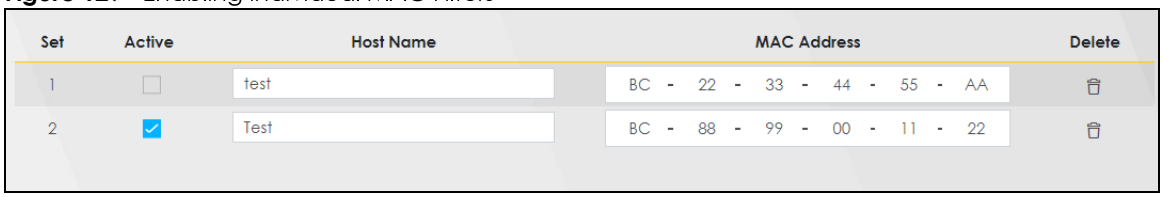
Figure 129 Enabling individual MAC Filters



The following table describes the labels in this screen.

Table 84 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate the MAC filter function.
MAC Restrict Mode	Select **Allow** to only permit the listed MAC addresses access to the Zyxel Device. Select **Deny** to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Click this button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 18
Parental Control

18.1 Parental Control Overview

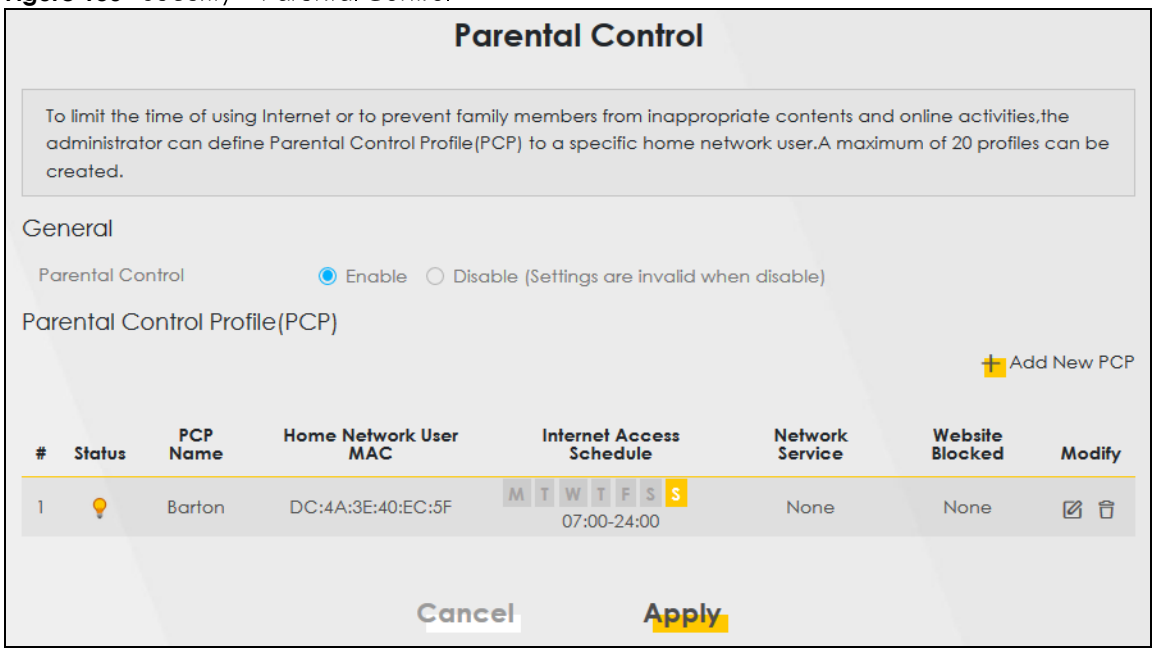
Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

18.2 Parental Control Settings

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

Click **Security** > **Parental Control** to open the following screen.

Figure 130 Security > Parental Control



The following table describes the fields in this screen.

Table 85 Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select **Enable** to activate parental control.

Table 85 Security > Parental Control (continued)

LABEL	DESCRIPTION
Parental Control Profile (PCP)	
Add new PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Block	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

18.2.1 Add/Edit a Parental Control Profile

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 131 Security > Parental Control > Add/Edit PCP (General, Rule List & Internet Access Schedule)

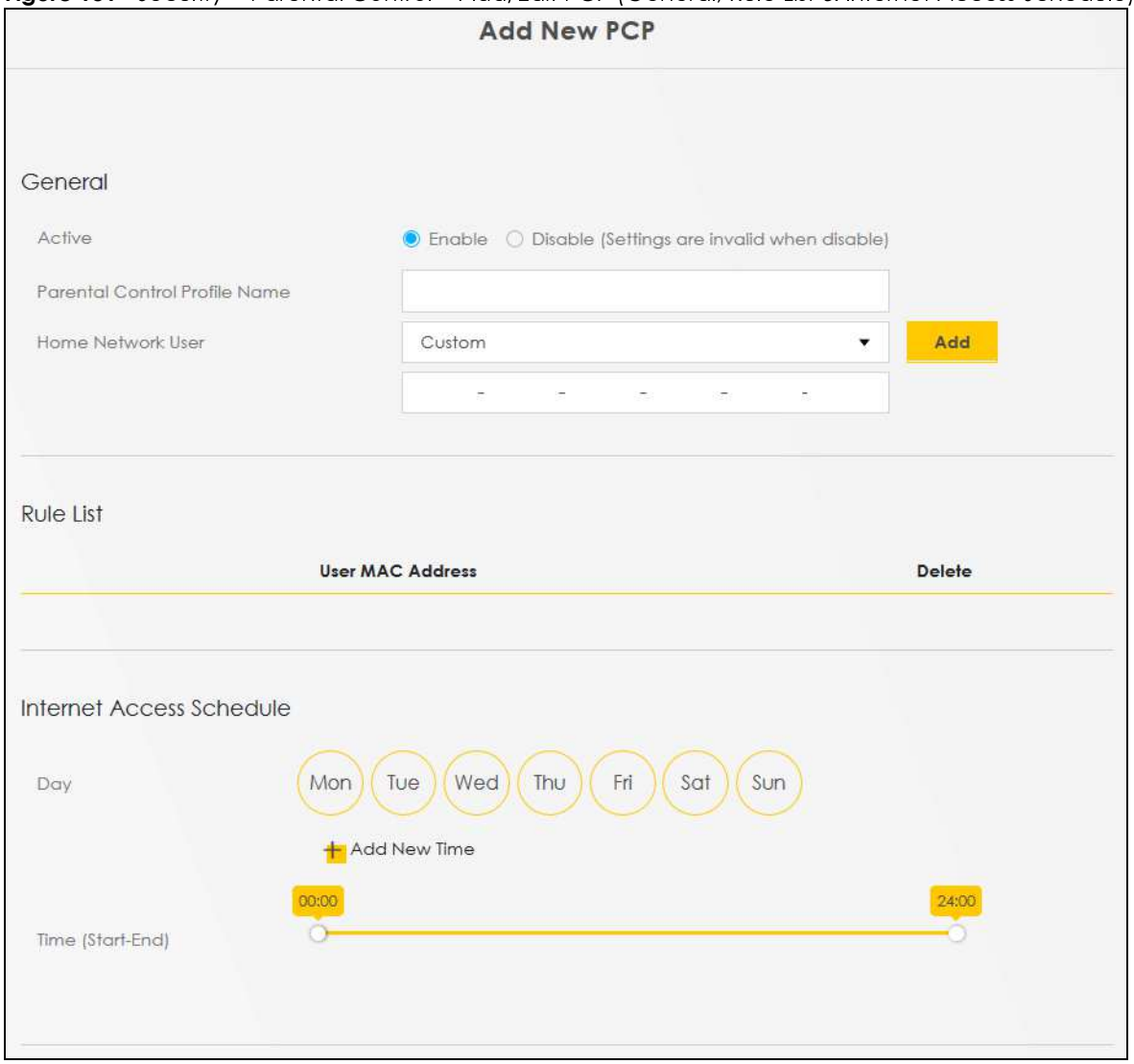
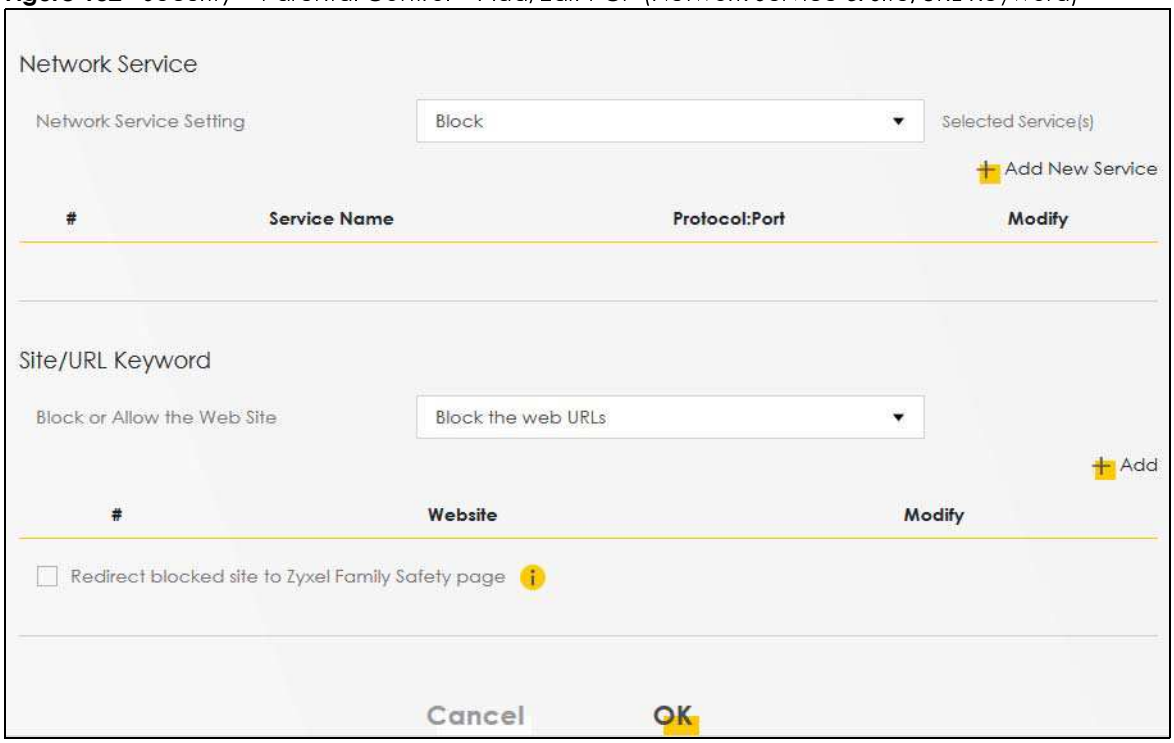


Figure 132 Security > Parental Control > Add/Edit PCP (Network Service & Site/URL Keyword)



The following table describes the fields in this screen.

Table 86 Security > Parental Control >Add/Edit PCP

LABEL	DESCRIPTION
General	
Active	Select **Enable** or **Disable** to activate or deactivate the parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Rule List	In **Home Network User**, select **Custom**, enter the LAN user's MAC address, then click the **Add** icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the **Delete** icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Zyxel Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access (**Authorized access**) or denied access (**No access**).
Add New Service	Click this to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select **Block**, the Zyxel Device prohibits the users from viewing the web sites with the URLs listed below. If you select **Allow**, the Zyxel Device blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Port** of the new rule, as shown in Figure 134.
#	This shows the index number of the rule.

Table 86 Security > Parental Control >Add/Edit PCP (continued)

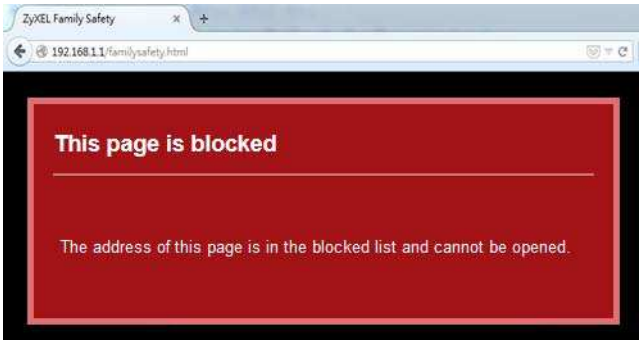
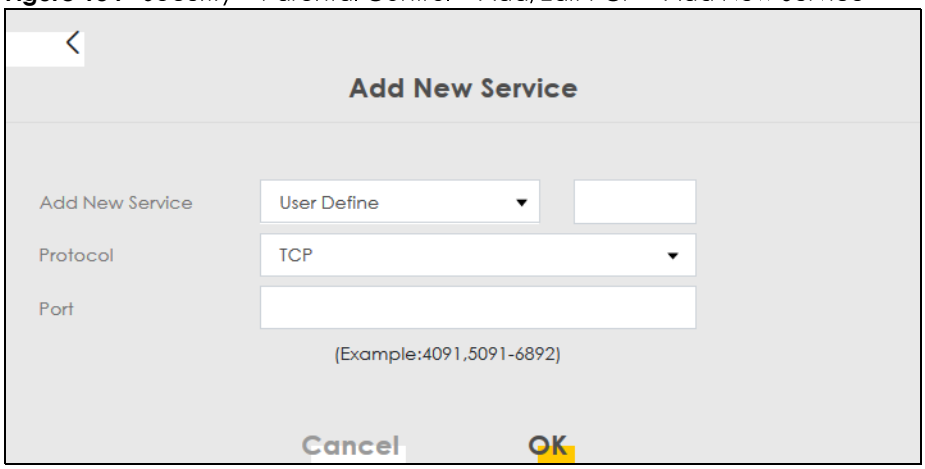
LABEL	DESCRIPTION
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select **Block the Web URLs**, the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow the Web URLs**, the Zyxel Device blocks access to all URLs except ones listed below.
Add	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
#	This shows the index number of the rule.
Website	This shows the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Redirect blocked site to Zyxel Family Safety page	Select this to redirect users who access any blocked websites listed above to the Zyxel Family Safety page as shown next. **Figure 133** Zyxel Family Safety Page Example 
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Figure 134 Security > Parental Control > Add/Edit PCP > Add New Service



The following table describes the fields in this screen.

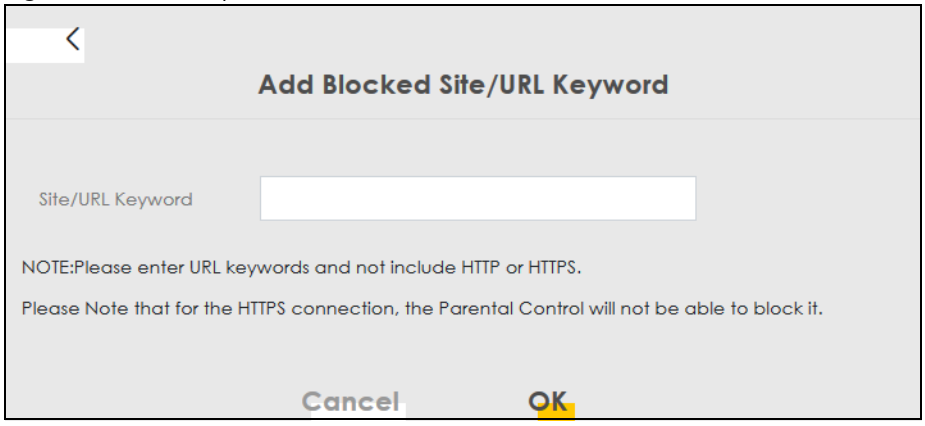
Table 87 Security > Parental Control > Add/Edit PCP > Add New Service

LABEL	DESCRIPTION
Add New Service	Select the name of the service from the drop-down list. Otherwise, select **User Define** and specify the name, protocol, and port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are **TCP**, **UDP**, or **TCP & UDP**.
Port	Enter the port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Click **Security** > **Parental Control** > **Add New PCP** > **Add** to open the following screen.

Note: Do not include "HTTP" or "HTTPS" in the keyword. HTTPS connections cannot be blocked by Parental Control.

Figure 135 Security > Parental Control > Add/Edit PCP > Add



The following table describes the fields in this screen.

Table 88 Parental Control Rule: Add/Edit > Add Keyword

LABEL	DESCRIPTION
Site/URL Keyword	Enter a keyword and click **OK** to have the Zyxel Device block access to the website URLs that contain the keyword.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 19
Scheduler Rule

19.1 Scheduler Rule Overview

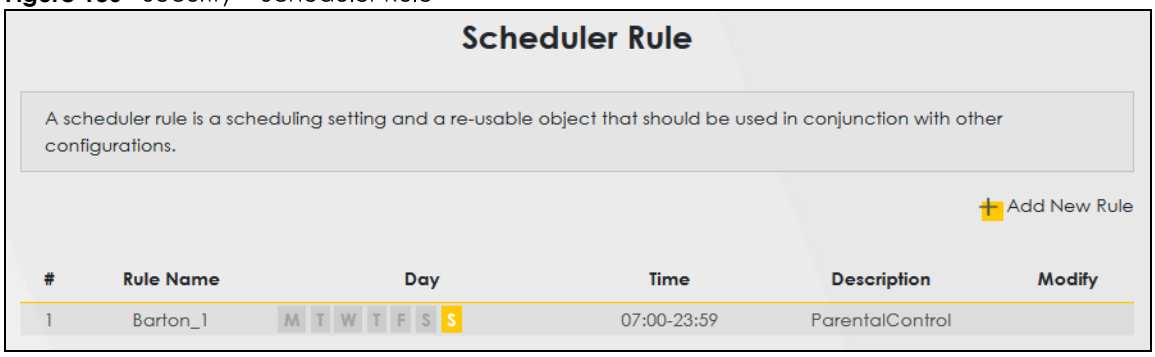
A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

19.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

Click **Security > Scheduler Rule** to open the following screen.

Figure 136 Security > Scheduler Rule



The following table describes the fields in this screen.

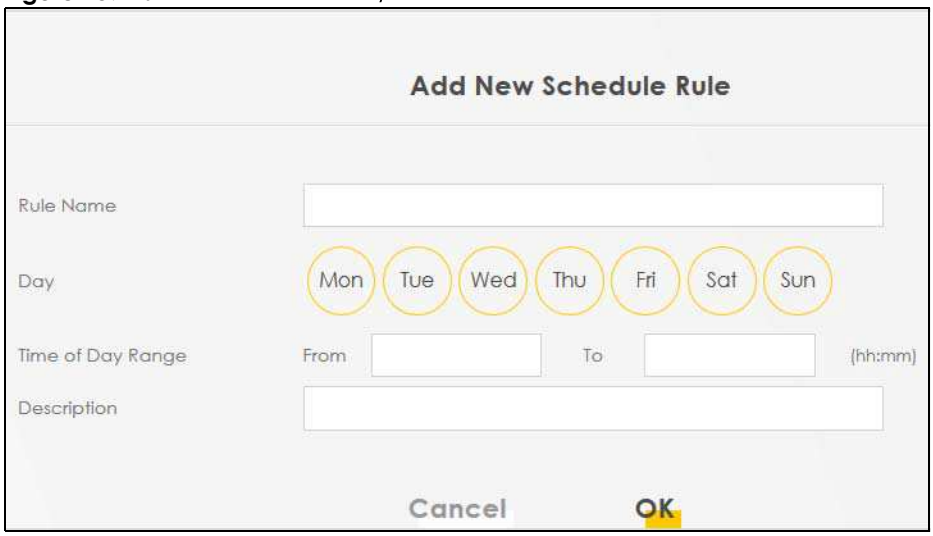
Table 89 Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

19.2.1 Add/Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a schedule rule.

Figure 137 Scheduler Rule: Add/Edit



The following table describes the fields in this screen.

Table 90 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 20
Certificates

20.1 Certificates Overview

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

20.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Zyxel Device's CA-signed certificates (Section 20.4 on page 224).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Zyxel Device (Section 20.4 on page 224).

20.2 What You Need to Know

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

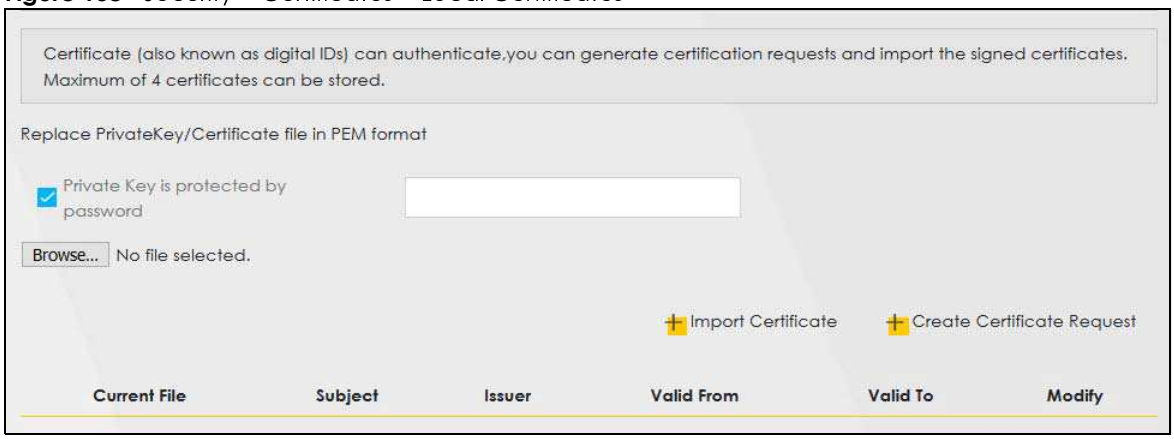
Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

20.3 Local Certificates

Click **Security > Certificates** to open the **Local Certificates** screen. Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Figure 138 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

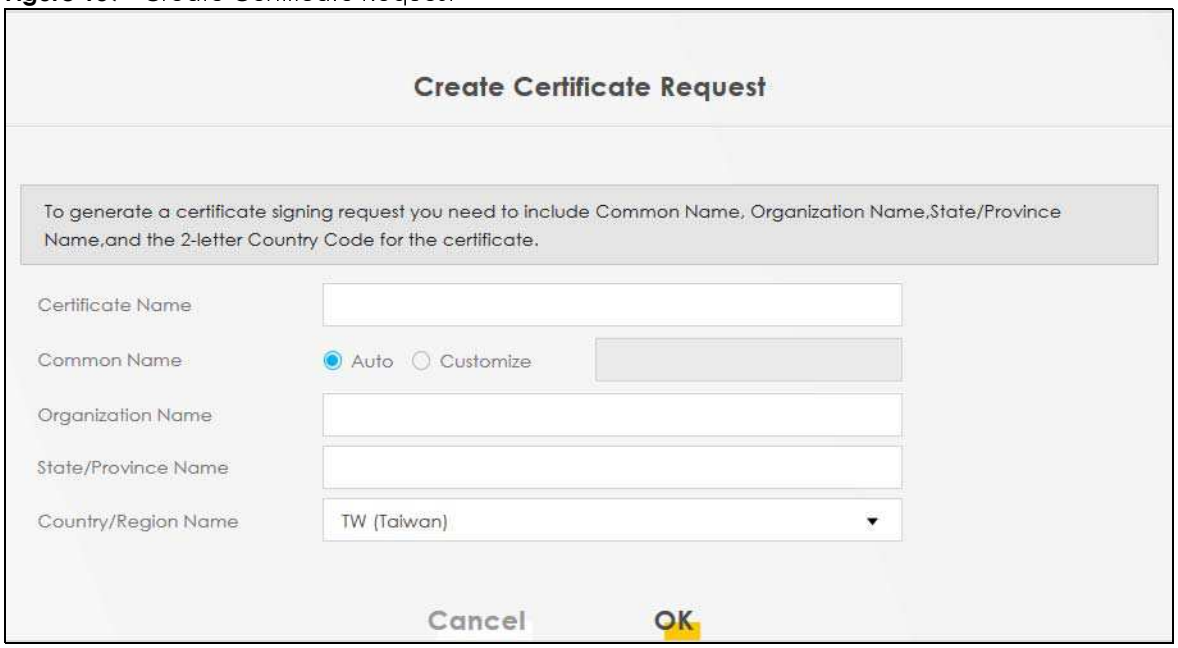
Table 91 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password	Select the check box and enter the private key into the text box to store it on the Zyxel Device. The private key should not exceed 63 ASCII characters (not including spaces).
Browse / Choose File	Click **Browse** or **Choose File** to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

20.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 139 Create Certificate Request



The following table describes the labels in this screen.

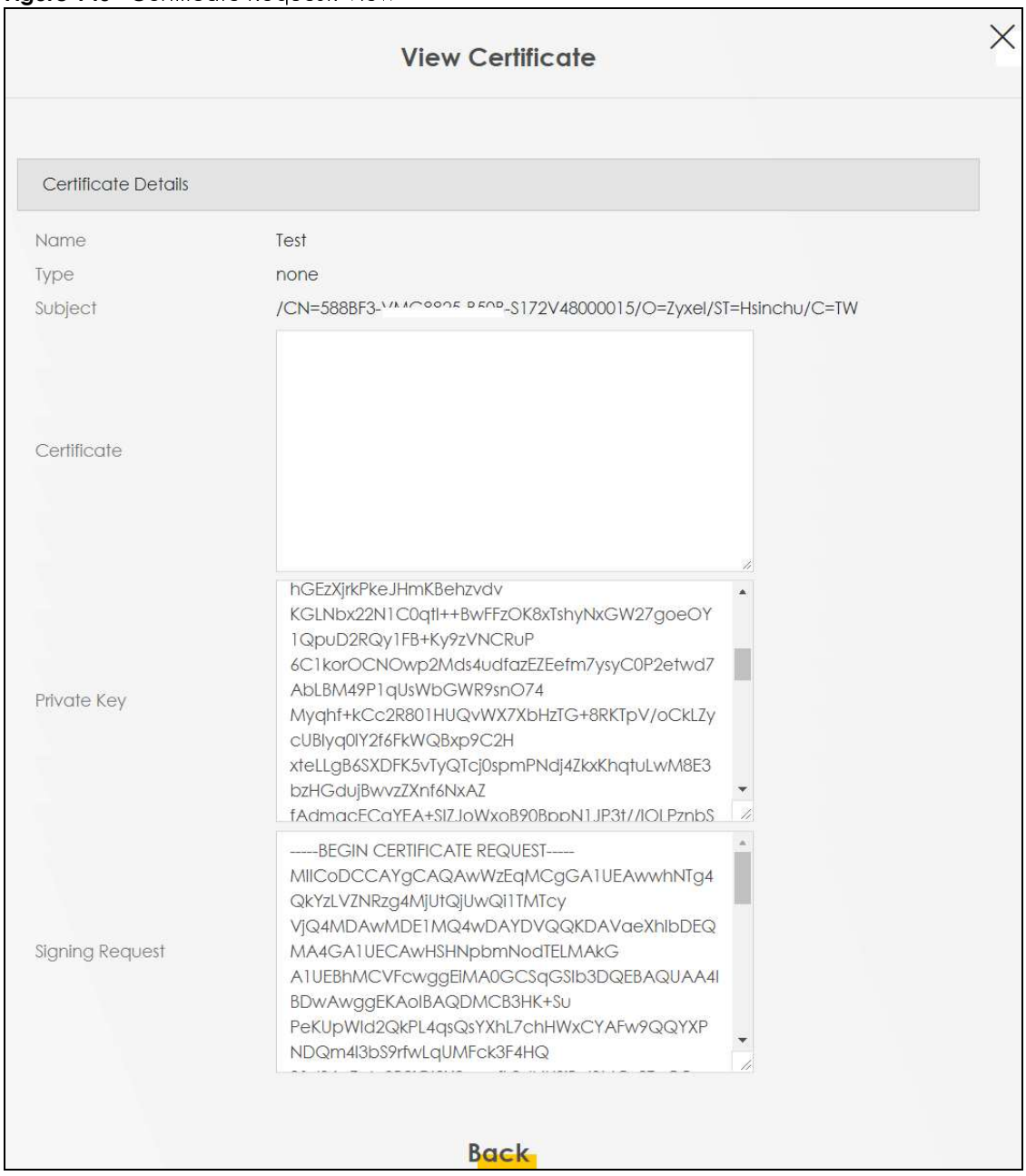
Table 92 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the Zyxel Device configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

20.3.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored.

Figure 140 Certificate Request: View



The following table describes the fields in this screen.

Table 93 Certificate Request: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 93 Certificate Request: View (continued)

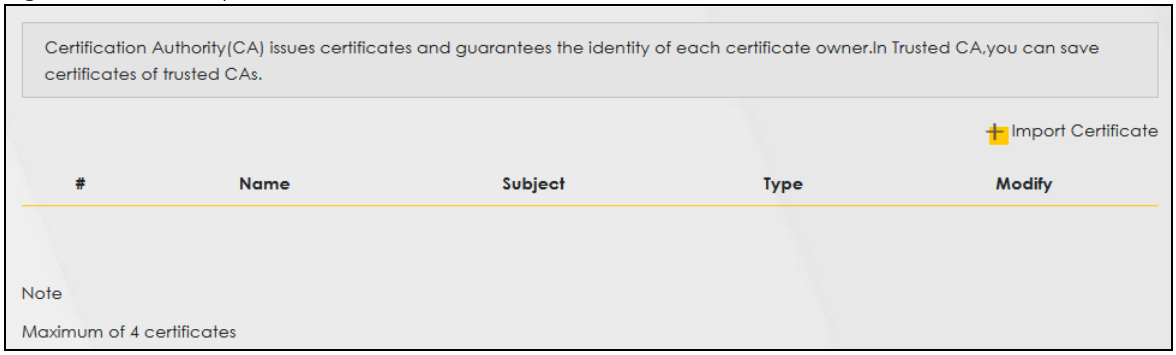
LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

20.4 Trusted CA

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

Note: You can have a maximum of 4 trusted certificates.

Figure 141 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

Table 94 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.

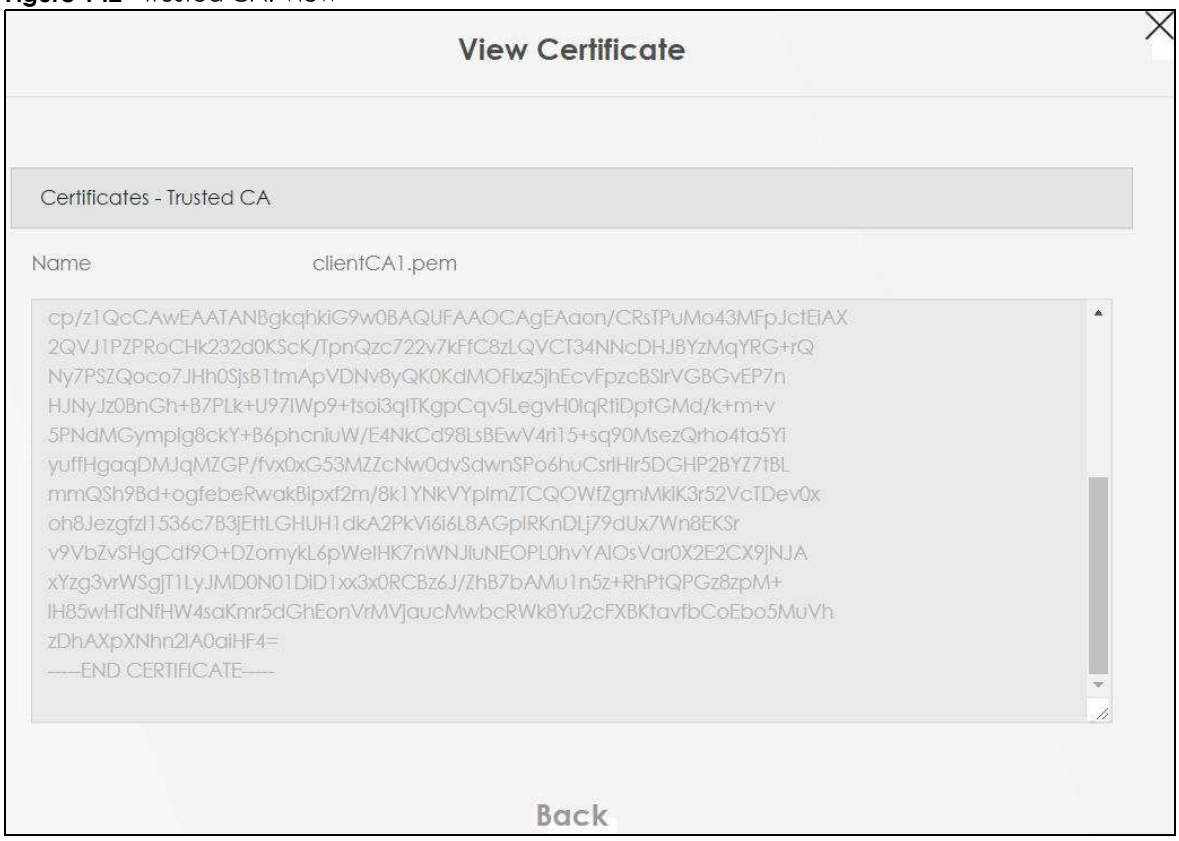
Table 94 Security > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

20.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Figure 142 Trusted CA: View



The following table describes the fields in this screen.

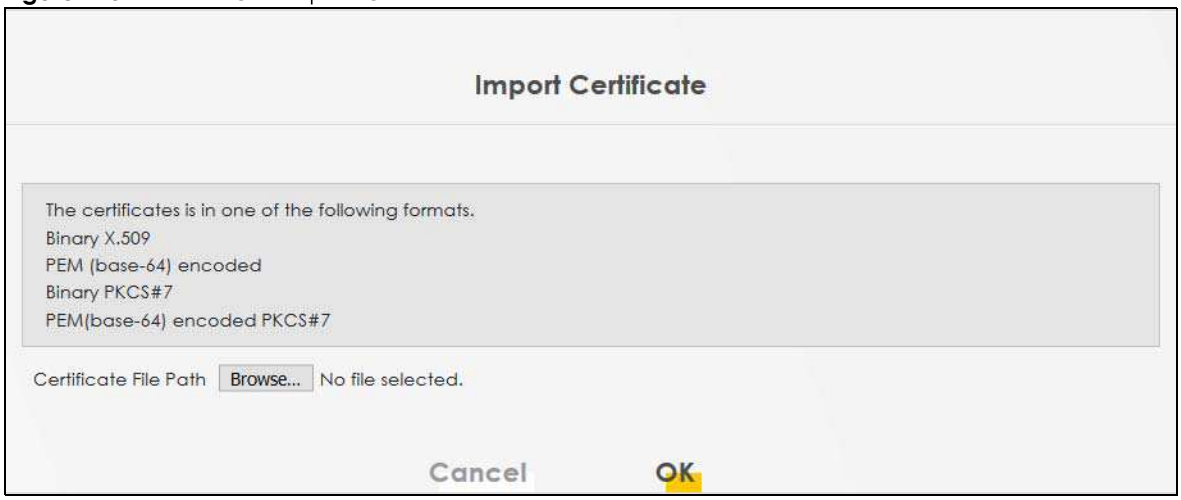
Table 95 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

20.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Zyxel Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

Figure 143 Trusted CA: Import Certificate



The following table describes the fields in this screen.

Table 96 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Click **Browse** or **Choose File** and select the certificate you want to upload.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 21
Log

21.1 Log Overview

These screens allow you to determine the categories of events that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through e-mail) or to a syslog server.

21.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 21.2 on page 228).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 21.3 on page 229).

21.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 97 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

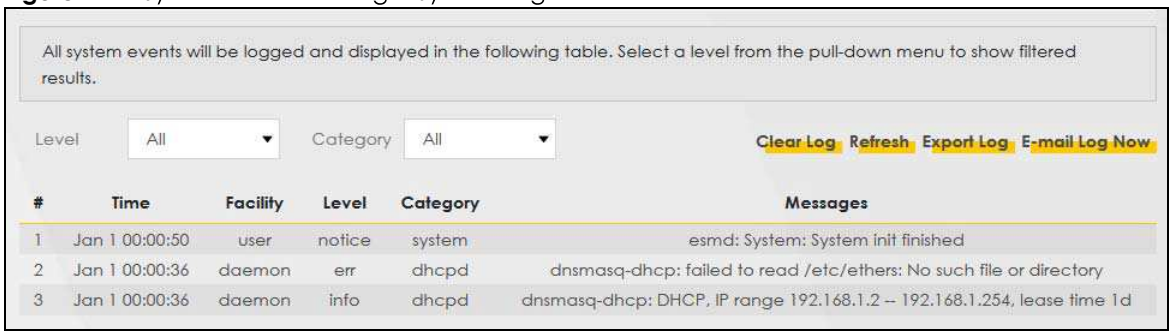
Table 97 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

21.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log** > **System Log** to open the **System Log** screen.

Figure 144 System Monitor > Log > System Log



The following table describes the fields in this screen.

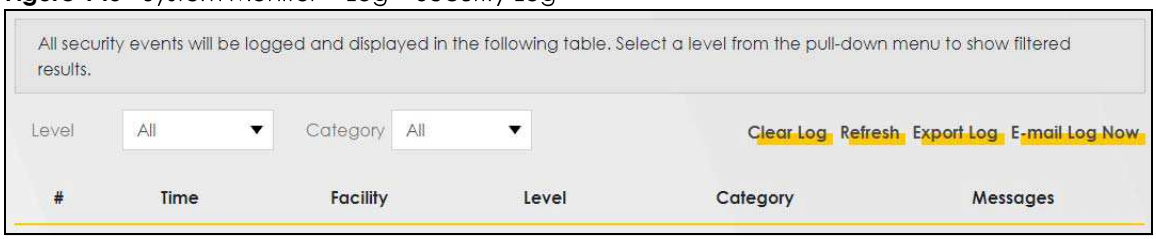
Table 98 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to save the current list of logs to your computer.
E-mail Log Now	Click this to send the log file(s) to the e-mail address you specify in the **Maintenance > E-mail Notification** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

21.3 Security Log

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 145 System Monitor > Log > Security Log



The following table describes the fields in this screen.

Table 99 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to save the current list of logs to your computer.
E-mail Log Now	Click this to send the log file(s) to the e-mail address you specify in the **Maintenance > E-mail Notification** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 22
Traffic Status

22.1 Traffic Status Overview

Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN/LAN interfaces and NAT.

22.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 22.2 on page 230).
- Use the **LAN** screen to view the LAN traffic statistics (Section 22.3 on page 231).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's client(s) (Section 22.4 on page 232).

22.2 WAN Status

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figures in this screen show the total number of bytes received and sent through the Zyxel Device's WAN interface. Packet statistics for each WAN interface are listed in the tables below.

Figure 146 System Monitor > Traffic Status > WAN

The following table describes the fields in this screen.

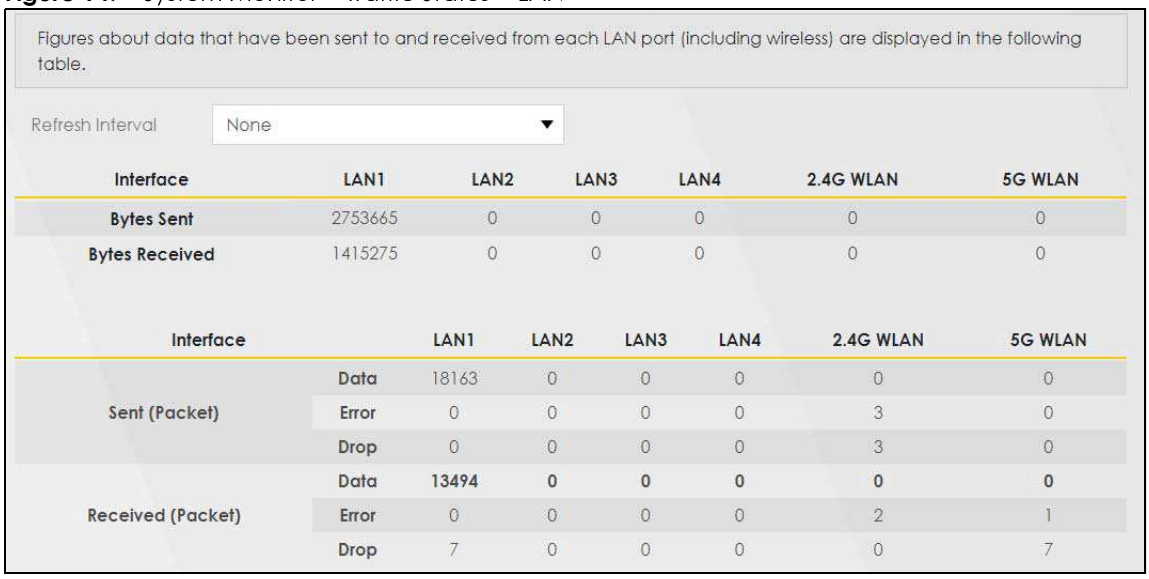
Table 100 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

22.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 147 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

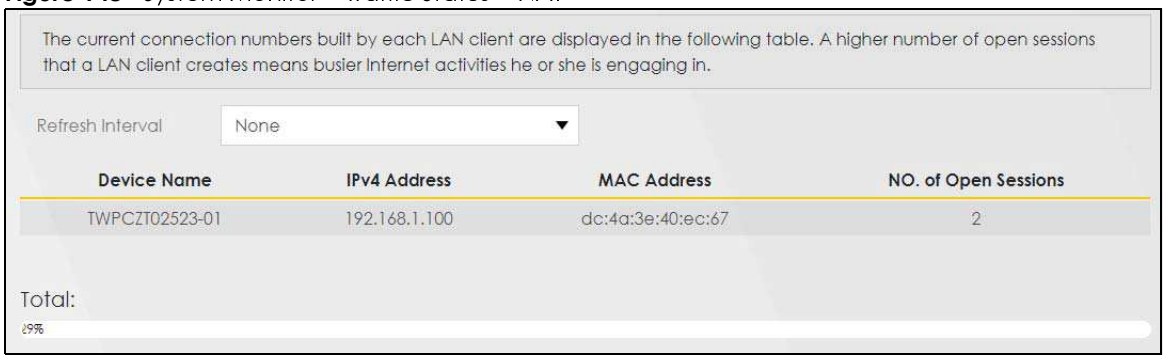
Table 101 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or wireless LAN interface on the Zyxel Device.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or wireless LAN interfaces on the Zyxel Device.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

22.4 NAT Status

Click **System Monitor > Traffic Status > NAT** to open the following screen. This screen lists the devices that have received an IP address from the Zyxel Device's LAN or WLAN interface(s) and have ever established a session with the Zyxel Device.

Figure 148 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 102 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Session	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the Zyxel Device can support is currently being used by all connected hosts.

CHAPTER 23
ARP Table

23.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

23.1.1 How ARP Works

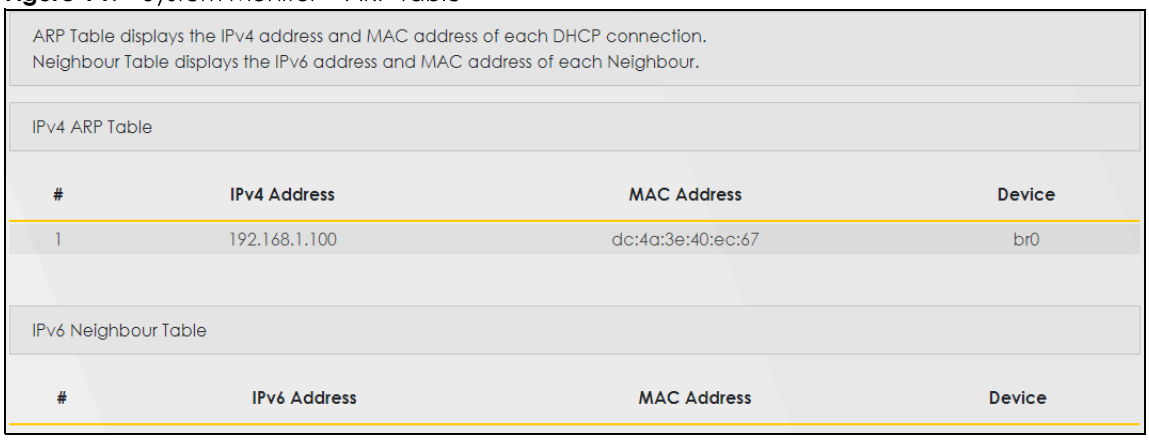
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

23.2 ARP Table Settings

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the client devices on the LAN or WLAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 149 System Monitor > ARP Table



The following table describes the labels in this screen.

Table 103 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP or neighbor table entry.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port on the Zyxel Device.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the name of the Zyxel Device's interface to which the device is connected.

CHAPTER 24
Routing Table

24.1 Routing Table Overview

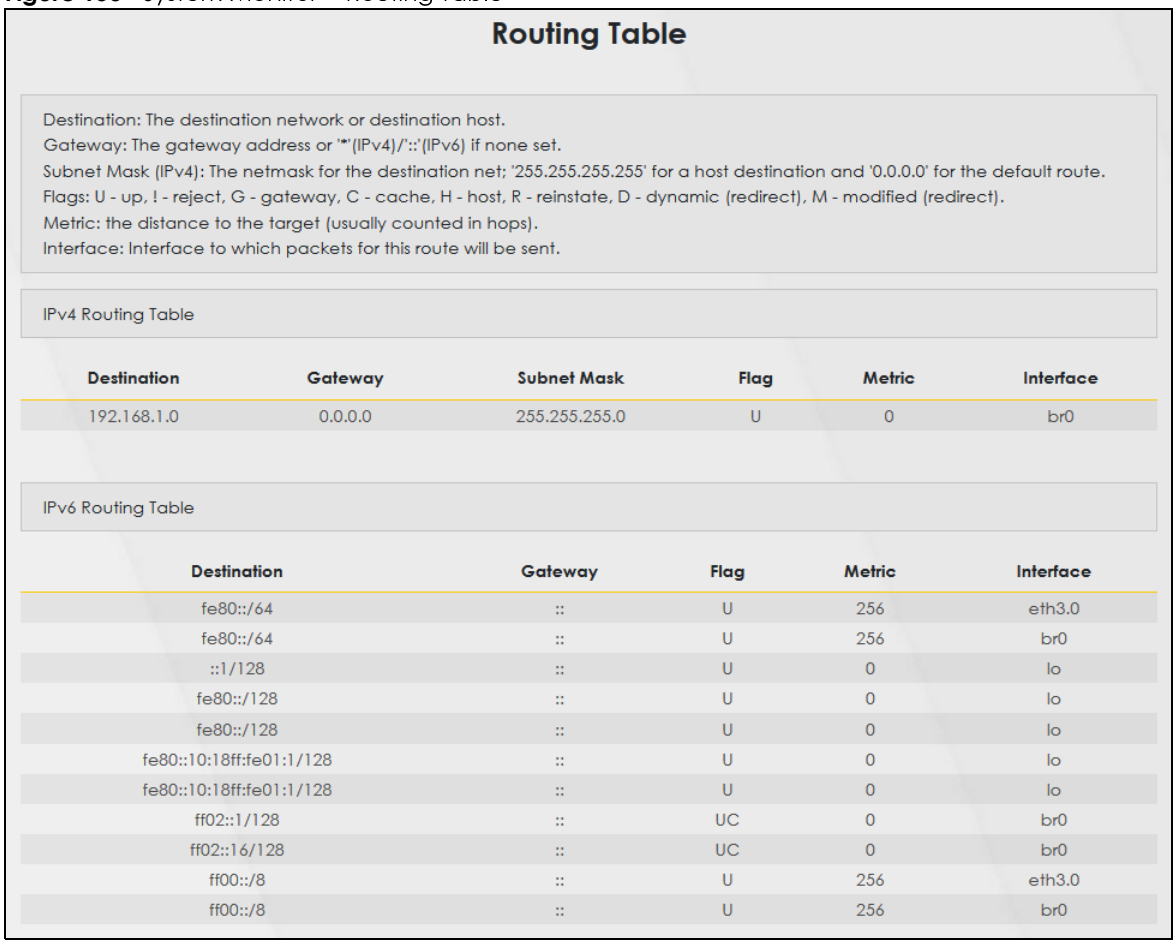
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

24.2 Routing Table Settings

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*'(IPv4)/'::'(IPv6) if none is set.

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 150 System Monitor > Routing Table



Routing Table

Destination: The destination network or destination host.
Gateway: The gateway address or '*'(IPv4)/'::'(IPv6) if none set.
Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route.
Flags: U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).
Metric: the distance to the target (usually counted in hops).
Interface: Interface to which packets for this route will be sent.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth3.0
fe80::/64	::	U	256	br0
::1/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::10:18ff:fe01:1/128	::	U	0	lo
fe80::10:18ff:fe01:1/128	::	U	0	lo
ff02::1/128	::	UC	0	br0
ff02::16/128	::	UC	0	br0
ff00::/8	::	U	256	eth3.0
ff00::/8	::	U	256	br0

The following table describes the labels in this screen.

Table 104 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4/IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.
Flag	This indicates the route status. **U-Up:** The route is up. **!-Reject:** The route is blocked and will force a route lookup to fail. **G-Gateway:** The route uses a gateway to forward traffic. **H-Host:** The target of the route is a host. **R-Reinstate:** The route is reinstated for dynamic routing. **D-Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M-Modified (redirect):** The route is modified from a routing daemon or redirect.

Table 104 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface	This indicates the name of the interface through which the route is forwarded. **brx** indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively. **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. **ppp0** indicates a WAN interface using PPPoE. **wlx** indicates a wireless interface where x can be 0~1. For some models, **wl1** indicates 5 GHz wireless interface, and **wl0** indicates 2.4 GHz wireless interface. For the other models, **wl1** indicates 5 GHz wireless interface, and **wl0** indicates 2.4 GHz wireless interface.

CHAPTER 25
Multicast Status

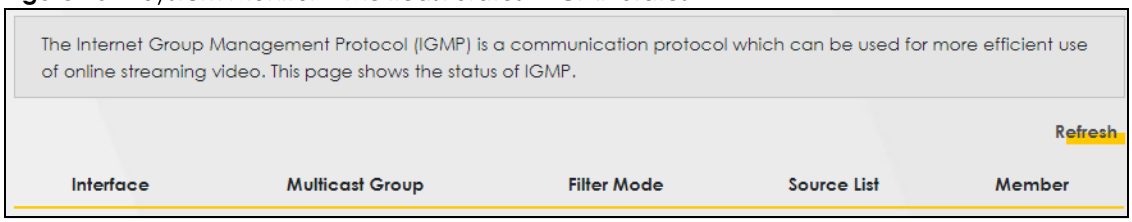
25.1 Multicast Status Overview

Use the **Multicast Status** screens to view IPv4 or IPv6 multicast group information.

25.2 IGMP Status

Use this screen to look at the current list of IPv4 multicast groups the Zyxel Device manages through IGMP. Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. You can configure IGMP settings in **System Monitor > Multicast Status > IGMP Status**.

Figure 151 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

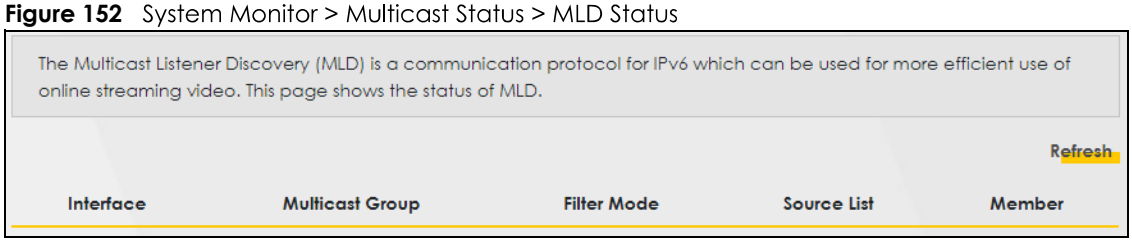
Table 105 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of the Zyxel Device's interface that belongs to an IGMP multicast group.
Multicast Group	This field displays the address of the IGMP multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

25.3 MLD Status

Use this screen to look at the current list of IPv6 multicast groups the Zyxel Device manages through MLD. Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3. You can configure MLD in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 152 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 106 System Monitor > Multicast Status > MLD Status

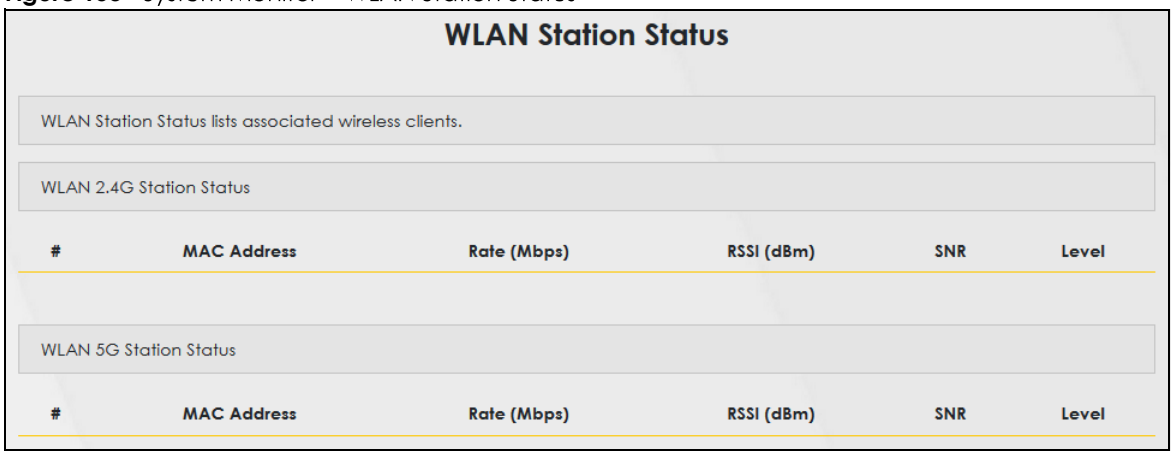
LABEL	DESCRIPTION
Refresh	Click this button to update the status on this screen.
Interface	This field displays the name of the Zyxel Device's interface that belongs to an MLD multicast group.
Multicast Group	This field displays the address of the MLD multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

CHAPTER 26
WLAN Station Status

26.1 WLAN Station Status Overview

Click **System Monitor > WLAN Station Status** to open the following screen. Use this screen to view information and status of the wireless stations (wireless clients) that are currently associated with the Zyxel Device. Being associated means that a wireless client (for example, your computer with a wireless network card installed) has connected successfully to an AP (or wireless router) using the same SSID, channel, and WiFi security settings.

Figure 153 System Monitor > WLAN Station Status



The following table describes the labels in this screen.

Table 107 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated wireless station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's wireless connection. The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.

Table 107 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated wireless station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal. **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 27
System

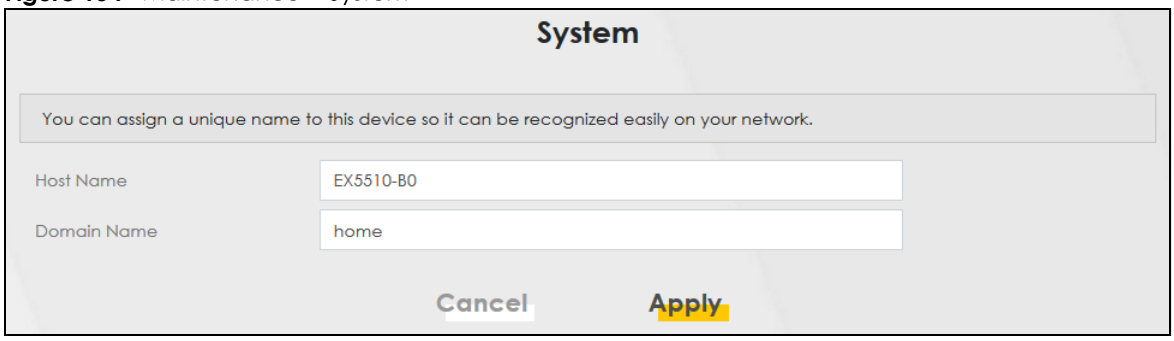
27.1 System Overview

In the **System** screen, you can name your Zyxel Device (Host) and give it an associated domain name. Domain is the name given to a network. It will be required to reach a network from an external point (like the Internet). Knowing the domain name will allow you to reach a particular network, and knowing the host name will allow you to reach a particular device. For this reason, accessing a device from another device within a network may work with just the host name (without the use of the domain name).

27.2 System Settings

Click **Maintenance > System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 154 Maintenance > System



The following table describes the labels in this screen.

Table 108 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 28
User Account

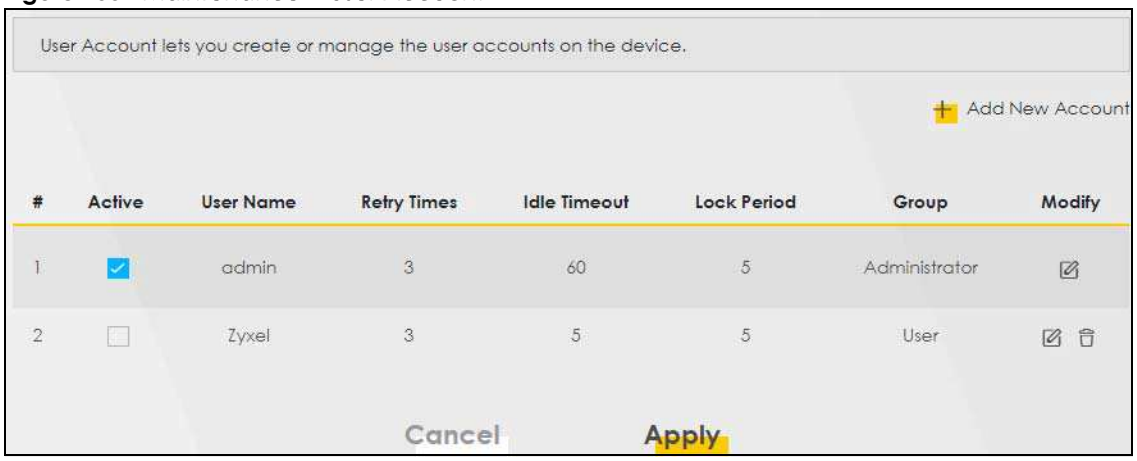
28.1 User Account Overview

In the **User Account** screen, you can view the settings of the 'admin' and other user accounts that you use to log into the Zyxel Device to manage it.

28.2 User Account Settings

Click **Maintenance > User Account** to open the following screen. Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

Figure 155 Maintenance > User Account



The following table describes the labels in this screen.

Table 109 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number of the user account.
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

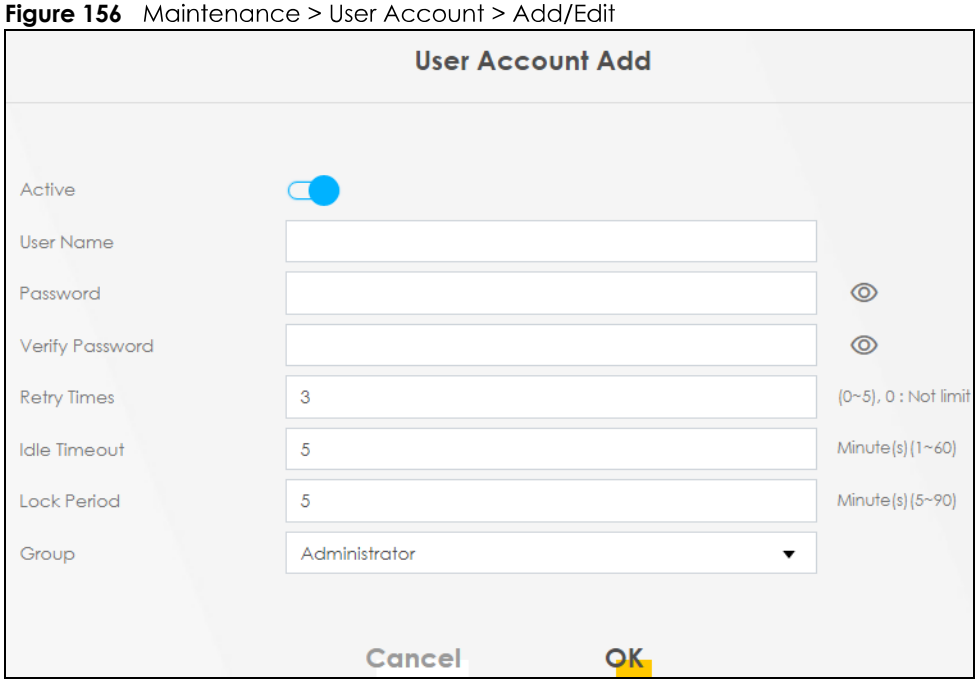
Table 109 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Idle Timeout	This field displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privileges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

28.2.1 User Account Add/Edit

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen.

Figure 156 Maintenance > User Account > Add/Edit



The following table describes the labels in this screen.

Table 110 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the user account.
User Name	Enter a new name for the account. The **User Name** must contain 1 to 15 characters, including 0 to 9, a to z, and !@#%*()-_+=~.,{}[]\. Spaces are not allowed.
Password	Type your new system password (up to 256 characters). The **Password** must contain 6 to 64 characters, including 0 to 9 and a to z. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.

Table 110 Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privileges. **Administrator** and **User** privileges are mostly the same, but the following menu items will only display when you log in as an **Administrator**. • Quick Start **Wizard** • **Network Setting** • **Security** settings • **Maintenance** > **System** • **Maintenance** > **SNMP**
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 29
Remote Management

29.1 Remote Management Overview

Use remote management to control what services you can use through which interface(s) in order to manage the Zyxel Device.

29.1.1 What You Can Do in this Chapter

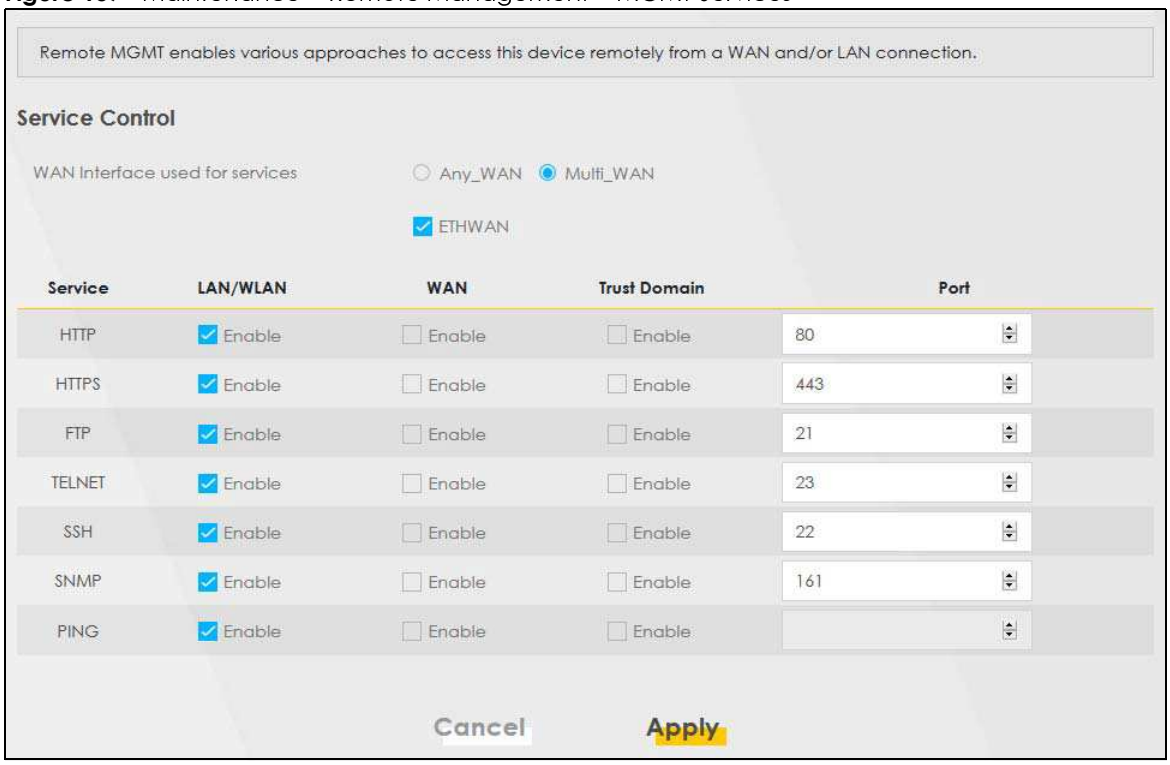
- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 29.2 on page 247).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 29.3 on page 249).

Note: The Zyxel Device is managed using the Web Configurator.

29.2 MGMT Services

Use this screen to configure through which interface(s), each service can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance > Remote Management > MGMT Services** to open the following screen.

Figure 157 Maintenance > Remote Management > MGMT Services



The following table describes the fields in this screen.

Table 111 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Service	This is the service you may use to access the Zyxel Device. • **HTTP** provides a non secured way. • **HTTPS** is the secured version of HTTP, it makes sure that your data cannot be read during transmission. • **FTP** is the most common way of communication between two devices. • **TELNET** provides a way to control your Zyxel Device remotely. • **SSH** prevents leakage of data during remote management. Additionally, it can encrypt all transmitted data. • **SNMP** is a management system that monitors devices connected to the Internet. • **PING** is a diagnostic tool that can check if your Zyxel Device is connected to the Internet.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the **Maintenance > Remote MGMT > Trust Domain** screen. If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear **WAN**, select **Trust Domain** and configure the allowed IP address(es) in the **Trust Domain** screen.