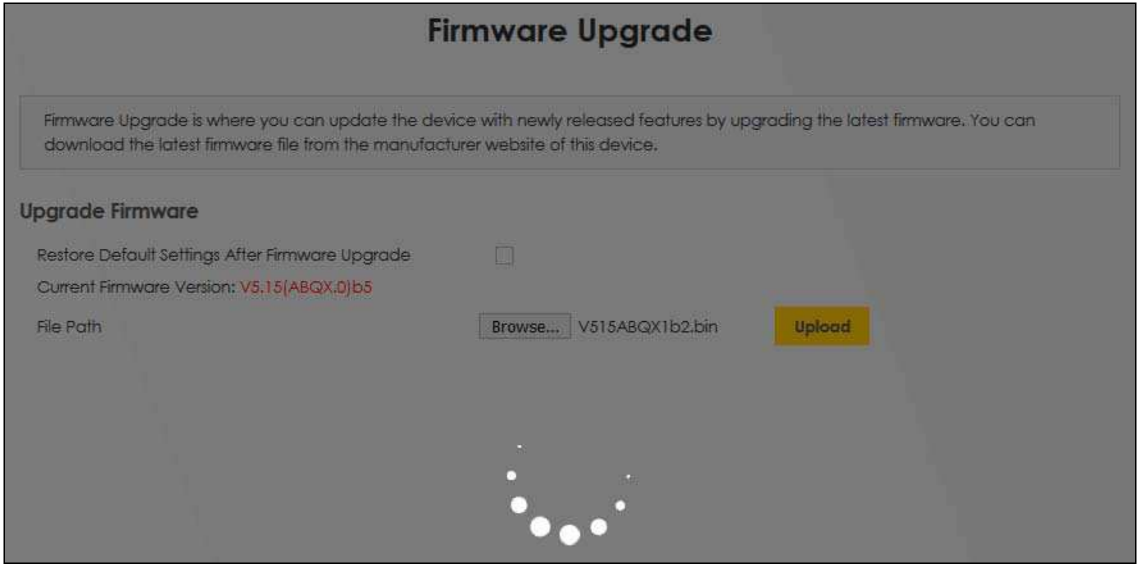
Table 119 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select the check box to have the Zyxel Device automatically reset itself after the new firmware is uploaded.

Table 119 Maintenance > Firmware Upgrade

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

Figure 168 Firmware Uploading


Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade □

Current Firmware Version: V5.15(ABQX.0)b5

File Path Browse... V515ABQX1b2.bin Upload

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

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 169 Error Message

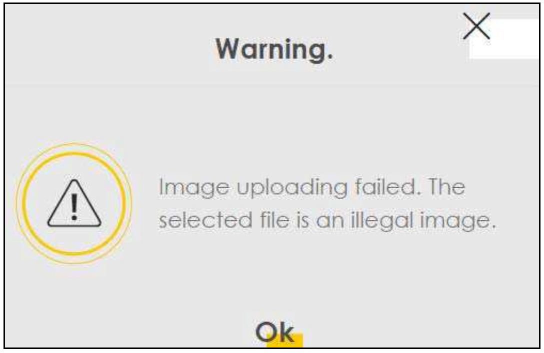
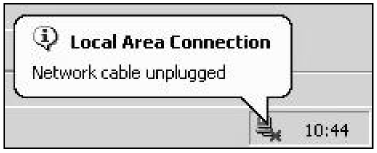

Warning.

Image uploading failed. The selected file is an illegal image.

Ok

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

Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

CHAPTER 35
Backup/Restore

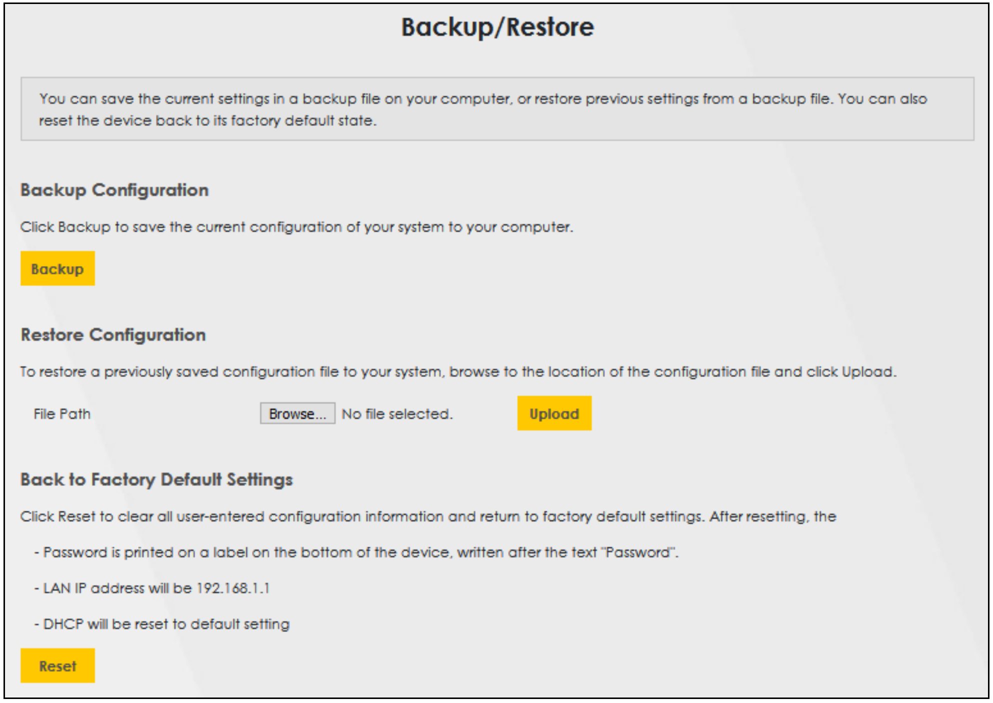
35.1 Backup/Restore Overview

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

35.2 Backup/Restore Settings

Click **Maintenance > Backup/Restore**. Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

Figure 170 Maintenance > Backup/Restore



Backup/Restore

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path Browse... No file selected.

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

Backup Configuration

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

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

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device.

Table 120 Restore Configuration

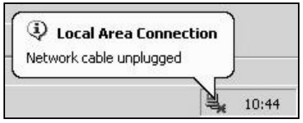
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

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

After the Zyxel Device configuration has been restored successfully, the login screen appears. Login again to restart the Zyxel Device.

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

Figure 171 Network Temporarily Disconnected

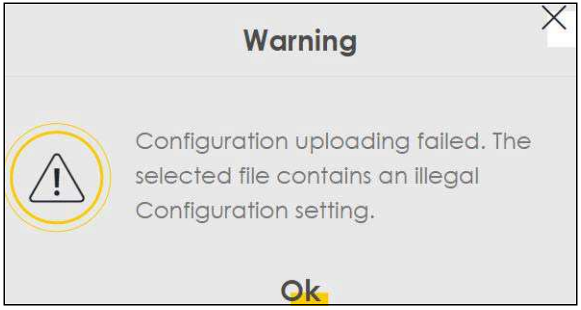


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Backup/ Restore** screen.

Figure 172 Configuration Upload Error



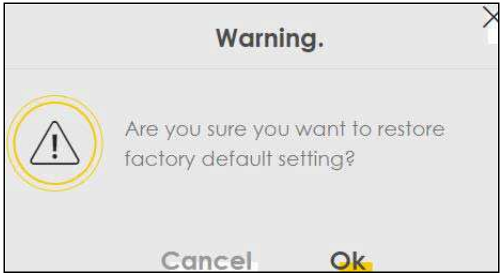
Warning

Configuration uploading failed. The selected file contains an illegal Configuration setting.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults. The following warning screen appears.

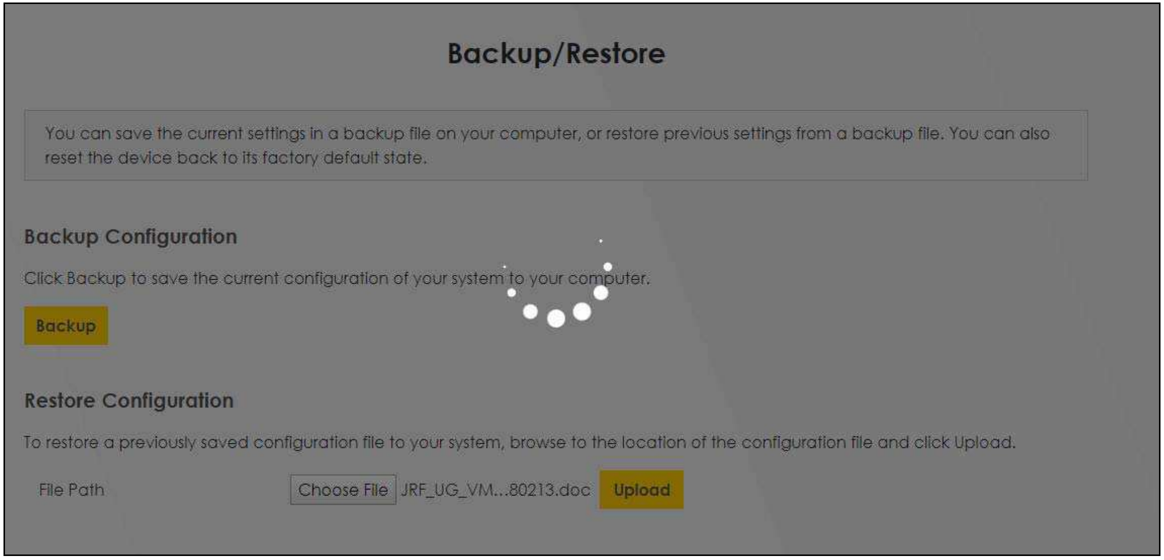
Figure 173 Reset Warning Message



Warning.

Are you sure you want to restore factory default setting?

Figure 174 Reset In Process Message



Backup/Restore

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path Choose File JRF_UG_VM...80213.doc

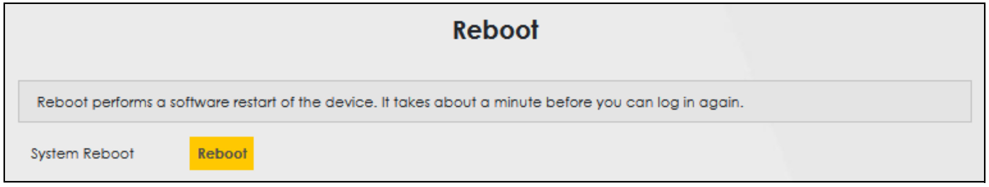
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Zyxel Device. Refer to Section 1.5.4 on page 21 for more information on the **RESET** button.

35.3 Reboot

System Reboot allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the Zyxel Device reboot. This does not affect the Zyxel Device's configuration.

Figure 175 Maintenance > Reboot



Reboot

Reboot performs a software restart of the device. It takes about a minute before you can log in again.

System Reboot

CHAPTER 36 Diagnostic

36.1 Diagnostic Overview

The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

The route between a Central Office Very-high-bit-rate Digital Subscriber Line (CO VDSL) switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

36.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host (Section 36.3 on page 271).
- The **802.1ag** screen lets you perform CFM actions (Section 36.4 on page 271).
- The **802.3ah** screen lets you configure link OAM port parameters(Section 36.5 on page 273).

36.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

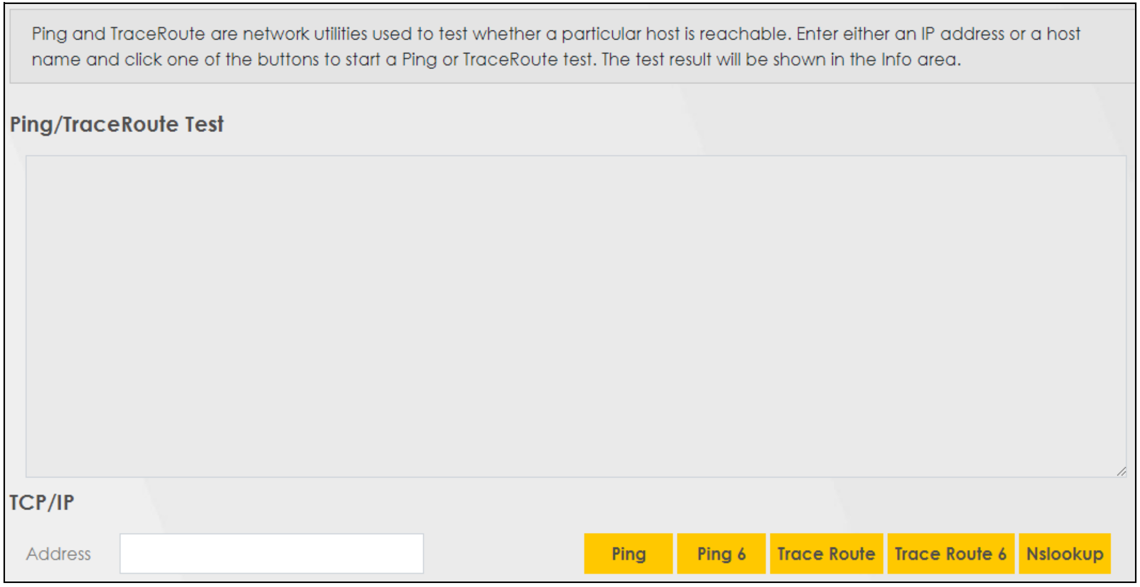
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

36.3 Ping & TraceRoute & NsLookup

Use this screen use ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

Figure 176 Maintenance > Diagnostic > Ping&TraceRoute&NsLookup



Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

The following table describes the fields in this screen.

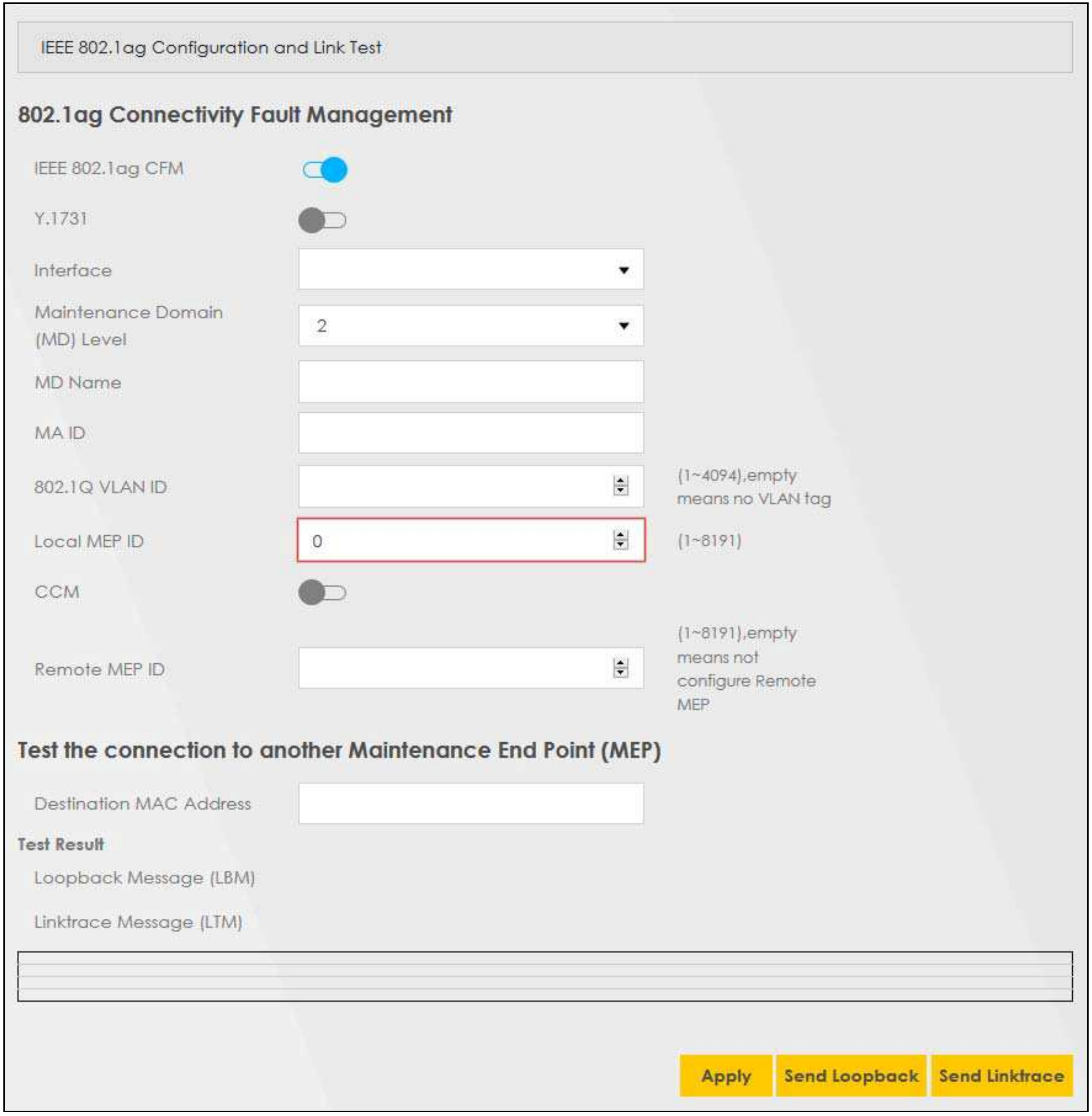
Table 121 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IPv4 address that you entered.
Ping 6	Click this to ping the IPv6 address that you entered.
Trace Route	Click this to display the route path and transmission delays between the Zyxel Device to the IPv4 address that you entered.
Trace Route 6	Click this to display the route path and transmission delays between the Zyxel Device to the IPv6 address that you entered.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

36.4 802.1ag (CFM)

Click **Maintenance > Diagnostic** > **802.1ag** to open the following screen. Use this screen to configure and perform Connectivity Fault Management (CFM) actions as defined by the IEEE 802.1ag standard. CFM protocols include Continuity Check Protocol (CCP), Link Trace (LT), and Loopback (LB).

Figure 177 Maintenance > Diagnostic > 802.1ag



IEEE 802.1ag Configuration and Link Test

802.1ag Connectivity Fault Management

IEEE 802.1ag CFM	● on	
Y.1731	○ off	
Interface		
Maintenance Domain (MD) Level	2	
MD Name		
MA ID		
802.1Q VLAN ID		(1~4094),empty means no VLAN tag
Local MEP ID	0	(1~8191)
CCM	○ off	
Remote MEP ID		(1~8191),empty means not configure Remote MEP

Test the connection to another Maintenance End Point (MEP)

Destination MAC Address	

Test Result

Loopback Message (LBM)

Linktrace Message (LTM)

The following table describes the fields in this screen.

Table 122 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
IEEE 802.1ag CFM	Click this switch to enable or disable the IEEE802.1ag CFM specification, which allows network administrators to identify and manage connection faults. When the switch goes to the right ●, the function is enabled. Otherwise, it is not.
Y.1731	Click this switch to enable or disable Y.1731, which monitors Ethernet performance. When the switch goes to the right ●, the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEE 802.1ag CFM.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.

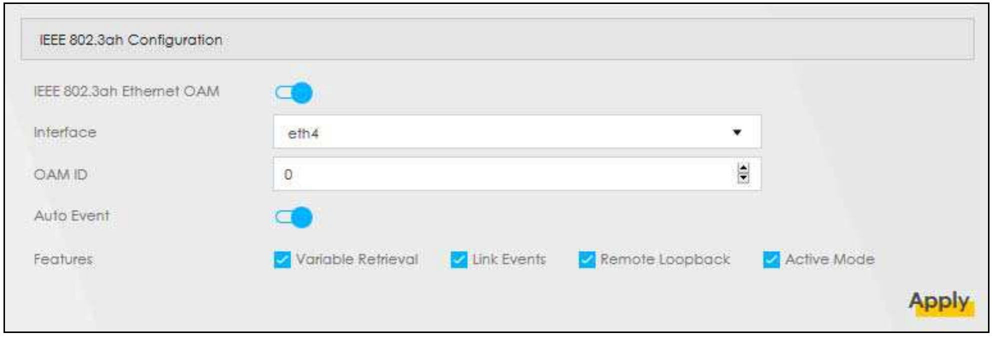
Table 122   Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
MD Name	Enter a descriptive name for the MD (Maintenance Domain). This field only appears if the **Y.1731** field is disabled.
MA ID	Enter a descriptive name to identify the Maintenance Association. This field only appears if the **Y.1731** field is disabled.
MEG ID	Enter a descriptive name to identify the Maintenance Entity Group. This field only appears if the **Y.1731** field is enabled.
802.1Q VLAN ID	Type a VLAN ID (1-4094) for this MA.
Local MEP ID	Enter the local Maintenance Endpoint Identifier (1~8191).
CCM	Select **Enable** to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the Zyxel Device will always process it, whether **CCM** is enabled or not.
Remote MEP ID	Enter the remote Maintenance Endpoint Identifier (1~8191).
Test the connection to another Maintenance End Point (MEP)	
Destination MAC Address	Enter the target device's MAC address to which the Zyxel Device performs a CFM loopback and linktrace test.
Test Result	
Loopback Message (LBM)	This shows **Pass** if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows **Fail**.
Linktrace Message (LTM)	This shows the MAC address of MEPs that respond to the LTMs.
Apply	Click this button to save your changes.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

36.5 802.3ah (OAM)

Click **Maintenance > Diagnostic** > **803.ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units (OAM PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 178   Maintenance > Diagnostic > 802.3ah



IEEE 802.3ah Configuration

IEEE 802.3ah Ethernet OAM: ●

Interface: eth4

OAM ID: 0

Auto Event: ●

Features: ☑ Variable Retrieval ☑ Link Events ☑ Remote Loopback ☑ Active Mode

The following table describes the labels in this screen.

Table 123 Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE802.3ah.
OAM ID	Enter a positive integer to identify this node.
Auto Event	Click this switch to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, disable this and you will not be notified. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Features	Select **Variable Retrieval** so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events. Select **Link Events** so the Zyxel Device can interpret link events, such as link fault and dying asp.Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of error frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well. Select **Remote Loopback** so the Zyxel Device can accept loopback control PDUs to convert Zyxel Device into loopback mode. Select **Active Mode** so the Zyxel Device initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.
Apply	Click this button to save your changes.

PART III

Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 37 Troubleshooting

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

- Power, Hardware Connections, and LEDs
- Zyxel Device Access and Login
- Internet Access
- Wireless Internet Access
- UPnP
- IP Address Setup

37.1 Power, Hardware Connections, and LEDs

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

1 Make sure the Zyxel Device is turned on.

2 Make sure you are using the power adapter included with the Zyxel Device.

3 Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Table 2 on page 20.

2 Check the hardware connections.

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

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

37.2 Zyxel Device Access and Login

I forgot the IP address for the Zyxel Device.

1 The default LAN IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Zyxel Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.5.4 on page 21.

I forgot the password.

1 See the cover page for the default login names and associated passwords.

2 If those do not work, you have to reset the device to its factory defaults. See Section 1.5.4 on page 21.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 8.2 on page 121), 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.
- Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See Section 37.6 on page 281.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Table 2 on page 20.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote Management**).

5 Reset the device to its factory defaults, and try to access the Zyxel Device with the default IP address. See Section 1.5.4 on page 21.

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

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

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

1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.

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

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 37.1 on page 276.

I cannot Telnet to the Zyxel Device.

See the troubleshooting suggestions for I cannot see or access the **Login screen in the Web Configurator.** Ignore the suggestions about your browser.

I cannot use FTP to upload/download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the **Login screen in the Web Configurator.** Ignore the suggestions about your browser.

37.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Table 2 on page 20.

2 Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure that you enabled WiFi in the Zyxel Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Zyxel Device.

4 Disconnect all the cables from your device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a MODEM or Router.

2 Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot access the Zyxel Device anymore. I had access to the Zyxel Device, but my connection is not available anymore.

1 Your session with the Zyxel Device may have expired. Try logging into the Zyxel Device again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Table 2 on page 20.

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact your vendor.

37.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

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 wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

37.5 UPnP

When using UPnP and the Zyxel Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the Zyxel Device’s LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

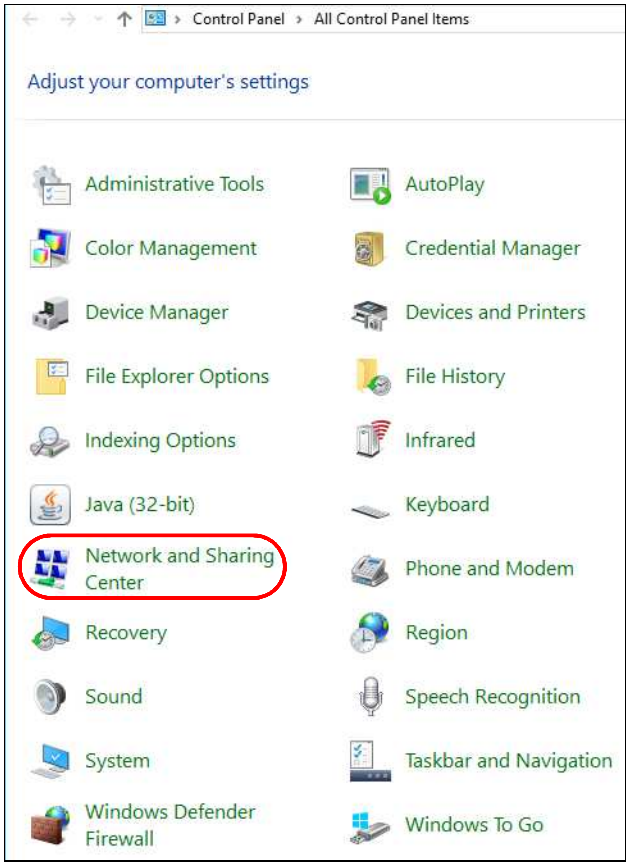
Restart your computer.

37.6 IP Address Setup

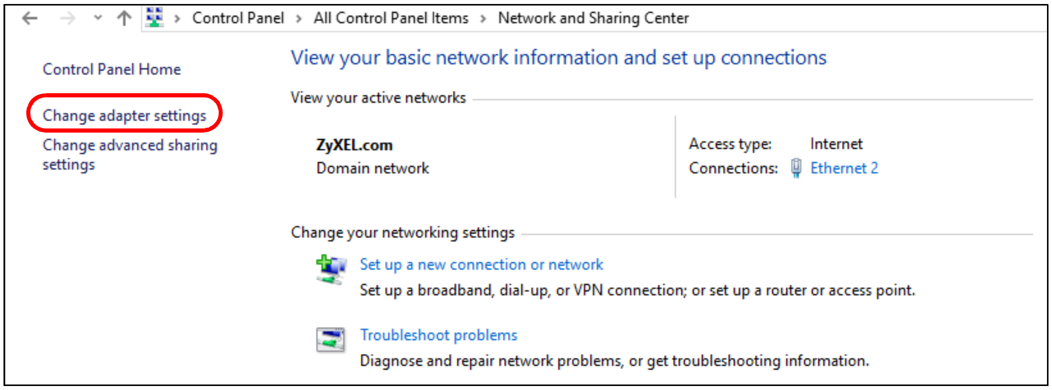
I need to set the computer's IP address to be in the same subnet as the Zyxel Device.

1 In Windows 10, open the **Control Panel**.

2 Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.



3 Click **Change adapter settings**.



Control Panel > All Control Panel Items > Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

ZyXEL.com
Domain network

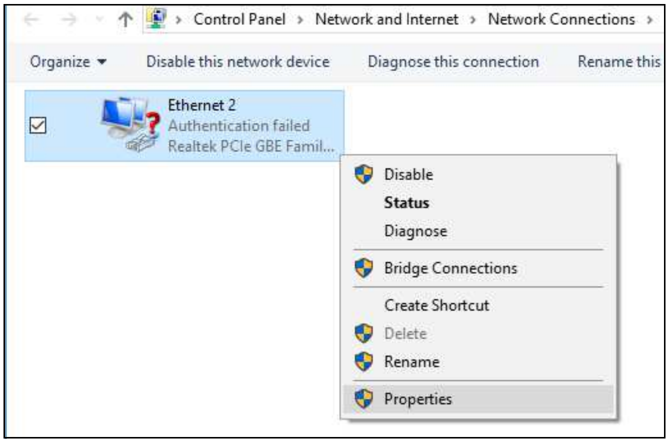
Access type: Internet
Connections: Ethernet 2

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

4 Right-click the **Ethernet** icon, and then select **Properties**

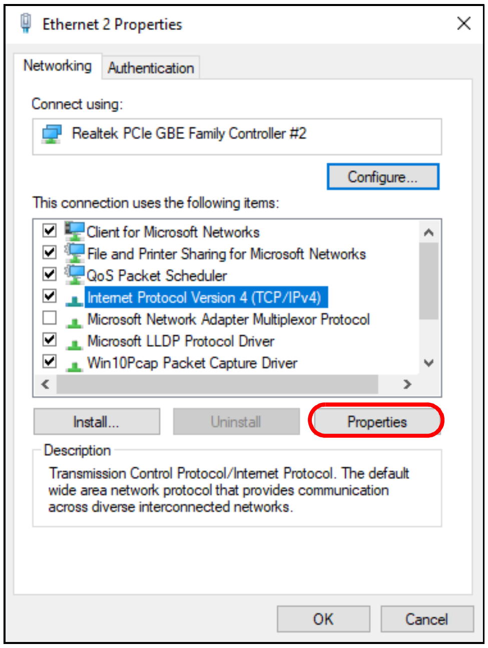


Control Panel > Network and Internet > Network Connections >

Organize ▾ Disable this network device Diagnose this connection Rename this

☑ Ethernet 2
Authentication failed
Realtek PCIe GBE Famil...

5 Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.



Ethernet 2 Properties

Networking Authentication

Connect using:

Realtek PCIe GBE Family Controller #2

Configure...

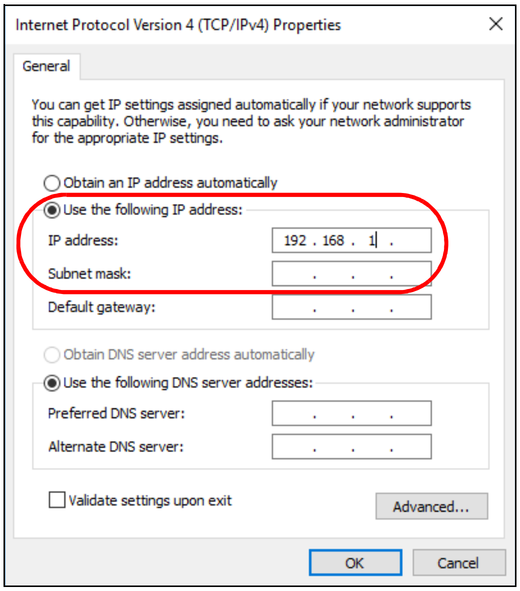
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Win10Pcap Packet Capture Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6 Select **Use the following IP address** and enter an **IP address** from **192.168.1.2** to **192.168.1.254**. The **Subnet mask** will be entered automatically.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

7 Click **OK** when you are done and close all windows.

APPENDIX A
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.

See *https://www.zyxel.com/homepage.shtml* and also *https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

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

Vietnam

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

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/