Table 299 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

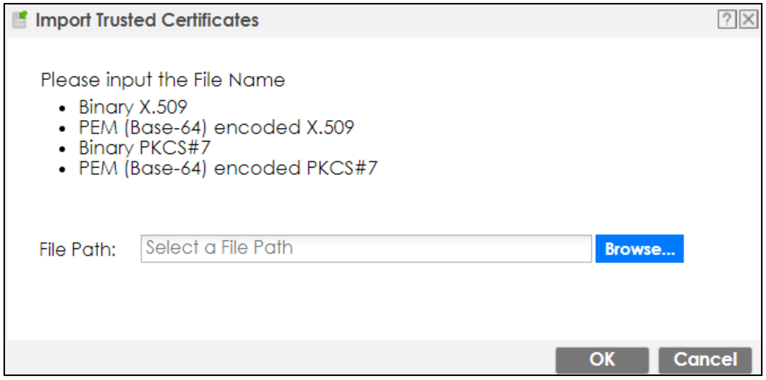
LABEL	DESCRIPTION
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays the method that the Zyxel Device generates and stores a request for server authentication, client authentication, or IKE Intermediate authentication certificate.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

35.11.4.2 The Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the Zyxel Device.

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

Figure 474 Configuration > Object > Certificate > Trusted Certificates > Import



Import Trusted Certificates

Please input the File Name

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path: Select a File Path

The following table describes the labels in this screen.

Table 300 Configuration > Object > Certificate > Trusted Certificates > Import

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

35.11.5 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the Zyxel Device checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the Zyxel Device only gets information on the certificates that it needs to verify, not a huge list. When the Zyxel Device requests certificate status information, the OCSP server returns a “expired”, “current” or “unknown” response.

35.12 ISP Account Overview

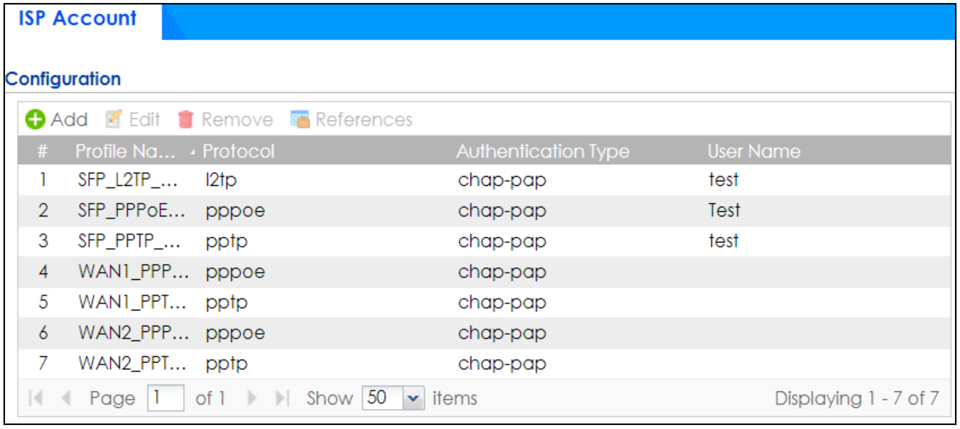
Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP/L2TP interfaces. An ISP account is a profile of settings for Internet access using PPPoE, PPTP or L2TP.

Use the **Object** > **ISP Account** screens (Section 35.12.1 on page 710) to create and manage ISP accounts in the Zyxel Device.

35.12.1 ISP Account Summary

This screen provides a summary of ISP accounts in the Zyxel Device. To access this screen, click **Configuration > Object** > **ISP Account**.

Figure 475 Configuration > Object > ISP Account



#	Profile Na...	Protocol	Authentication Type	User Name
1	SFP_L2TP_...	l2tp	chap-pap	test
2	SFP_PPPoE...	pppoe	chap-pap	Test
3	SFP_PPTP_...	pptp	chap-pap	test
4	WAN1_PPP...	pppoe	chap-pap	
5	WAN1_PPT...	pptp	chap-pap	
6	WAN2_PPP...	pppoe	chap-pap	
7	WAN2_PPT...	pptp	chap-pap	

The following table describes the labels in this screen. See the ISP Account Add/Edit section below for more information as well.

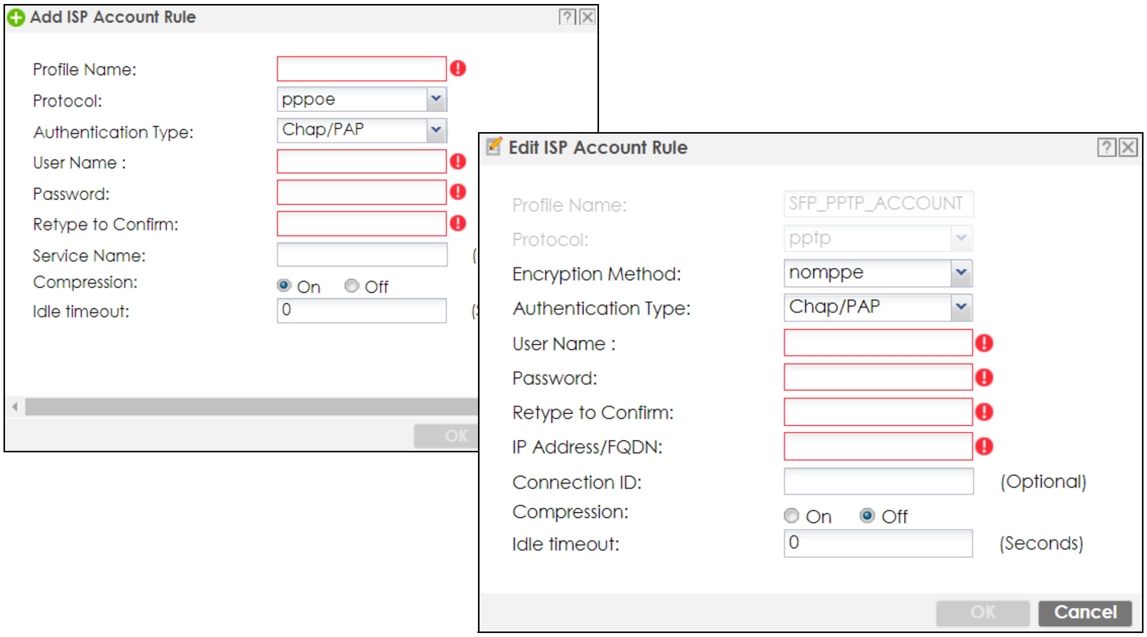
Table 301 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

35.12.1.1 ISP Account Add/Edit

The **ISP Account Add/Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See Section 35.12.1 on page 710.) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 476 Configuration > Object > ISP Account > Edit



Add ISP Account Rule

Profile Name:

Protocol: pppoe

Authentication Type: Chap/PAP

User Name :

Password:

Retype to Confirm:

Service Name:

Compression: ● On ○ Off

Idle timeout: 0

Edit ISP Account Rule

Profile Name: SFP_PPTP_ACCOUNT

Protocol: pptp

Encryption Method: nomppe

Authentication Type: Chap/PAP

User Name :

Password:

Retype to Confirm:

IP Address/FQDN:

Connection ID: (Optional)

Compression: ○ On ● Off

Idle timeout: 0 (Seconds)

The following table describes the labels in this screen.

Table 302 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Your ISP will provide you with a related username, password and IP (server) information. Options are: **pppoe** - This ISP account uses the PPPoE protocol. **pptp** - This ISP account uses the PPTP protocol. **l2tp** - This ISP account uses the L2TP protocol.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Zyxel Device accepts either CHAP or PAP when requested by this remote node. **Chap** - Your Zyxel Device accepts CHAP only. **PAP** - Your Zyxel Device accepts PAP only. **MSCHAP** - Your Zyxel Device accepts MSCHAP only. **MSCHAP-V2** - Your Zyxel Device accepts MSCHAP-V2 only.
Encryption Method	This field is available if this ISP account uses the **PPTP** protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **nomppe** - This ISP account does not use MPPE. **mppe-40** - This ISP account uses 40-bit MPPE. **mppe-128** - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.

Table 302 Configuration > Object > ISP Account > Edit (continued)

LABEL	DESCRIPTION
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the PPTP or L2TP server.
Connection ID	This field is available if this ISP account uses the **PPTP** protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select **On** button to turn on stac compression, and select **Off** to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the Zyxel Device automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click **OK** to save your changes back to the Zyxel Device. If there are no errors, the program returns to the **ISP Account** screen. If there are errors, a message box explains the error, and the program stays in the **ISP Account Edit** screen.
Cancel	Click **Cancel** to return to the **ISP Account** screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

35.13 DHCPv6 Overview

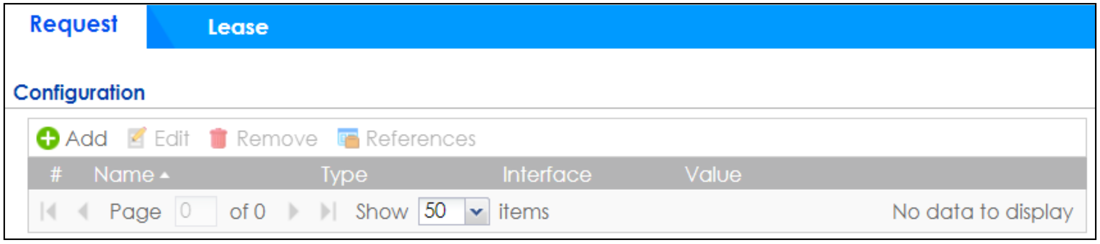
This section describes how to configure DHCPv6 request type and lease type objects.

- The **Request** screen (see Section 35.13.1 on page 713) allows you to configure DHCPv6 request type objects.
- The **Lease** screen (see Section 35.2.3 on page 624) allows you to configure DHCPv6 lease type objects.

35.13.1 The DHCPv6 Request Screen

The **Request** screen allows you to add, edit, and remove DHCPv6 request type objects. To access this screen, login to the Web Configurator, and click **Configuration > Object > DHCPv6 > Request**.

Figure 477 Configuration > Object > DHCPv6 > Request



The following table describes the labels in this screen.

Table 303 Configuration > Object > DHCPv6 > Request

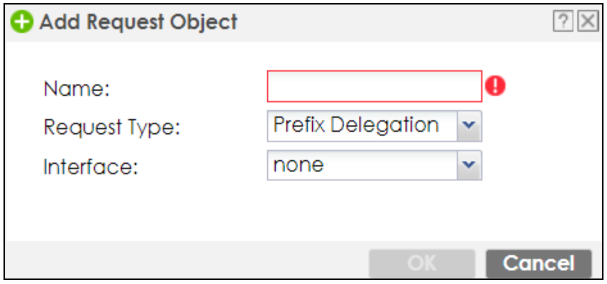
LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific object.
Name	This field displays the name of each request object.
Type	This field displays the request type of each request object.
Interface	This field displays the interface used for each request object.
Value	This field displays the value for each request object.

35.13.1.1 DHCPv6 Request Add/Edit Screen

The **Request Add/Edit** screen allows you to create a new request object or edit an existing one.

To access this screen, go to the **Request** screen (see Section 35.13.1 on page 713), and click either the **Add** icon or an **Edit** icon.

Figure 478 Configuration > DHCPv6 > Request > Add



Add Request Object

Name:

Request Type: Prefix Delegation

Interface: none

The following table describes the labels in this screen.

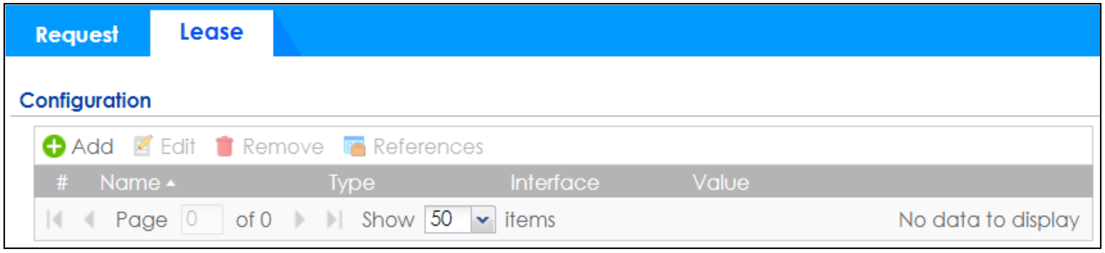
Table 304 Configuration > DHCPv6 > Request > Add

LABEL	DESCRIPTION
Name	Type the name for this request object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Request Type	Select the request type for this request object. You can choose from **Prefix Delegation**, **DNS Server**, **NTP Server**, or **SIP Server**.
Interface	Select the interface for this request object.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.13.2 The DHCPv6 Lease Screen

The **Lease** screen allows you to add, edit, and remove DHCPv6 lease type objects. To access this screen, login to the Web Configurator, and click **Configuration > Object > DHCPv6 > Lease**.

Figure 479 Configuration > Object > DHCPv6 > Lease



The following table describes the labels in this screen.

Table 305 Configuration > Object > DHCPv6 > Lease

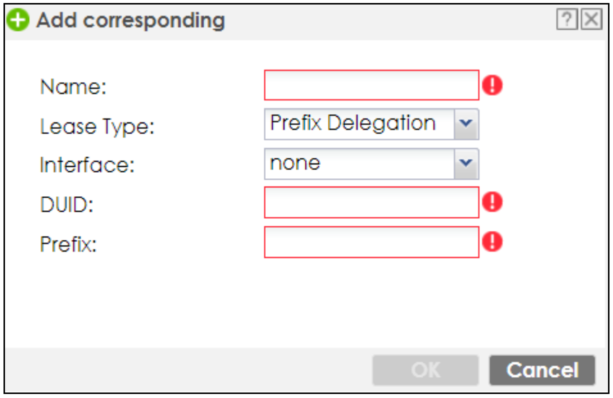
LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific object.
Name	This field displays the name of each lease object.
Type	This field displays the request type of each lease object.
Interface	This field displays the interface used for each lease object.
Value	This field displays the value for each lease object.

35.13.2.1 DHCPv6 Lease Add/Edit Screen

The **Lease Add/Edit** screen allows you to create a new lease object or edit an existing one.

To access this screen, go to the **Lease** screen (see Section 35.13.2 on page 715), and click either the **Add** icon or an **Edit** icon.

Figure 480 Configuration > DHCPv6 > Lease > Add



Name:
Lease Type: Prefix Delegation
Interface: none
DUID:
Prefix:

The following table describes the labels in this screen.

Table 306 Configuration > DHCPv6 > Lease > Add/Edit

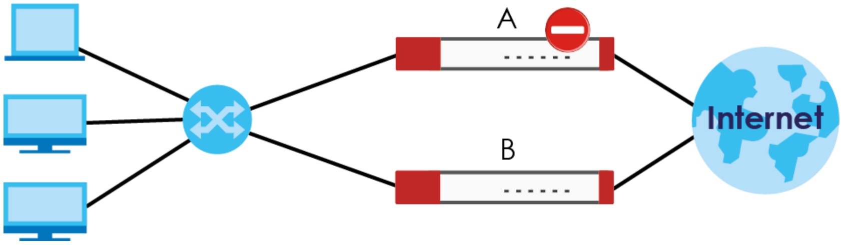
LABEL	DESCRIPTION
Name	Type the name for this lease object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Lease Type	Select the lease type for this lease object. You can choose from **Prefix Delegation**, **DNS Server**, **Address**, **Address Pool**, **NTP Server**, or **SIP Server**.
Interface	Select the interface for this lease object.
DUID	If you select **Prefix Delegation** or **Address** in the **Lease Type field**, enter the DUID of the interface.
Address	If you select **Address** in the **Lease Type** field, enter the IP address of the DHCPv6 server.
Prefix	If you select **Prefix Delegation** or **Address** in the **Lease Type field**, enter the IPv6 prefix of the interface.
DNS Server	If you select **DNS Server** in the **Lease Type field**, select a request object or **User Defined** in the **DNS Server** field and enter the IP address of the DNS server in the **User Defined Address** field below.
Starting IP Address	If you select **Address Pool** in the **Lease Type field**, enter the first of the contiguous addresses in the IP address pool.
End IP Address	If you select **Address Pool** in the **Lease Type field**, enter the last of the contiguous addresses in the IP address pool.
NTP Server	If you select **NTP Server** in the **Lease Type field**, select a request object or **User Defined** in the **NTP Server** field and enter the IP address of the NTP server in the **User Defined Address** field below.
SIP Server	If you select **SIP Server** in the **Lease Type field**, select a request object or **User Defined** in the **SIP** field and enter the IP address of the SIP server in the **User Defined Address** field below.
User Defined Address	If you select **DNS Server**, **NTP Server**, or **SIP Server** as your lease type, you must enter the IP address of the server your selected.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 36 Device HA

36.1 Device HA Overview

Device HA lets a backup (or passive) Zyxel Device (**B**) automatically take over if the master (or active) Zyxel Device (**A**) fails.

Figure 481 Device HA Backup Taking Over for the Master



36.1.1 What You Can Do in These Screens

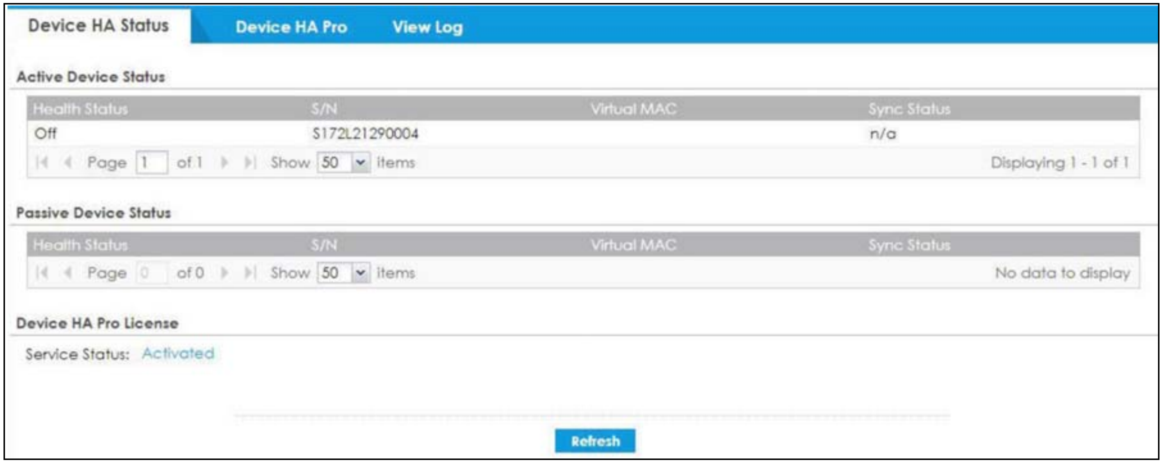
- Use the **Device HA Status** screen (Section 36.2 on page 717) to see the license status for Device HA Pro, and see the status of the active and passive devices.
- Use the **Device HA Pro** screen (Section 36.3 on page 719) to configure Device HA Pro global settings, monitored interfaces and synchronization settings.
- Use the **View Log** screen (Section 36.4 on page 722) to see logs of the active and passive devices.

36.2 Device HA Status

Use this screen to view Device HA Pro license status and details on the active and passive Zyxel Devices.

Go to **Configuration > Device HA > Device HA Status** to view the following screen.

Figure 482 Configuration > Device HA > Device HA Status



Active Device Status

Health Status	S/N	Virtual MAC	Sync Status
Off	S172L21290004		n/a

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Passive Device Status

Health Status	S/N	Virtual MAC	Sync Status

Page 0 of 0 Show 50 items No data to display

Device HA Pro License

Service Status: Activated

The following table describes the labels in this screen.

Table 307 Configuration > Device HA > Device HA Status

LABEL	DESCRIPTION
Active Device Status	This section displays information on the active Zyxel Device with an activated Device HA Pro license.
Health Status	This displays **Off** or **On** depending on whether Device HA Pro is disabled or enabled on the active Zyxel Device.
S/N	This displays the serial number of the active Zyxel Device.
Virtual MAC	This displays the hardware MAC address of the active Zyxel Device with an activated Device HA Pro license.
Synch Status	This displays the synchronization progress, **No Progress** / **Fail** / **Abort** / **Success** / **In Progress**, between the active Zyxel Device with an activated Device HA Pro license and the passive Zyxel Device.
Passive Device Status	This section displays information on the passive Zyxel Device with an activated Device HA Pro license.
Health Status	This displays **Off** or **On** depending on whether Device HA Pro is disabled or enabled on the passive Zyxel Device.
S/N	This displays the serial number of the passive Zyxel Device.
Virtual MAC	This displays the hardware MAC address of the passive Zyxel Device.
Synch Status	This displays the synchronization progress, **No Progress** / **Fail** / **Abort** / **Success** / **In Progress**, between the passive Zyxel Device with an activated Device HA Pro license and the active Zyxel Device.
Device HA Pro License	These are the steps to activate a Device HA Pro license on your active and passive Zyxel Devices. 1. See your Device HA Pro iCard. The card contains two keys. 2. Register your active and passive Zyxel Devices at myZyxel. 3. Activate the license by entering one key on the active Zyxel Device and the other key on the passive Zyxel Device. It doesn't matter which Zyxel Device is actually active or passive as this is dynamic in Device HA Pro.

Table 307 Configuration > Device HA > Device HA Status (continued)

LABEL	DESCRIPTION
Service Status	This field displays whether a service license is enabled at myZyxel (**Activated**) or not (**Not Activated**) or expired (**Expired**). It displays the remaining Grace Period if your license has **Expired**. It displays **Not Licensed** if there isn't a license to be activated for this service. If you need a license or a trial license has expired, click **Buy** to buy a new one. If a **Standard** license has expired, click **Renew** to extend the license. Then, click **Activate** to connect with the myZyxel server to activate the new license.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

36.3 Device HA Pro

You need a license to use Device HA Pro. Device HA Pro is easier to deploy than Device HA, is more reliable (no risk of overloading), and faster (Device HA causes a connection break of 10~30 seconds while Device HA Pro just has 1~2 seconds). In addition to configuration file backup in Device HA, device time, TCP sessions (IPv4/IPv6), IPSec VPN sessions, login/logout information, DHCP table, IP/MAC binding table and license status can also be backed up using Device HA Pro.

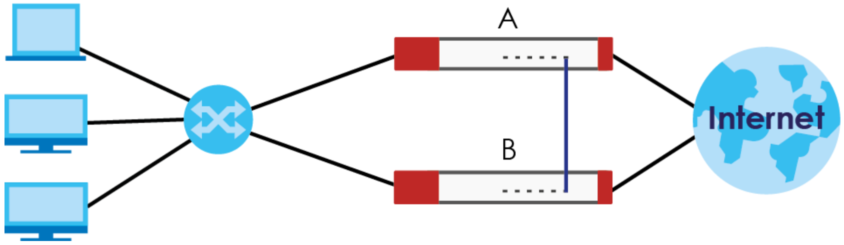
Active and Passive Devices

Device HA Pro uses a dedicated heartbeat link between an active device ('master') and a passive device ('backup') for status syncing and backup to the passive device. On the passive device, all ports are disabled except for the port with the heartbeat link.

In the following example, Zyxel Device **A** is the active device that is connected to passive device Zyxel Device **B** via a dedicated link that is used for heartbeat control, configuration synchronization and troubleshooting. All links on Zyxel Device **B** are down except for the dedicated heartbeat link.

Note: The dedicated heartbeat link port must be the highest-numbered copper Ethernet port on each Zyxel Device for Device HA Pro to work.

Figure 483 Device HA Pro



Failover from the active Zyxel Device to the passive Zyxel Device is activated when:

- A monitored interface is down.
- A monitored service (daemon) is down.
- The heartbeat link exceeds the failure tolerance.

After failover, the initial active Zyxel Device becomes the passive Zyxel Device after it recovers.

36.3.1 Deploying Device HA Pro

1 Register either the active or passive Zyxel Device with a Device HA Pro license at myZyxel. Check that it's properly licensed in **Licensing > Registration > Service** in the active Zyxel Device.

2 Make sure the passive Zyxel Device is offline, then enable Device HA in **Device HA > General** in the passive Zyxel Device.

3 Must make sure the FTP port in **System > FTP** (default 21) is the same on both Zyxel Devices. FTP is used for transferring files in the event of failover from active to passive Zyxel Device.

4 Connect the passive Zyxel Device to the active Zyxel Device using the highest-numbered copper Ethernet ports on both Zyxel Devices. This is the heartbeat interface. Make sure that this interface is not already configured for other features such as LAG, VLAN, Bridge.

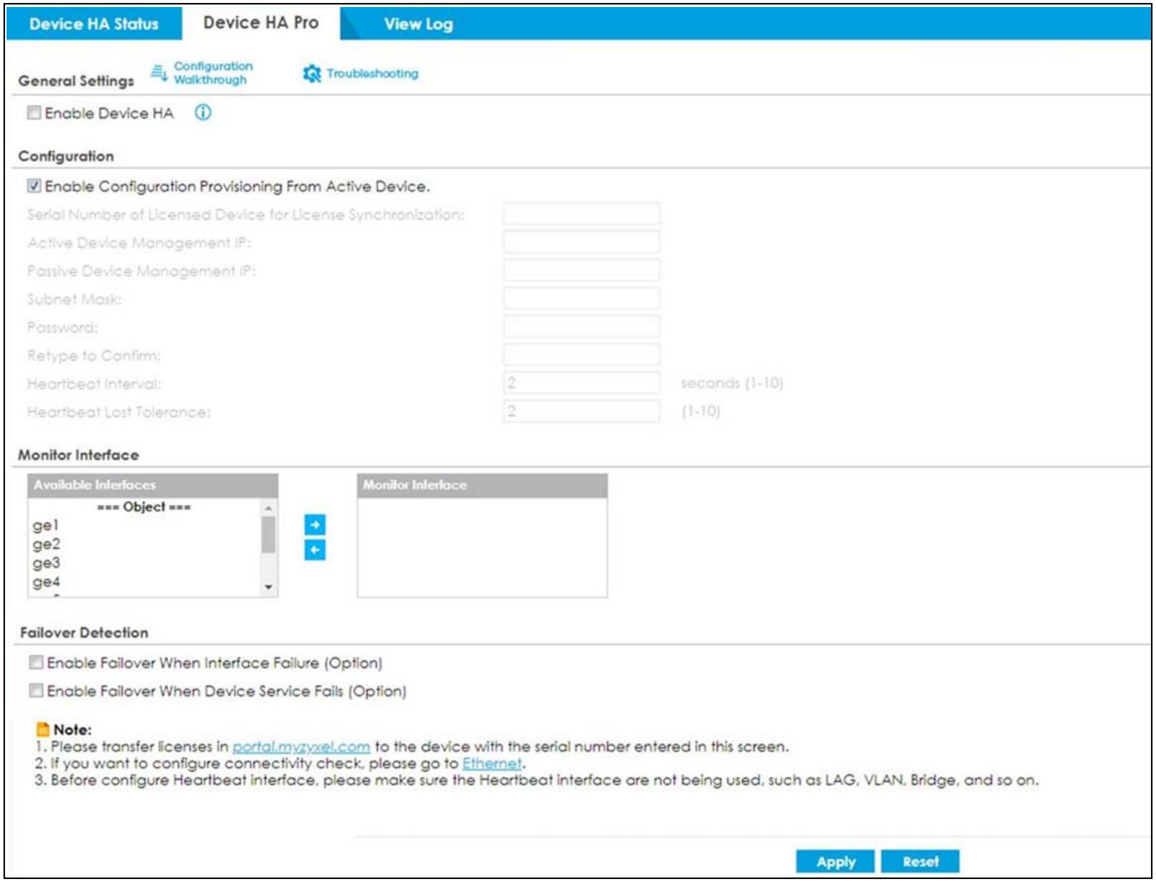
5 If both Zyxel Devices are turned on at the same time with Device HA enabled, then they may send the heartbeat at the same time. In this case, the Zyxel Device with the bigger MAC address becomes the passive Zyxel Device.

6 When using Device HA Pro to synchronize firmware, the location of the running firmware must be the same in both active and passive Zyxel Devices. For example, if the running firmware is in partition 1 in the active Zyxel Device (standby firmware in partition 2), then the running firmware must also be in partition 1 in the passive Zyxel Device (standby firmware in partition 2).

36.3.2 Configuring Device HA Pro

Go to **Configuration > Device HA > Device HA Pro** and configure the following screen.

Figure 484 Configuration > Device HA > Device HA Pro



General Settings

□ Enable Device HA

Configuration

☑ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:

Active Device Management IP:

Passive Device Management IP:

Subnet Mask:

Password:

Retype to Confirm:

Heartbeat Interval: 2 seconds (1-10)

Heartbeat Lost Tolerance: 2 (1-10)

Monitor Interface

Available Interfaces	Monitor Interface
=== Object === ge1 ge2 ge3 ge4	

Failover Detection

□ Enable Failover When Interface Failure (Option)

□ Enable Failover When Device Service Fails (Option)

Note:
1. Please transfer licenses in portal.myzyxel.com to the device with the serial number entered in this screen.
2. If you want to configure connectivity check, please go to Ethernet.
3. Before configure Heartbeat interface, please make sure the Heartbeat interface are not being used, such as LAG, VLAN, Bridge, and so on.

The following table describes the labels in this screen.

Table 308 Configuration > Device HA > Device HA Pro

LABEL	DESCRIPTION
Enable Device HA	Select this to turn the Zyxel Device's Device HA Pro feature on.
Enable Configuration Provisioning From Active Device.	Select this to have a passive Zyxel Device copy the active Zyxel Device's configuration, signatures (anti-malware, IDP/application patrol, botnet filter, and IP reputation), and certificates. Note: Only Zyxel Devices of the same model and firmware version can synchronize.
Serial Number of Licensed Device for License Synchronization	Type the serial number of the Zyxel Device (active or passive) with the Device HA Pro subscribed license.
Active Device Management IP	Type the IPv4 address of the highest-numbered copper Ethernet port on the active Zyxel Device (the heartbeat dedicated link port).
Passive Device Management IP	Type the IPv4 address of the highest-numbered copper Ethernet port on the passive Zyxel Device (the heartbeat dedicated link port). Note: The active and passive Zyxel Device Management IP addresses must be in the same subnet.
Subnet Mask	Type the subnet mask for the management IP addresses.

Table 308 Configuration > Device HA > Device HA Pro (continued)

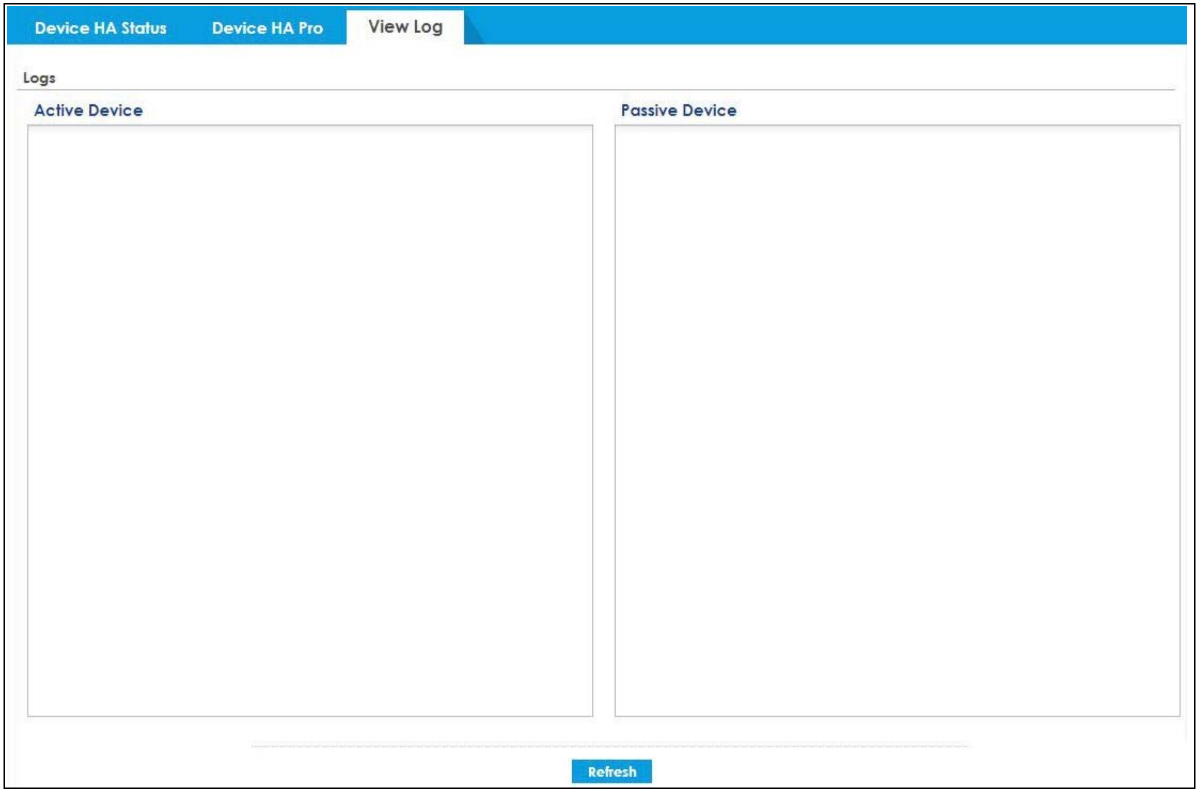
LABEL	DESCRIPTION
Password	Type a synchronization password of between 1 and 32 single-byte printable characters. You will be prompted for the password before synchronization takes place.
Retype to Confirm	Type the exact same synchronization password as typed above.
Heartbeat Interval	Type the number of seconds (1-10) allowed for absence of a heartbeat signal before a failure of the active Zyxel Device is recorded.
Heartbeat Lost Tolerance	Type the number of heartbeat failures allowed before failover is activated on the passive Zyxel Device.
Monitor Interface	Select an interface in **Available Interfaces** and click the right-arrow button to move it to **Monitor Interface** to become a Device HA pro monitored interface. To remove a Device HA pro monitored interface, select it in **Monitor Interface** and click the left-arrow button to move it to **Available Interfaces**.
Failover Detection	
Enable Failover When Interface Failure (Option)	Select this to have the passive Zyxel Device take over when a monitored interface fails.
Enable Failover When Device Service Fails (Option)	Select this to have the passive Zyxel Device take over when a monitored service daemon on the active Zyxel Device fails.
Apply	Click **Apply** to save your Device HA Pro configurations back to the Zyxel Device but keep the Zyxel Device using Device HA (general).
Reset	Click **Reset** to return the screen to its last-saved settings.

36.4 View Log

Use this screen to see Device HA Pro logs on the active and passive Zyxel Devices.

Go to **Configuration > Device HA > View Log** to display the following screen.

Figure 485 Configuration > Device HA > View Log



The following table describes the labels in this screen.

Table 309 Configuration > Device HA > View Log

LABEL	DESCRIPTION
Logs	
Active Device	This displays Device HA Pro logs on the active Zyxel Device.
Passive Device	This displays Device HA Pro logs on the passive Zyxel Device.
Refresh	Click **Refresh** to update information in this screen.

CHAPTER 37 Cloud CNM

37.1 Cloud CNM Overview

You need licenses to use Cloud CNM SecuManager and Cloud CNM SecuReporter. You need the SecuManager license to get a **CNM ID** with which you can access the SecuManager server. It is independent from the Zyxel Devices. The SecuReporter license must be activated on each Zyxel Device.

37.1.1 What You Can Do in this Chapter

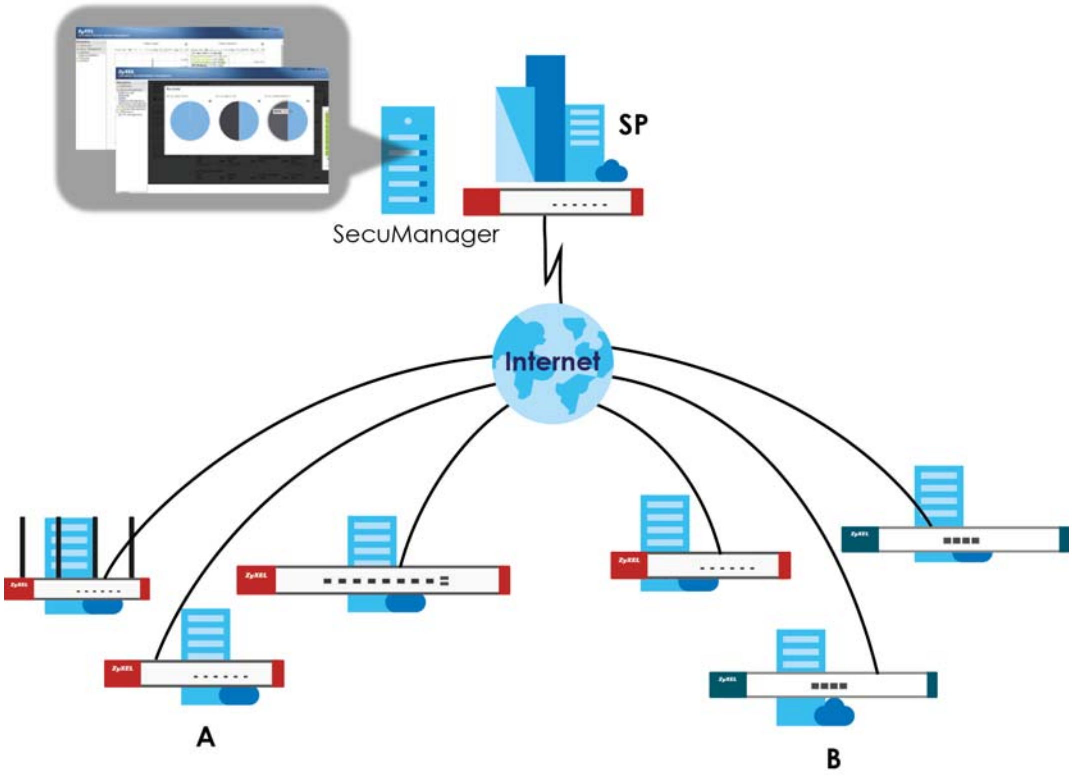
- Use the **Cloud CNM > SecuManager** screen (Section 37.2 on page 724) to enable and configure management of the Zyxel Device by a Central Network Management system.
- Use the **Cloud CNM > SecuReporter** screen (Section 37.3 on page 727) to enable SecuReporter logging on your Zyxel Device, see license status, type, expiration date and access a link to the SecuReporter web portal. The SecuReporter web portal collects and analyzes logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.

37.2 Cloud CNM SecuManager

Cloud CNM SecuManager is a Virtual Machine-based (VM) management system that uses the TR-069 protocol to encapsulate commands to ZyWALL/USG devices for management and monitoring; these devices must have firmware that supports the TR-069 protocol.

In the following figure, SP is the management service provider, while A and B are sites with devices being managed by SP.

Figure 486 Cloud CNM SecuManager Example Network Topology



Cloud CNM SecuManager features include:

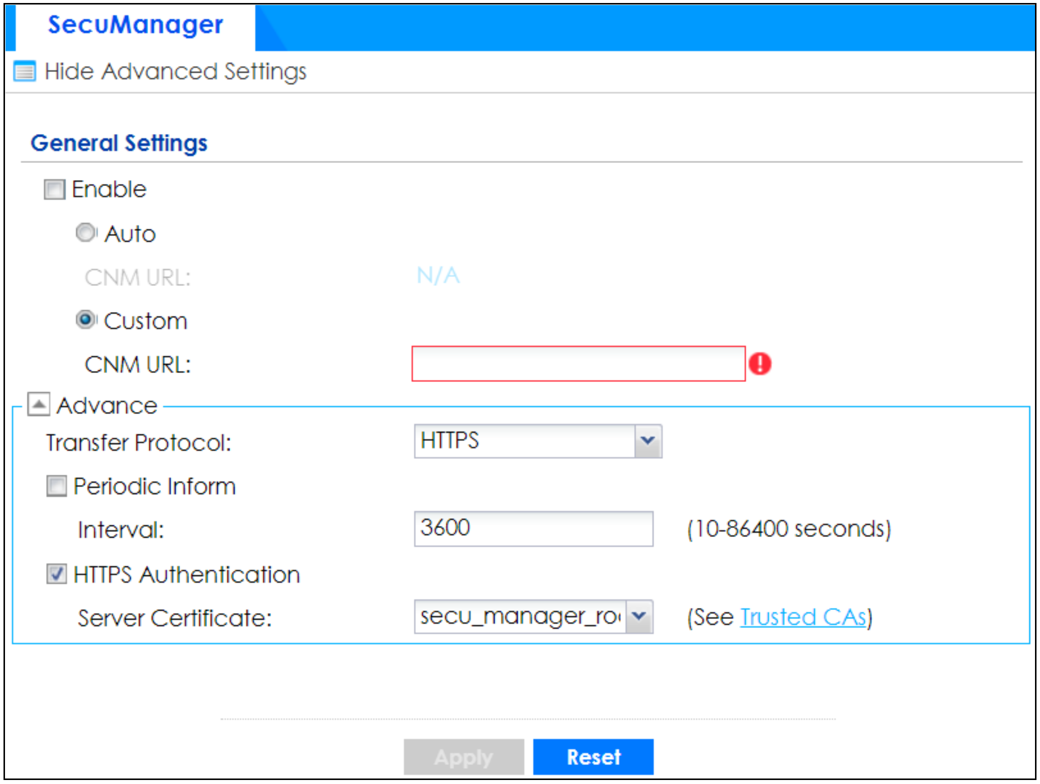
- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Backup and restore device configuration
- View the location of managed devices on a map
- Receive notification for events and alarms, such as when a device goes down
- Graphically monitor individual devices and see related statistics
- Directly access a device for remote configuration
- Create four types of administrators with different privileges
- Perform Site-to-Site, Hub & Spoke, Fully-meshed and Remote Access VPN provisioning.

To allow Cloud CNM SecuManager management of your Zyxel Device:

- You must have a Cloud CNM SecuManager license with CNM ID number or a Cloud CNM SecuManager server URL.
- The Zyxel Device must be able to communicate with the Cloud CNM SecuManager server.

You must configure **Configuration > Cloud CNM > SecuManager** to allow the Zyxel Device to find the Cloud CNM SecuManager server.

Figure 487 Configuration > Cloud CNM > SecuManager



SecuManager

Hide Advanced Settings

General Settings

☐ Enable

○ Auto

CNM URL: N/A

● Custom

CNM URL:

Advance

Transfer Protocol: HTTPS

☐ Periodic Inform

Interval: 3600 (10-86400 seconds)

☑ HTTPS Authentication

Server Certificate: secu_manager_ro (See Trusted CAs)

Apply Reset

The following table describes the labels in this screen.

Table 310 Configuration > Cloud CNM > SecuManager

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable	Select this to allow management of the Zyxel Device by Cloud CNM SecuManager.
Auto	Select this if your Cloud CNM SecuManager server can access myZyxel to automatically get the VM server URL from myZyxel. You also need **CNM ID** from the Cloud CNM SecuManager license.
CNM URL	myZyxel associates the **CNM ID** with the **CNM URL** which identifies the server on which Cloud CNM SecuManager is installed. Therefore you don't need to enter the CNM URL when you select **Auto**.
Custom	Select this if your Cloud CNM SecuManager server cannot access myZyxel.
CNM URL	Select this if your VM server or Zyxel Device are in a private network, or if the VM server is behind a NAT router. You then need to manually enter the VM server URL into the Zyxel Device. Enter the IPv4 IP address of the Cloud CNM SecuManager server followed by the port number (default 7547 for HTTPS or 7549 for HTTP) followed by the **CNM ID** from the license in **CNM URL**. For example, if you installed Cloud CNM SecuManager on a server with IP address 1.1.1.1 and **CNM ID** V6ABQNTPYGD, then type `1.1.1.1:7547/V6ABQNTPYG` or `1.1.1.1:7549/V6ABQNTPYG` as the **CNM URL**.
Transfer Protocol	Choose the CNM URL protocol: **HTTP** or **HTTPS**. If you enter 1.1.1.1:7547 as the **CNM URL**, you must choose **HTTPS** as the **Transfer Protocol**, and then the whole CNM URL is https://1.1.1.1:7547. If you enter 1.1.1.1:7549 as the **CNM URL**, you must choose **HTTP** as the **Transfer Protocol**, and then the whole CNM URL is http://1.1.1.1:7549.
Periodic Inform	Enable this to have the Zyxel Device inform the Cloud CNM SecuManager server of its presence at regular intervals.

Table 310 Configuration > Cloud CNM > SecuManager (continued)

LABEL	DESCRIPTION
Interval	Type how often the Zyxel Device should inform Cloud CNM SecuManager server of its presence.
HTTPS Authentication	Select the check box if you have a HTTPs server certificate.
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

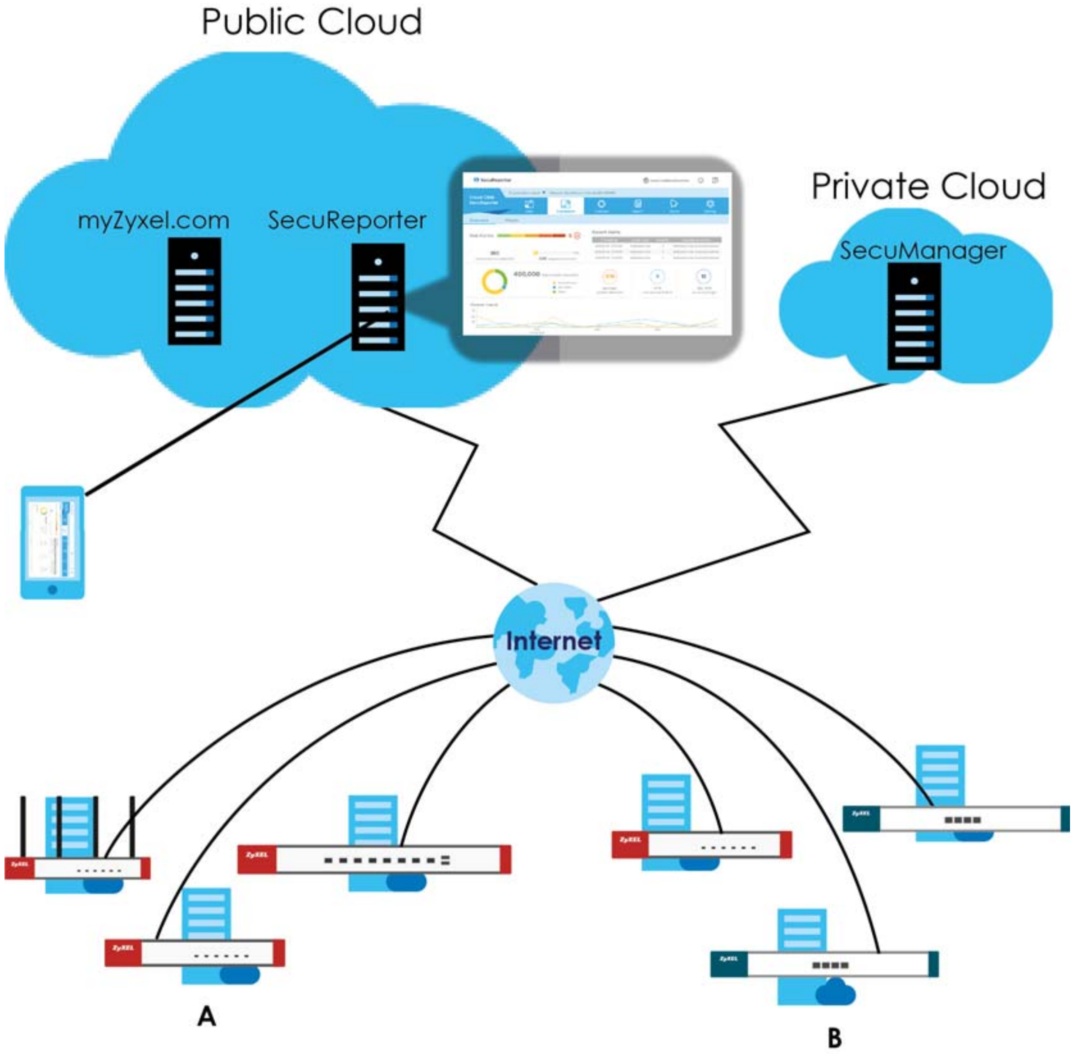
Note: See the Cloud CNM SecuManager User's Guide for more information on Cloud CNM SecuManager.

37.3 Cloud CNM SecuReporter

Cloud CNM SecuReporter is a security analytics portal that collects and analyzes logs from SecuReporter-licensed Zyxel Devices in order to identify anomalies, alert on potential internal / external threats, and report on network usage. You need to buy a license for SecuReporter for your Zyxel Device and register it at myZyxel. You must be a registered user at myZyxel.

You can access the portal from a web browser and also get notifications sent to an app on your mobile phone.

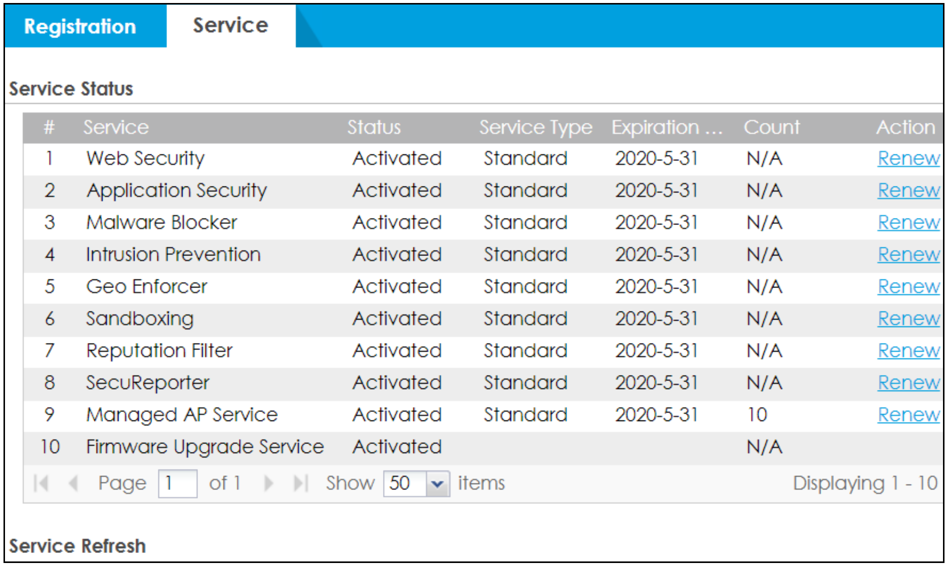
Figure 488 Cloud CNM SecuReporter Application Scenario



How to activate and enable SecuReporter

1 Does **Service Status** displays **Activated** in the **Configuration** > **Cloud CNM** > **SecuReporter** screen? If not, you have to log in to myZyxel.com and activate the SecuReporter license for this Zyxel Device. The Zyxel Device must be able to communicate with the myZyxel server.
Your SecuReporter license displays in **Configuration > Licensing > Registration > Service** after you activate the SecuReporter license at myZyxel.

Figure 489 Configuration > Licensing > Registration > Service



Service Status

#	Service	Status	Service Type	Expiration ...	Count	Action
1	Web Security	Activated	Standard	2020-5-31	N/A	Renew
2	Application Security	Activated	Standard	2020-5-31	N/A	Renew
3	Malware Blocker	Activated	Standard	2020-5-31	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2020-5-31	N/A	Renew
5	Geo Enforcer	Activated	Standard	2020-5-31	N/A	Renew
6	Sandboxing	Activated	Standard	2020-5-31	N/A	Renew
7	Reputation Filter	Activated	Standard	2020-5-31	N/A	Renew
8	SecuReporter	Activated	Standard	2020-5-31	N/A	Renew
9	Managed AP Service	Activated	Standard	2020-5-31	10	Renew
10	Firmware Upgrade Service	Activated			N/A	

Service Refresh

2 After the SecuReporter license is activated, go back to the **Configuration** > **Cloud CNM** > **SecuReporter** screen, and select the categories of logs that you want this Zyxel Device to send to the SecuReporter portal.

3 Select **Enable SecuReporter**. Do not go to the SecuReporter portal until after you have enabled SecuReporter on this Zyxel Devicee and applied the settings.
You can also see license status, type, expiration date.

4 Click **Apply** and wait.

How to add this Zyxel Device to SecuReporter

1 Log in to the SecuReporter portal.

2 Go to **Settings** > **Organization & Devices** > **Add** to create an organization.

3 Add this Zyxel Device to an **Organization** using the hyper link under **Unclaimed Device**.

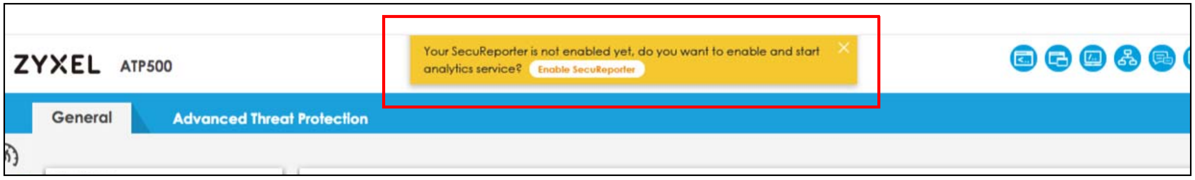
SecuReporter Banner

The SecuReporter banner appears when:

1 SecuReporter hasn’t been enabled before.

2 The Zyxel Device is not added to an organization yet.

Figure 490 SecuReporter Banner

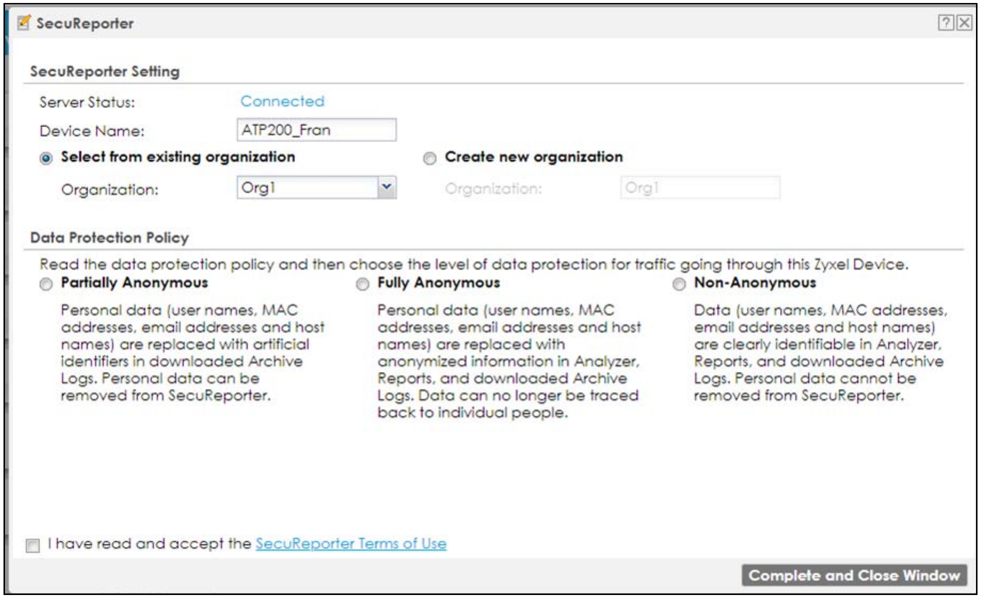


Your SecuReporter is not enabled yet, do you want to enable and start analytics service?

Click the **Continue** button in the SecuReporter banner to configure the SecuReporter settings.

- **Server Status**: This is the connection status between the Zyxel Device and the SecuReporter server. This field shows **Connected** when the Zyxel Device can synchronize with the SecuReporter server. This field shows **Timeout** when the Zyxel Device can't synchronize with the SecuReporter server. This field shows **Fail** when the connection between the Zyxel Device and the SecuReporter server is down.
- **Device Name**: Enter the name of the Zyxel Device. This Zyxel Device will be added to a new or existing organization.
- **Organization**: This field appears if you haven't created an organization in the SecuReporter server. Type a name of up to 255 characters and description to create a new organization.
- **Select from existing organization**: Select an existing organization from the drop-down list box to add the Zyxel Device to the selected organization.
- **Create new organization**: Type a name of up to 255 characters and description to create a new organization.
- **Partially Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be replaced with artificial identifiers in downloaded logs.
- **Fully Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be replaced with anonymized information in downloaded logs.
- **Non-Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be identifiable in downloaded logs.

Figure 491 SecuReporter Banner Settings



SecuReporter Setting

Server Status: Connected

Device Name: ATP200_Fran

● Select from existing organization ○ Create new organization

Organization: Org1 Organization: Org1

Data Protection Policy

Read the data protection policy and then choose the level of data protection for traffic going through this Zyxel Device.

○ **Partially Anonymous**

Personal data (user names, MAC addresses, email addresses and host names) are replaced with artificial identifiers in downloaded Archive Logs. Personal data can be removed from SecuReporter.

○ **Fully Anonymous**

Personal data (user names, MAC addresses, email addresses and host names) are replaced with anonymized information in Analyzer, Reports, and downloaded Archive Logs. Data can no longer be traced back to individual people.

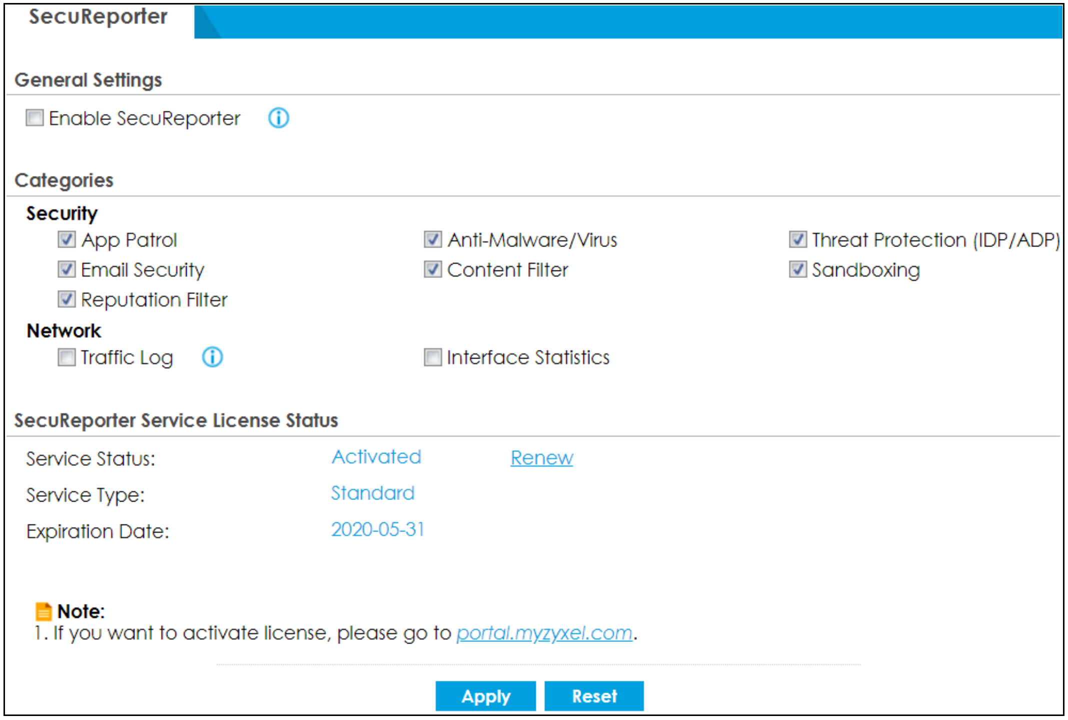
○ **Non-Anonymous**

Data (user names, MAC addresses, email addresses and host names) are clearly identifiable in Analyzer, Reports, and downloaded Archive Logs. Personal data cannot be removed from SecuReporter.

□ I have read and accept the SecuReporter Terms of Use

Click **Configuration** > **Cloud CNM** > **SecuReporter** to open the following screen.

Figure 492 Configuration > Cloud CNM > SecuReporter



SecuReporter

General Settings

□ Enable SecuReporter ⓘ

Categories

Security

☑ App Patrol ☑ Anti-Malware/Virus ☑ Threat Protection (IDP/ADP)

☑ Email Security ☑ Content Filter ☑ Sandboxing

☑ Reputation Filter

Network

□ Traffic Log ⓘ □ Interface Statistics

SecuReporter Service License Status

Service Status: Activated Renew

Service Type: Standard

Expiration Date: 2020-05-31

Note:
1. If you want to activate license, please go to portal.myzyxel.com.

The following table describes the labels in this screen.

Table 311 Configuration > Cloud CNM > SecuReporter

LABEL	DESCRIPTION
Enable SecuReporter	Security-related logs are sent to the SecuReporter portal. Click the General Data Protection Regulation (GDPR) privacy link below to see the Zyxel privacy policy. This must be selected to have SecuReporter collect and analyze logs from this Zyxel Device. • It's selected by default if you have activated a SecuReporter **Standard** license, • You need to select this if you have a SecuReporter **Trial** license. • This field is not available if you do not have a SecuReporter license.
Categories	Select the categories of logs that you want this Zyxel Device to send to SecuReporter for analysis and trend spotting.
SecuReporter Service License Status	
Service Status	This field displays whether a service license is enabled at myZyxel (**Activated**) or not (**Not Activated**) or expired (**Expired**). It displays the remaining Grace Period if your license has **Expired**. It displays **Not Licensed** if there isn't a license to be activated for this service.
Service Type	This field displays whether you applied for a trial application (**Trial**) or registered this service with your iCard's PIN number (**Standard**). This field is blank when the service is not activated.
Expiration Date	This field displays the date your service expires.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 38
System

38.1 Overview

Use the system screens to configure general Zyxel Device settings.

38.1.1 What You Can Do in this Chapter

- Use the **System > Host Name** screen (see Section 38.2 on page 733) to configure a unique name for the Zyxel Device in your network.
- Use the **System > USB Storage** screen (see Section 38.3 on page 733) to configure the settings for the connected USB devices.
- Use the **System > Date/Time** screen (see Section 38.4 on page 734) to configure the date and time for the Zyxel Device.
- Use the **System > Console Speed** screen (see Section 38.5 on page 738) to configure the console port speed when you connect to the Zyxel Device via the console port using a terminal emulation program.
- Use the **System > DNS** screen (see Section 38.6 on page 739) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the **System > WWW** screens (see Section 38.7 on page 749) to configure settings for HTTP or HTTPS access to the Zyxel Device and how the login and access user screens look.
- Use the **System > SSH** screen (see Section 38.8 on page 766) to configure SSH (Secure SHell) used to securely access the Zyxel Device's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the **System > TELNET** screen (see Section 38.9 on page 771) to configure Telnet to access the Zyxel Device's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the **System > FTP** screen (see Section 38.10 on page 773) to specify from which zones FTP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come. You can upload and download the Zyxel Device's firmware and configuration files using FTP.
- Your Zyxel Device can act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Use the **System > SNMP** screen (see Section 38.11 on page 775) to configure SNMP settings, including from which zones SNMP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.
- Use the **Auth. Server** screen (Section 38.12 on page 781) to configure the Zyxel Device to operate as a RADIUS server.
- Use the **Notification > Mail Server** screen (Section 38.13 on page 783) to configure the Zyxel Device to operate as a RADIUS server.
- Use the **Notification > SMS** screen (Section 38.14 on page 785) to turn on the SMS service on the Zyxel Device in order to send dynamic guest account information in text messages and authorization for VPN tunnel access to a secured network.
- Use the **System > Language** screen (see Section 38.15 on page 786) to set a language for the Zyxel Device's Web Configurator screens.

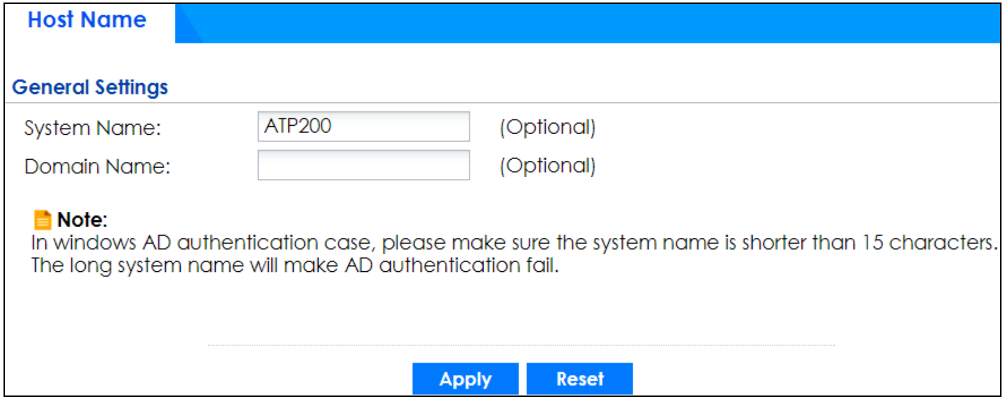
- Use the **System > IPv6** screen (see Section 38.16 on page 787) to enable or disable IPv6 support on the Zyxel Device.
- Use the **System > ZON** screen (see Section 38.17 on page 787) to enable or disable the Zyxel One Network (ZON) utility that uses Zyxel Discovery Protocol (ZDP) for discovering and configuring ZDP-aware Zyxel devices in the same network as the computer on which ZON is installed.

Note: See each section for related background information and term definitions.

38.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open the **Host Name** screen.

Figure 493 Configuration > System > Host Name



System Name: ATP200 (Optional)

Domain Name: (Optional)

Note:
In windows AD authentication case, please make sure the system name is shorter than 15 characters. The long system name will make AD authentication fail.

The following table describes the labels in this screen.

Table 312 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Enter a descriptive name to identify your Zyxel Device device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

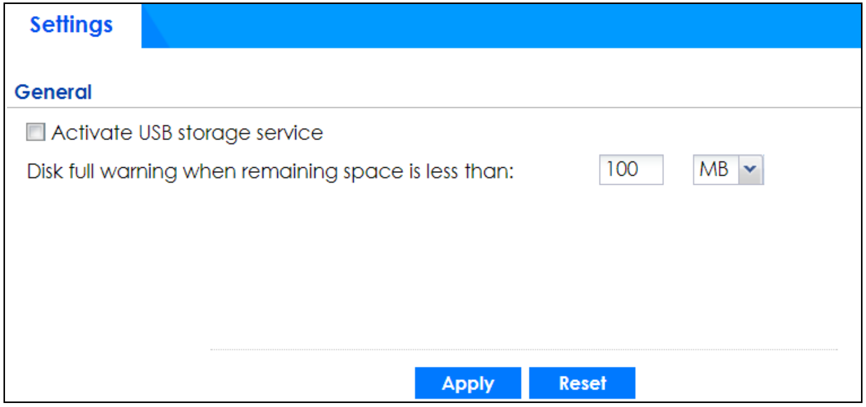
38.3 USB Storage

The Zyxel Device can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

Click **Configuration > System > USB Storage** to open the screen as shown next.

Figure 494 Configuration > System > USB Storage



☐ Activate USB storage service

Disk full warning when remaining space is less than: 100 MB

The following table describes the labels in this screen.

Table 313 Configuration > System > USB Storage

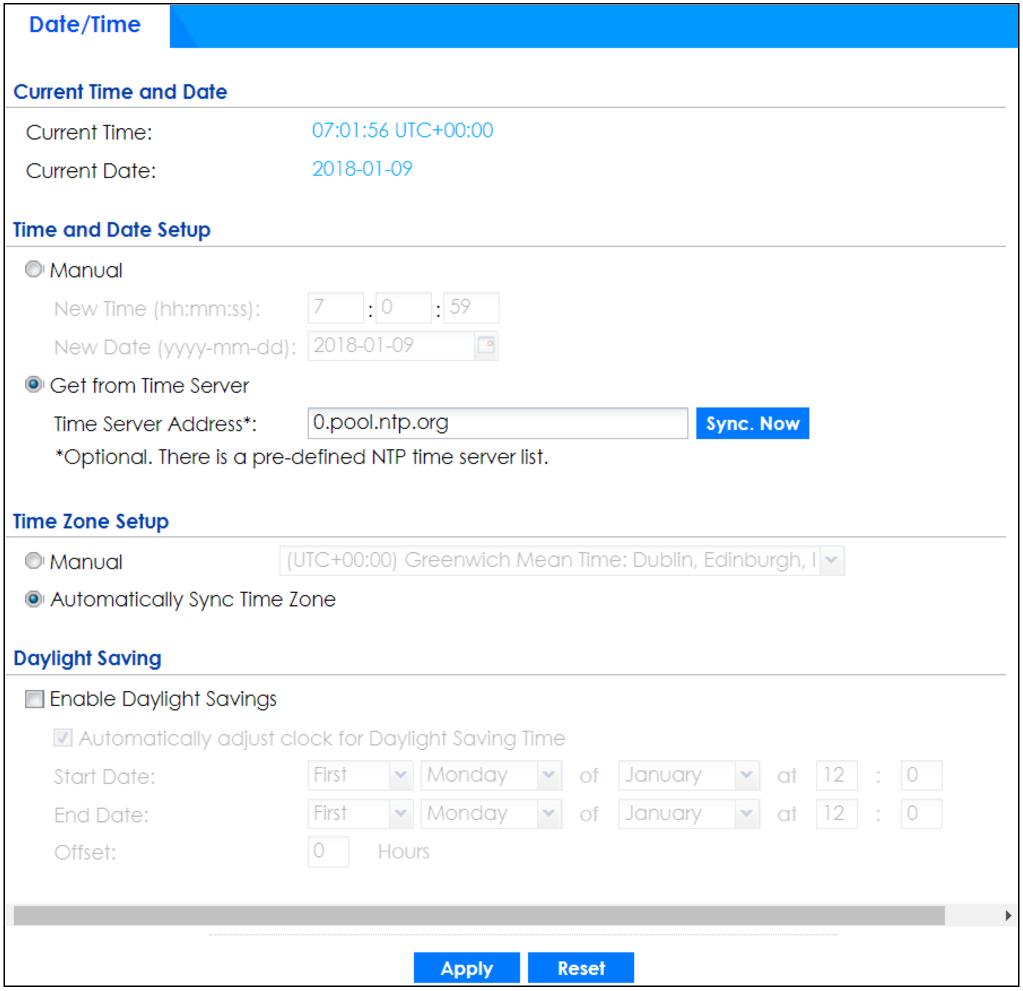
LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (**MB** or **%**) to have the Zyxel Device send a warning message when the remaining USB storage space is less than the value you set here.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.4 Date and Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. The Zyxel Device's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your Zyxel Device's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the Zyxel Device's time and date or have the Zyxel Device get the date and time from a time server.

Figure 495 Configuration > System > Date and Time



Date/Time

Current Time and Date

Current Time: 07:01:56 UTC+00:00

Current Date: 2018-01-09

Time and Date Setup

○ Manual

New Time (hh:mm:ss): 7 : 0 : 59

New Date (yyyy-mm-dd): 2018-01-09

● Get from Time Server

Time Server Address*: 0.pool.ntp.org Sync. Now

*Optional. There is a pre-defined NTP time server list.

Time Zone Setup

○ Manual (UTC+00:00) Greenwich Mean Time: Dublin, Edinburgh, l

● Automatically Sync Time Zone

Daylight Saving

□ Enable Daylight Savings

☑ Automatically adjust clock for Daylight Saving Time

Start Date: First Monday of January at 12 : 0

End Date: First Monday of January at 12 : 0

Offset: 0 Hours

The following table describes the labels in this screen.

Table 314 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your Zyxel Device.
Current Date	This field displays the present date of your Zyxel Device.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the Zyxel Device uses the new setting once you click **Apply**.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.

Table 314   Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the Zyxel Device get the time and date from the time server you specify below. The Zyxel Device requests time and date settings from the time server under the following circumstances. • When the Zyxel Device starts up. • When you click **Apply** or **Synchronize Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Automatically Sync Time Zone	Select this for the Zyxel Device to automatically get its time zone.
Daylight Saving	
Enable Daylight Savings	Daylight savings 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. Select this option if you use Daylight Saving Time.
Automatically adjust clock for Daylight Saving Time	Select this for the Zyxel Device to automatically adjust the time if daylight savings is implemented in its time zone.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 314 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.4.1 Pre-defined NTP Time Servers List

When you turn on the Zyxel Device for the first time, the date and time start at 2003-01-01 00:00:00. The Zyxel Device then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The Zyxel Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 315 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

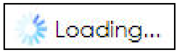
When the Zyxel Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Zyxel Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

38.4.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading** screen appears, you may have to wait up to one minute.

Figure 496 Synchronization in Process



Loading...

The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the Zyxel Device date and time.

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the Zyxel Device's time in the **New Time** field.

4 Enter the Zyxel Device's date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** check box to adjust the Zyxel Device clock for daylight savings.

7 Click **Apply**.

To get the Zyxel Device date and time from a time server

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

4 As an option you can select the **Enable Daylight Saving** check box to adjust the Zyxel Device clock for daylight savings.

5 Under **Time and Date Setup**, enter a **Time Server Address** (Table 315 on page 737).

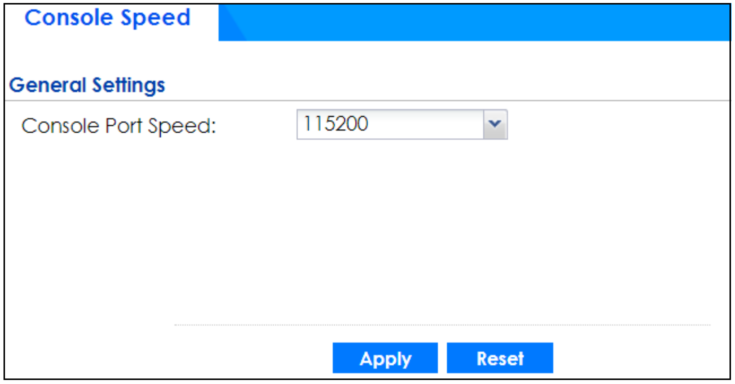
6 Click **Apply**.

38.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the Zyxel Device via the console port using a terminal emulation program.

Click **Configuration > System > Console Speed** to open the **Console Speed** screen.

Figure 497 Configuration > System > Console Speed



Console Port Speed: 115200

The following table describes the labels in this screen.

Table 316 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your Zyxel Device supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The **Console Port Speed** applies to a console port connection using terminal emulation software and NOT the **Console** in the Zyxel Device Web Configurator **Status** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

38.6.1 DNS Server Address Assignment

The Zyxel Device can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

38.6.2 Configuring the DNS Screen

Click **Configuration > System > DNS** to change your Zyxel Device's DNS settings. Use the **DNS** screen to configure the Zyxel Device to use a DNS server to resolve domain names for Zyxel Device system features like VPN, DDNS and the time server. You can also configure the Zyxel Device to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the Zyxel Device sends to the specified DHCP client devices.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The Zyxel Device can be a DNS client service. The Zyxel Device can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the Zyxel Device does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

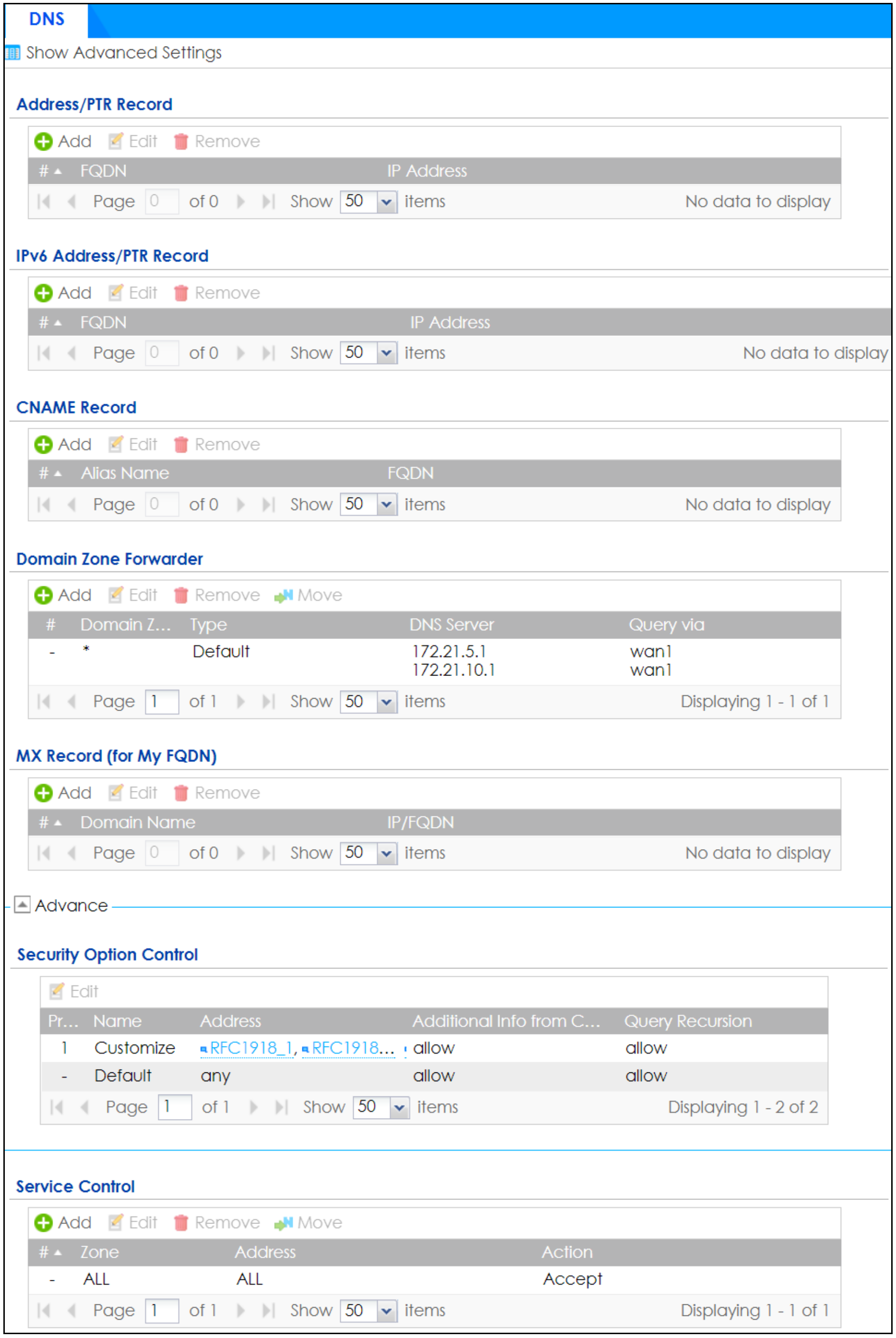
The Zyxel Device can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the Zyxel Device or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

Configure the **Security Option Control** section in the **Configuration > System > DNS** screen (click **Show Advanced Settings** to display it) if you suspect the Zyxel Device is being used (either by hackers or by a corrupted open DNS server) in a DNS amplification attack.

Figure 498 Configuration > System > DNS


DNS
Show Advanced Settings

Address/PTR Record

# ▲	FQDN	IP Address

Page 0 of 0 Show 50 items No data to display

IPv6 Address/PTR Record

# ▲	FQDN	IP Address

Page 0 of 0 Show 50 items No data to display

CNAME Record

# ▲	Alias Name	FQDN

Page 0 of 0 Show 50 items No data to display

Domain Zone Forwarder

#	Domain Z...	Type	DNS Server	Query via
-	*	Default	172.21.5.1 172.21.10.1	wan1 wan1

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

MX Record (for My FQDN)

# ▲	Domain Name	IP/FQDN

Page 0 of 0 Show 50 items No data to display
Advance

Security Option Control

Pr...	Name	Address	Additional Info from C...	Query Recursion
1	Customize	RFC1918_1, RFC1918...	allow	allow
-	Default	any	allow	allow

Service Control

# ▲	Zone	Address	Action
-	ALL	ALL	Accept

The following table describes the labels in this screen.

Table 317 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host's fully qualified domain name.
IP Address	This is the IP address of a host.
CNAME Record	This record specifies an alias for a FQDN. Use this record to bind all subdomains with the same IP address as the FQDN without having to update each one individually, which increases chance for errors. See CNAME Record (Section 38.6.6 on page 744) for more details.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The Zyxel Device uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Alias Name	Enter an Alias name. Use "*." as prefix for a wildcard domain name. For example, *.example.com.
FQDN	Enter the Fully Qualified Domain Name (FQDN).
Domain Zone Forwarder	This specifies a DNS server's IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the Zyxel Device needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The Zyxel Device uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.

Table 317   Configuration > System > DNS (continued)

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A "*" means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (**User-Defined**).
DNS Server	This is the IP address of a DNS server. This field displays **N/A** if you have the Zyxel Device get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the Zyxel Device sends DNS queries to the entry's DNS server. If the Zyxel Device connects through a VPN tunnel, **tunnel** displays.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Security Option Control	Click **Show Advanced Settings** to display this part of the screen. There are two control policies: **Default** and **Customize**.
Edit	Click either control policy and then click this button to change **allow** or **deny** actions for **Query Recursion** and **Additional Info from Cache**.
Priority	The **Customize** control policy is checked first and if an address object match is not found, the **Default** control policy is checked.
Name	You may change the name of the **Customize** control policy.
Address	These are the object addresses used in the control policy. RFC1918 refers to private IP address ranges. It can be modified in **Object > Address**.
Additional Info from Cache	This displays if the Zyxel Device is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Query Recursion	This displays if the Zyxel Device is allowed or denied to forward DNS client requests to DNS servers for resolution.
Service Control	This specifies from which computers and zones you can send DNS queries to the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.

Table 317 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the Zyxel Device accepts DNS queries from the computer with the IP address specified above through the specified zone (**Accept**) or discards them (**Deny**).

38.6.3 (IPv6) Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address.

The Zyxel Device allows you to configure address records about the Zyxel Device itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the Zyxel Device receives a DNS query for an FQDN for which the Zyxel Device has an address record, the Zyxel Device can send the IP address in a DNS response without having to query a DNS name server.

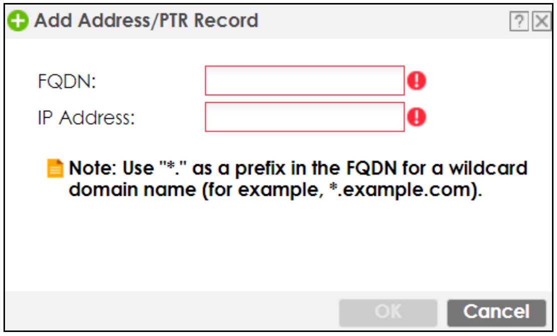
38.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

38.6.5 Adding an (IPv6) Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** or **IPv6 Address/PTR Record** table to add an IPv4 or IPv6 address/PTR record.

Figure 499 Configuration > System > DNS > Address/PTR Record Edit


Add Address/PTR Record

FQDN:

IP Address:

Note: Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).

The following table describes the labels in this screen.

Table 318 Configuration > System > DNS > (IPv6) Address/PTR Record Edit

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.6.6 CNAME Record

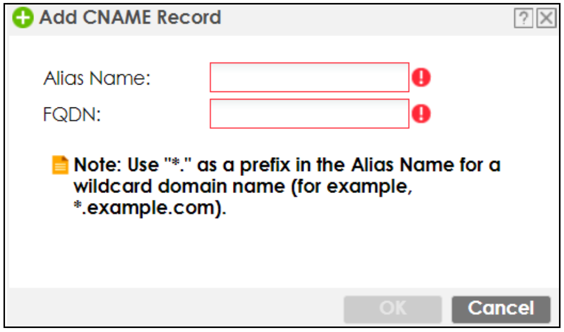
A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain name is an alias of another. This record also binds all the subdomains to the same IP address without having to create a record for each, so when the IP address is changed, all subdomain's IP address is updated as well, with one edit to the record.

For example, the domain name zyxel.com is hooked up to a record named A which translates it to 11.22.33.44. You also have several subdomains, like mail.zyxel.com, ftp.zyxel.com and you want this subdomain to point to your main domain zyxel.com. Edit the IP Address in record A and all subdomains will follow automatically. This eliminates chances for errors and increases efficiency in DNS management.

38.6.7 Adding a CNAME Record

Click the Add icon in the CNAME Record table to add a record. Use "*." as a prefix for a wildcard domain name. For example *.zyxel.com.

Figure 500 Configuration > System > DNS > CNAME Record > Add



Add CNAME Record

Alias Name:

FQDN:

Note: Use "*." as a prefix in the Alias Name for a wildcard domain name (for example, *.example.com).

The following table describes the labels in this screen.

Table 319 Configuration > System > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Alias name	Enter an Alias Name. Use "*." as a prefix in the Alias name for a wildcard domain name (for example, *.example.com).
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

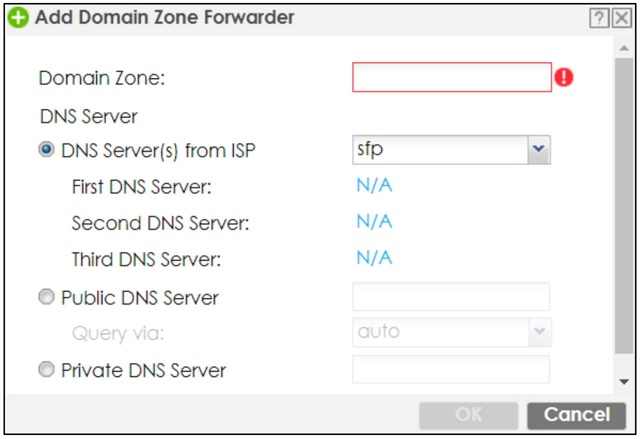
38.6.8 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

38.6.9 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

Figure 501 Configuration > System > DNS > Domain Zone Forwarder Add



Add Domain Zone Forwarder

Domain Zone:

DNS Server

● DNS Server(s) from ISP: sfp

First DNS Server: N/A

Second DNS Server: N/A

Third DNS Server: N/A

○ Public DNS Server

Query via: auto

○ Private DNS Server

The following table describes the labels in this screen.

Table 320 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the Zyxel Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select **DNS Server(s) from ISP** if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select **Public DNS Server** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The Zyxel Device must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the Zyxel Device’s local networks. You cannot use 0.0.0.0. Use the **Query via** field to select the interface through which the Zyxel Device sends DNS queries to a DNS server. Select **Private DNS Server** if you have the IP address of a DNS server to which the Zyxel Device connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

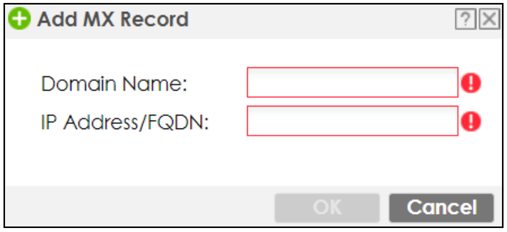
38.6.10 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external email from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

38.6.11 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 502 Configuration > System > DNS > MX Record Add



The following table describes the labels in this screen.

Table 321 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.6.12 Security Option Control

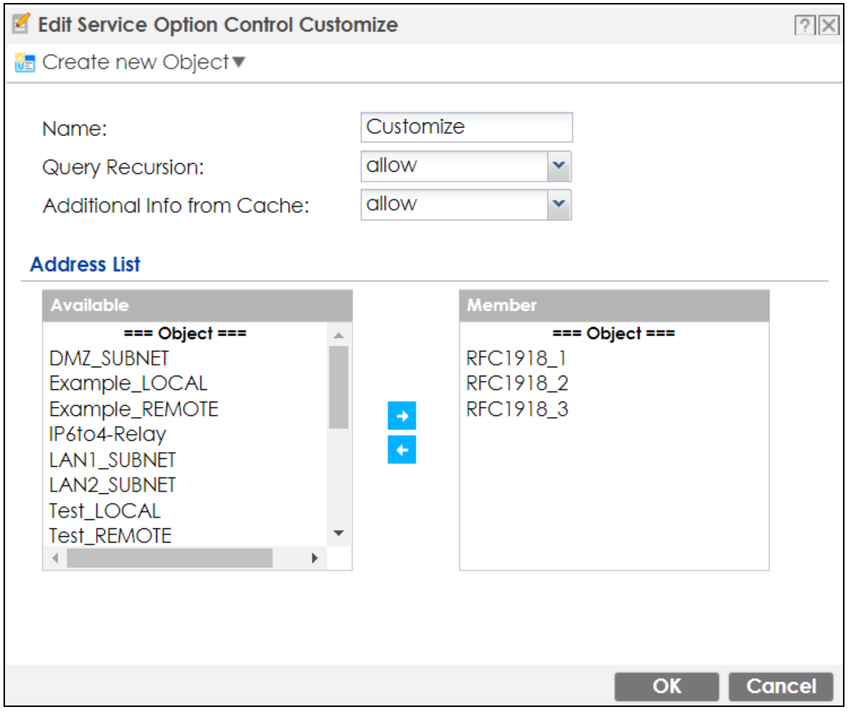
Configure the **Security Option Control** section in the **Configuration > System > DNS** screen (click **Show Advanced Settings** to display it) if you suspect the Zyxel Device is being used by hackers in a DNS amplification attack.

One possible strategy would be to deny **Query Recursion** and **Additional Info from Cache** in the default policy and allow **Query Recursion** and **Additional Info from Cache** only from trusted DNS servers identified by address objects and added as members in the customized policy.

38.6.13 Editing a Security Option Control

Click a control policy and then click **Edit** to change **allow** or **deny** actions for **Query Recursion** and **Additional Info from Cache**.

Figure 503 Configuration > System > DNS > Security Option Control Edit (Customize)



Edit Service Option Control Customize

Create new Object▼

Name: Customize

Query Recursion: allow

Additional Info from Cache: allow

Address List

Available	Member
=== Object ===	=== Object ===
DMZ_SUBNET	RFC1918_1
Example_LOCAL	RFC1918_2
Example_REMOTE	RFC1918_3
IP6to4-Relay	
LAN1_SUBNET	
LAN2_SUBNET	
Test_LOCAL	
Test_REMOTE	

The following table describes the labels in this screen.

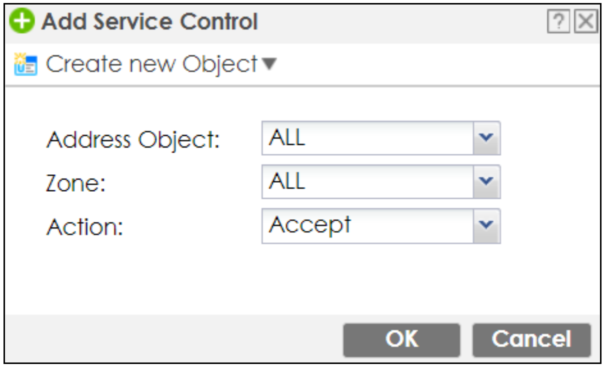
Table 322 Configuration > System > DNS > Security Option Control Edit (Customize)

LABEL	DESCRIPTION
Name	You may change the name for the customized security option control policy. The customized security option control policy is checked first and if an address object match is not found, the **Default** control policy is checked.
Query Recursion	Choose if the ZyWALL/USG is allowed or denied to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule.
Additional Info from Cache	Choose if the ZyWALL/USG is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Address List	Specifying address objects is not available in the default policy as all addresses are included.
Available	This box displays address objects created in **Object > Address**. Select one (or more), and click the **>** arrow to have it (them) join the **Member** list of address objects that will apply to this rule. For example, you could specify an open DNS server suspect of sending compromised resource records by adding an address object for that server to the member list.
Member	This box displays address objects that will apply to this rule.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.6.14 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

Figure 504 Configuration > System > DNS > Service Control Rule Add



Add Service Control

Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

Table 323 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to send DNS queries to the Zyxel Device. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the Zyxel Device.
Zone	Select **ALL** to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the Zyxel Device is allowed or denied.

Table 323 Configuration > System > DNS > Service Control Rule Add (continued)

LABEL	DESCRIPTION
Action	Select **Accept** to have the Zyxel Device allow the DNS queries from the specified computer. Select **Deny** to have the Zyxel Device reject the DNS queries from the specified computer.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.7 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Note: To allow the Zyxel Device to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-Zyxel Device security policy rule to block that traffic.

To stop a service from accessing the Zyxel Device, clear **Enable** in the corresponding service screen.

38.7.1 Service Access Limitations

A service cannot be used to access the Zyxel Device when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the Zyxel Device disallows the session).
3. The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
4. There is a security policy rule that blocks it.

38.7.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User/Group** screens.

38.7.3 HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

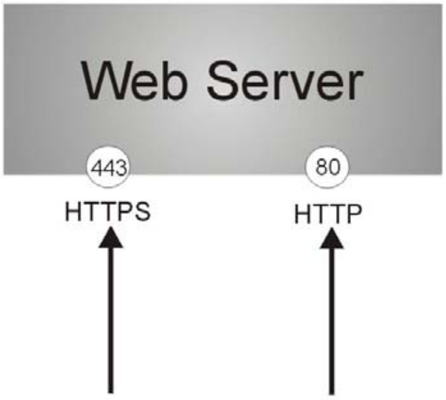
HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the Zyxel Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Zyxel Device.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Zyxel Device's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the Zyxel Device's web server.

Figure 505 HTTP/HTTPS Implementation



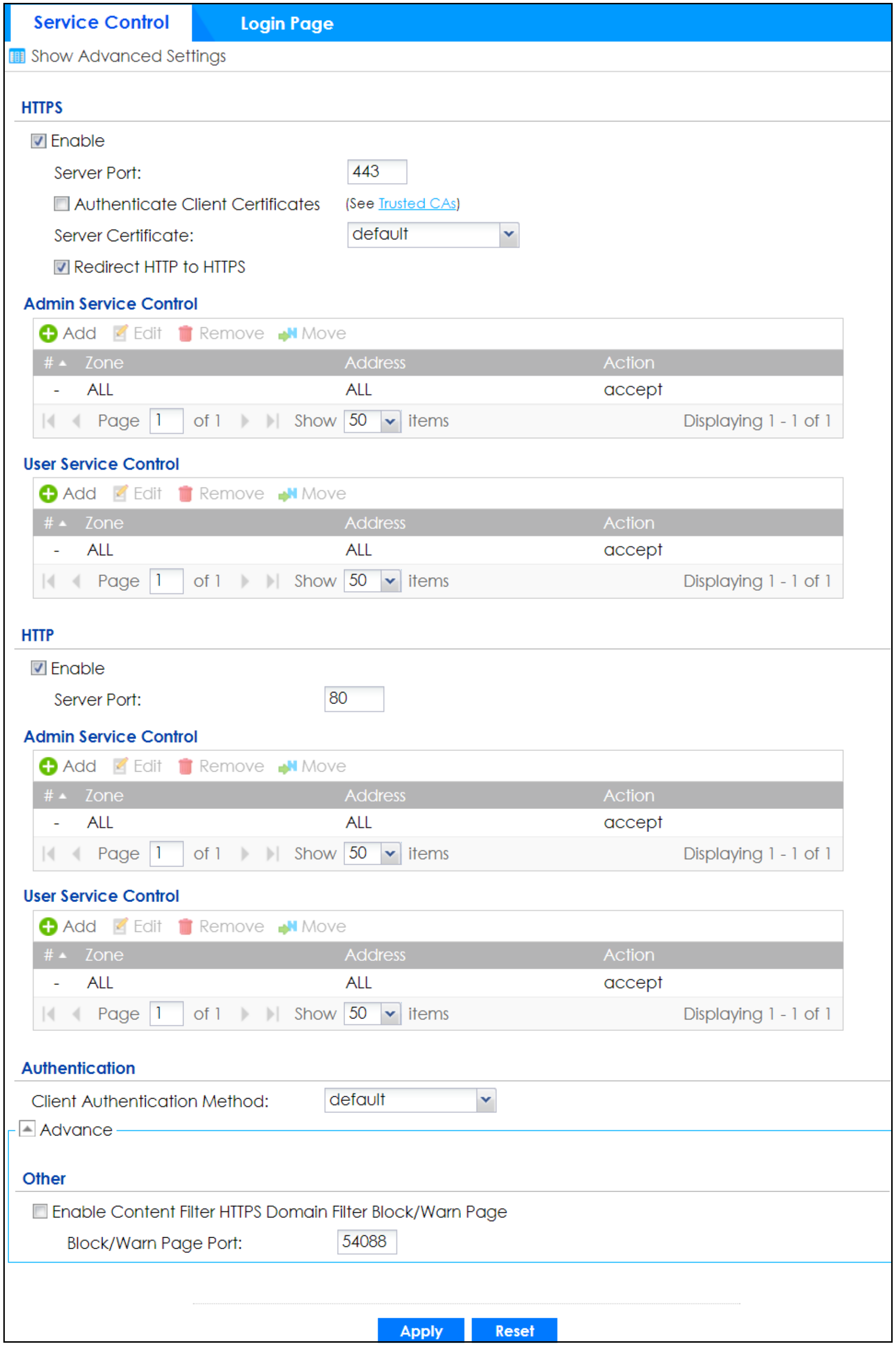
Note: If you disable **HTTP** in the **WWW** screen, then the Zyxel Device blocks all HTTP connection attempts.

38.7.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the Zyxel Device using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: **Admin Service Control** deals with management access (to the Web Configurator). **User Service Control** deals with user access to the Zyxel Device (logging into SSL VPN for example).

Figure 506 Configuration > System > WWW > Service Control



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

# ▲	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

User Service Control

# ▲	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

HTTP

☑ Enable

Server Port: 80

Admin Service Control

# ▲	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

User Service Control

# ▲	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Authentication

Client Authentication Method: default

Other

☐ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port: 54088

The following table describes the labels in this screen.

Table 324 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using secure HTTPs connections.

Table 324 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use "https://Zyxel Device IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the Zyxel Device by sending the Zyxel Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device (see Section 38.7.7.5 on page 761 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTPS to manage the Zyxel Device (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the Zyxel Device. **User Service Control** specifies from which zones a user can use HTTPS to log into the Zyxel Device (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the Zyxel Device.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTP to manage the Zyxel Device (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the Zyxel Device. **User Service Control** specifies from which zones a user can use HTTP to log into the Zyxel Device (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

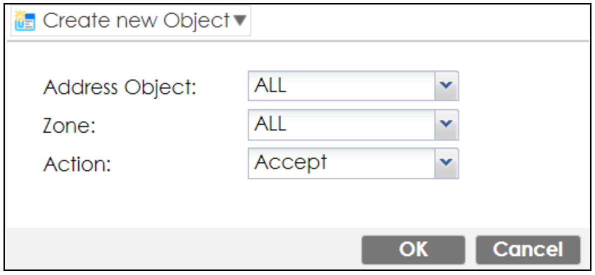
Table 324 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the **Auth. method** screen.
Other	When HTTPS Domain Filter blocks a page, the connection is redirected to a local web server to display the blocking message. HSTS (HTTP Strict Transport Security) may be activated in some browsers as the browser cached certificate is different to the one displayed by the local server. In this case, you cannot see a blocking warning message. Accessing a web page may require multiple connections to different sites to get all the information in the web page. When there is a connection to a HTTPS website that belongs to a blocked category, it is filtered, but you don't receive a warning page with the option to continue. For example, you want to block www.google.com and issue a **Warn** action. When you connect to www.google.com another connection to pic.google.com is created to get the pictures on the Google page. www.google.com can display a warning page in your browser (and you can click 'Continue' to forward the connection) but the connection to pic.google.com cannot display a 'Continue' dialog, so parts of the Google page will appear blank and will not display the related picture content.
Enable Content Filter HTTPS Domain Filter Block/Warn Page	Use this field to have the Zyxel Device display a warning page instead of a blank page when an HTPPS connection is redirected.
Block/Warn Page Port	Use the default port number as displayed for the warning page. If you change it, the new port number should be unique.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.7.5 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

Figure 507 Configuration > System > Service Control Rule > Edit



Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

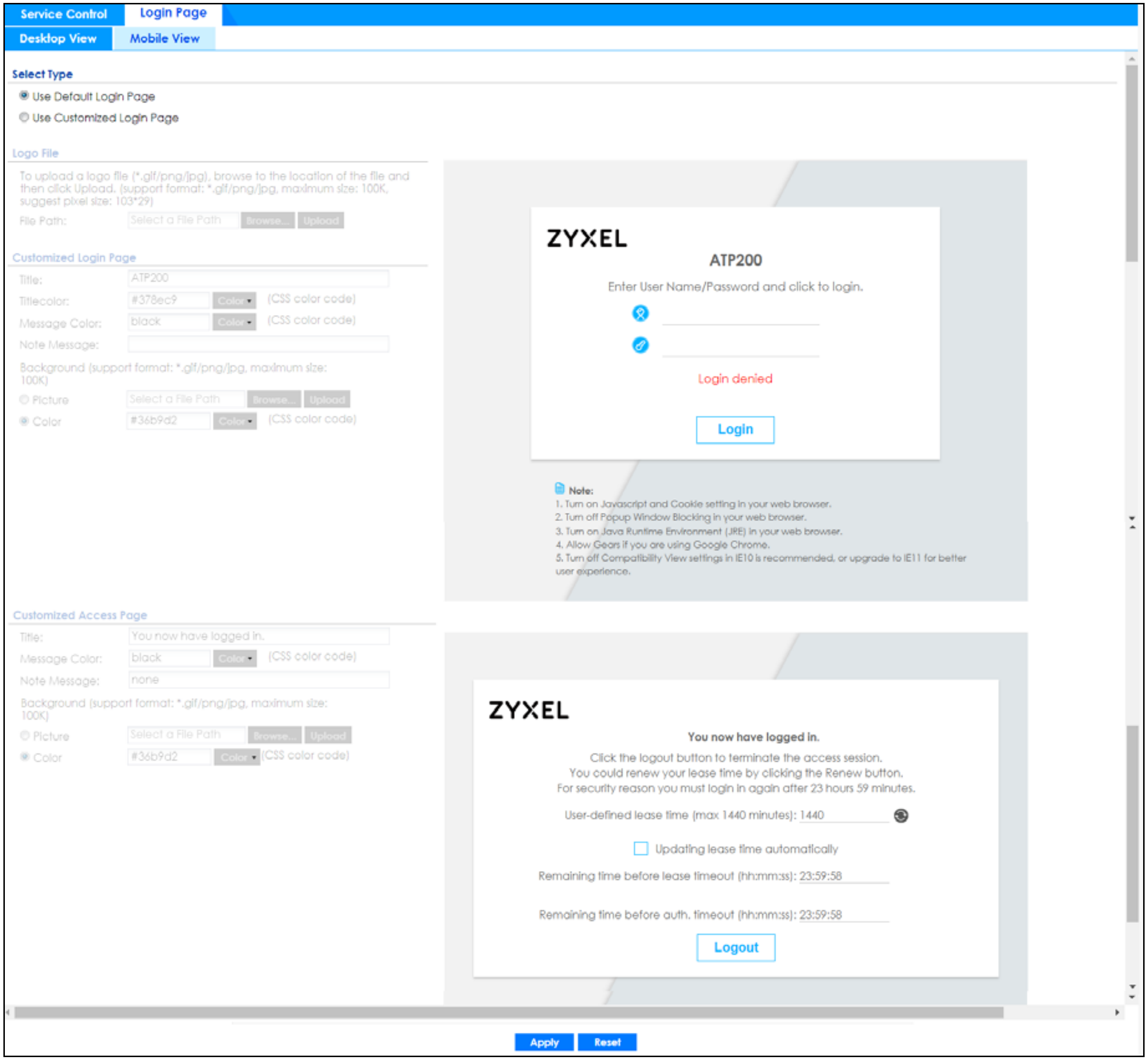
Table 325 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the Zyxel Device using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using this service.
Zone	Select **ALL** to allow or prevent any Zyxel Device zones from being accessed using this service. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the Zyxel Device from the specified computers. Select **Deny** to block the user's access to the Zyxel Device from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.7.6 Customizing the WWW Login Page

Click **Configuration > System > WWW > Login Page** to open the **Login Page** screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.

Figure 508 Configuration > System > WWW > Login Page (Desktop View)



Select Type

● Use Default Login Page

○ Use Customized Login Page

Logo File

To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload. (support format: *.gif/png/jpg, maximum size: 100K, suggest pixel size: 103*29)

File Path: Select a File Path Browse... Upload

Customized Login Page

Title: ATP200

Titlecolor: #378ec9 Color (CSS color code)

Message Color: black Color (CSS color code)

Note Message:

Background (support format: *.gif/png/jpg, maximum size: 100K)

○ Picture Select a File Path Browse... Upload

● Color #36b9d2 Color (CSS color code)

ZYXEL

ATP200

Enter User Name/Password and click to login.

Login denied

Login

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.
5. Turn off Compatibility View settings in IE10 is recommended, or upgrade to IE11 for better user experience.

Customized Access Page

Title: You now have logged in.

Message Color: black Color (CSS color code)

Note Message: none

Background (support format: *.gif/png/jpg, maximum size: 100K)

○ Picture Select a File Path Browse... Upload

● Color #36b9d2 Color (CSS color code)

ZYXEL

You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 23 hours 59 minutes.

User-defined lease time (max 1440 minutes): 1440

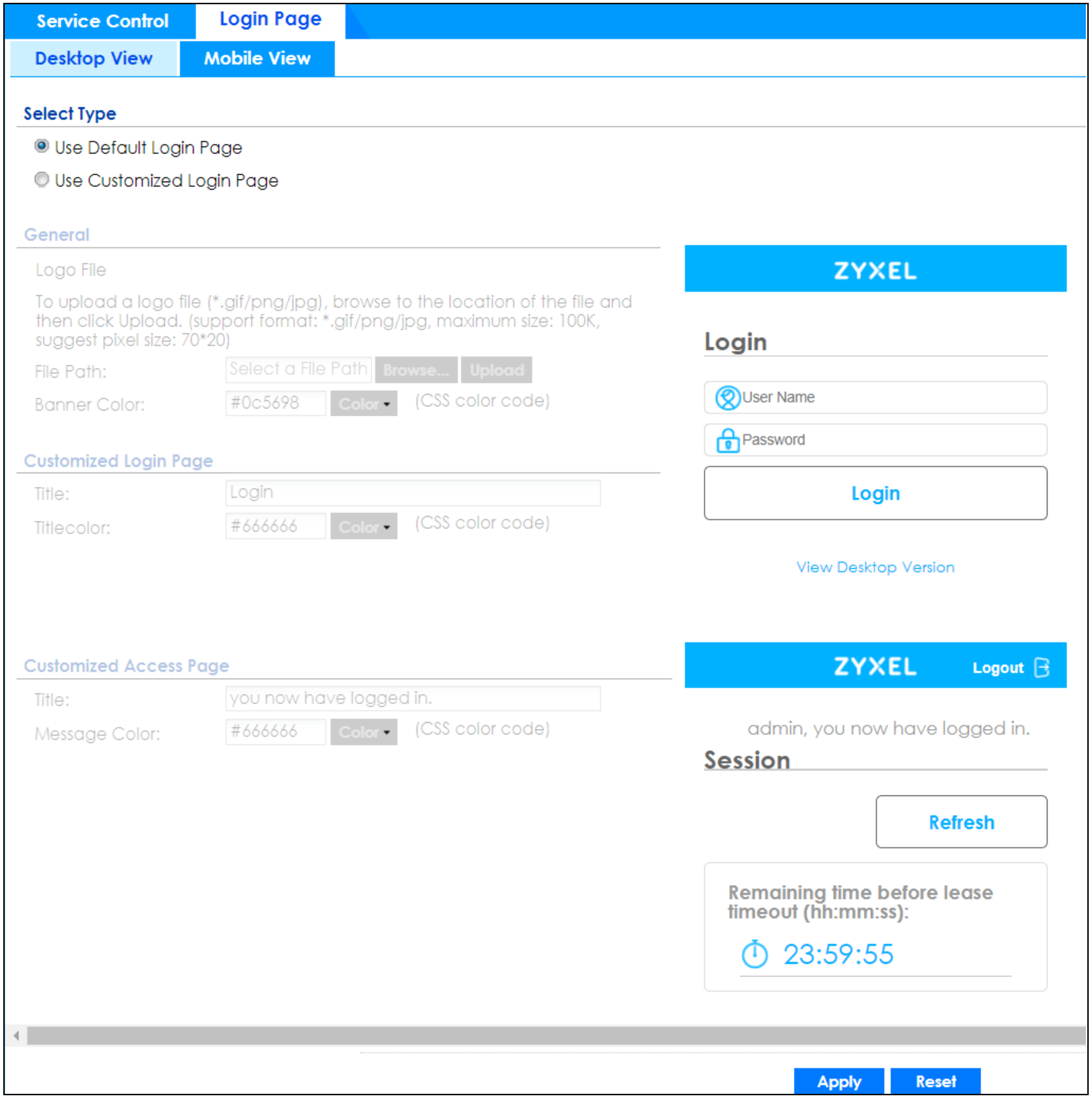
□ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 23:59:58

Remaining time before auth. timeout (hh:mm:ss): 23:59:58

Logout

Figure 509 Configuration > System > WWW > Login Page (Mobile View)



Service Control | Login Page

Desktop View | Mobile View

Select Type

● Use Default Login Page

○ Use Customized Login Page

General

Logo File

To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload. (support format: *.gif/png/jpg, maximum size: 100K, suggest pixel size: 70*20)

File Path: Select a File Path [Browse...] [Upload]

Banner Color: #0c5698 [Color] (CSS color code)

Customized Login Page

Title: Login

Titlecolor: #666666 [Color] (CSS color code)

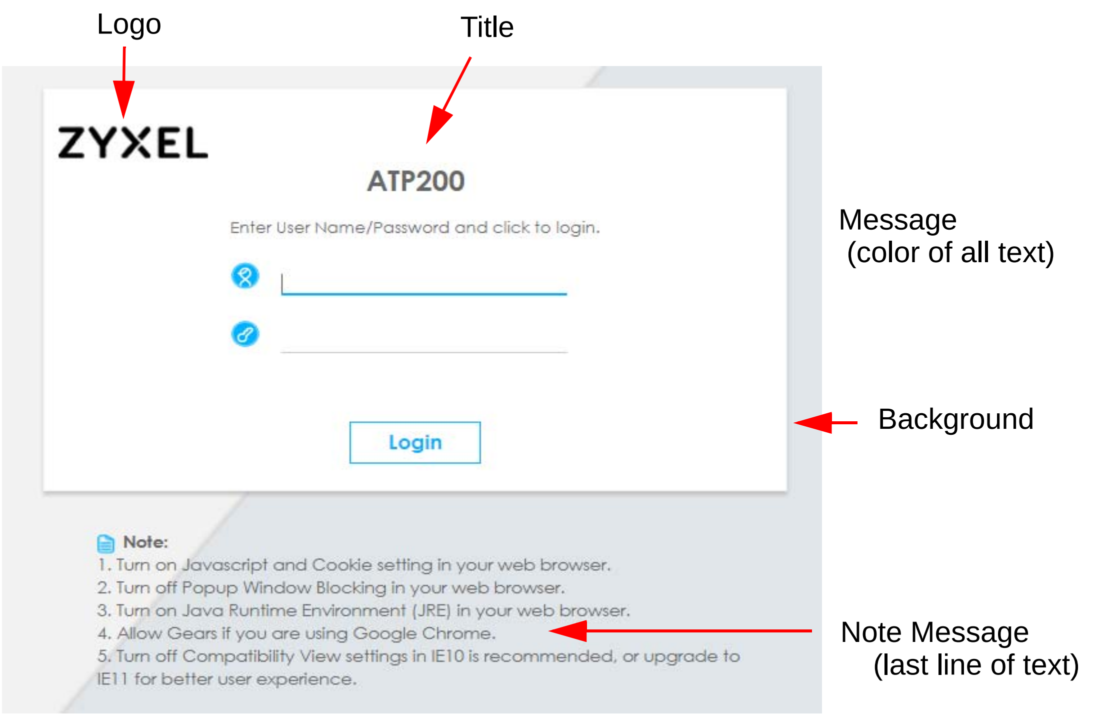
Customized Access Page

Title: you now have logged in.

Message Color: #666666 [Color] (CSS color code)

The following figures identify the parts you can customize in the login and access pages.

Figure 510 Login Page Customization



Logo

Title

Message
(color of all text)

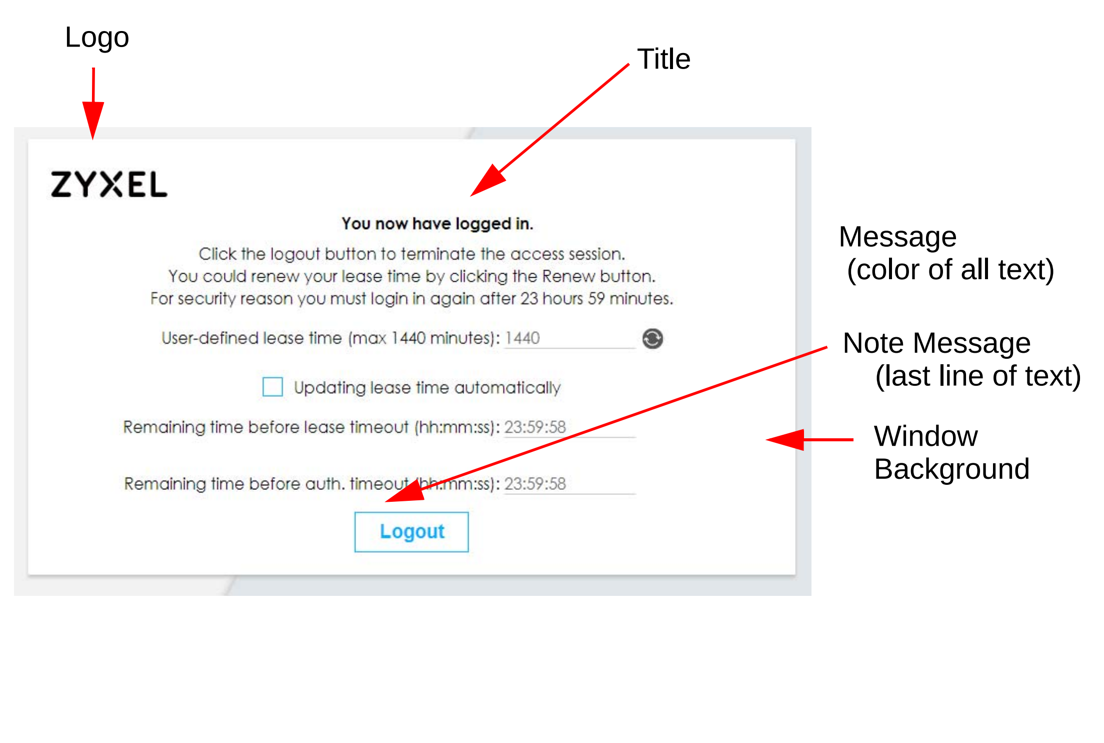
Background

Note Message
(last line of text)

Enter User Name/Password and click to login.

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.
5. Turn off Compatibility View settings in IE10 is recommended, or upgrade to IE11 for better user experience.

Figure 511 Access Page Customization



Logo

Title

Message
(color of all text)

Note Message
(last line of text)

Window
Background

You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 23 hours 59 minutes.

User-defined lease time (max 1440 minutes): 1440

□ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 23:59:58

Remaining time before auth. timeout (hh:mm:ss): 23:59:58

You can specify colors in one of the following ways:

- Click **Color** to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.

- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.
- Enter "rgb" followed by red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.

Your desired color should display in the preview screen on the right after you click in another field, click **Apply**, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

Table 326 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click **Upload** to transfer the specified graphic file from your computer to the Zyxel Device.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the window's background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.

Table 326 Configuration > System > WWW > Login Page (continued)

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

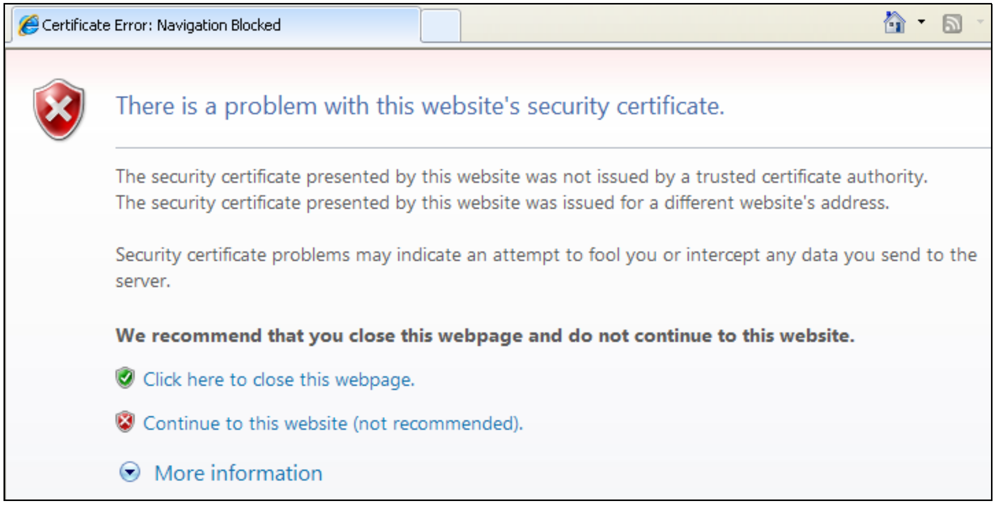
38.7.7 HTTPS Example

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

38.7.7.1 Internet Explorer Warning Messages

When you attempt to access the Zyxel Device HTTPS server, you will see the error message shown in the following screen.

Figure 512 Security Alert Dialog Box (Internet Explorer)



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

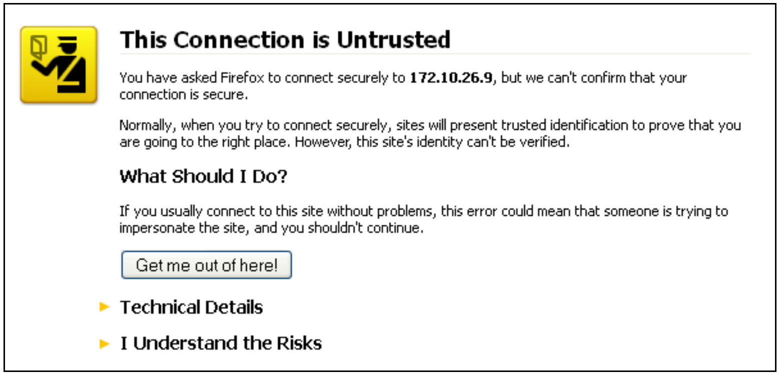
Select **Continue to this website** to proceed to the Web Configurator login screen. Otherwise, select **Click here to close this web page** to block the access.

38.7.7.2 Mozilla Firefox Warning Messages

When you attempt to access the Zyxel Device HTTPS server, a **The Connection is Untrusted** screen appears as shown in the following screen. Click **Technical Details** if you want to verify more information about the certificate from the Zyxel Device.

Select **I Understand the Risks** and then click **Add Exception** to add the Zyxel Device to the security exception list. Click **Confirm Security Exception**.

Figure 513 Security Certificate 1 (Firefox)



This Connection is Untrusted

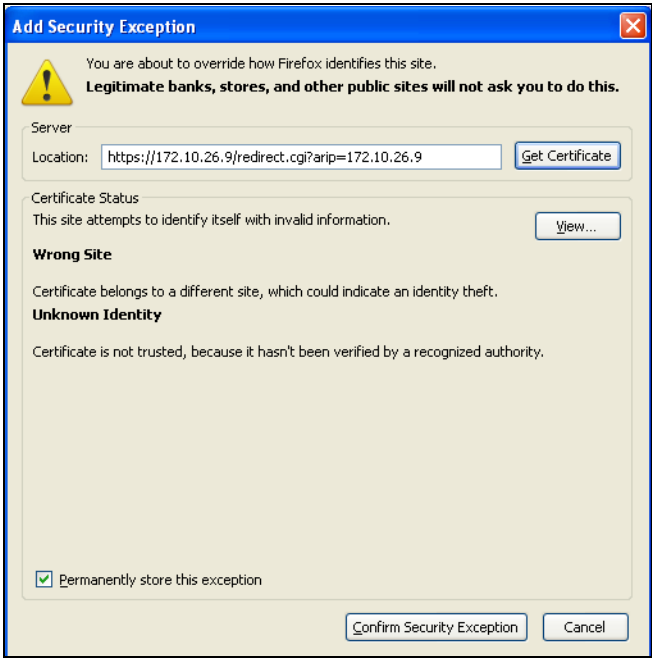
You have asked Firefox to connect securely to **172.10.26.9**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 514 Security Certificate 2 (Firefox)



You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://172.10.26.9/redirect.cgi?arip=172.10.26.9

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

38.7.7.3 Avoiding Browser Warning Messages

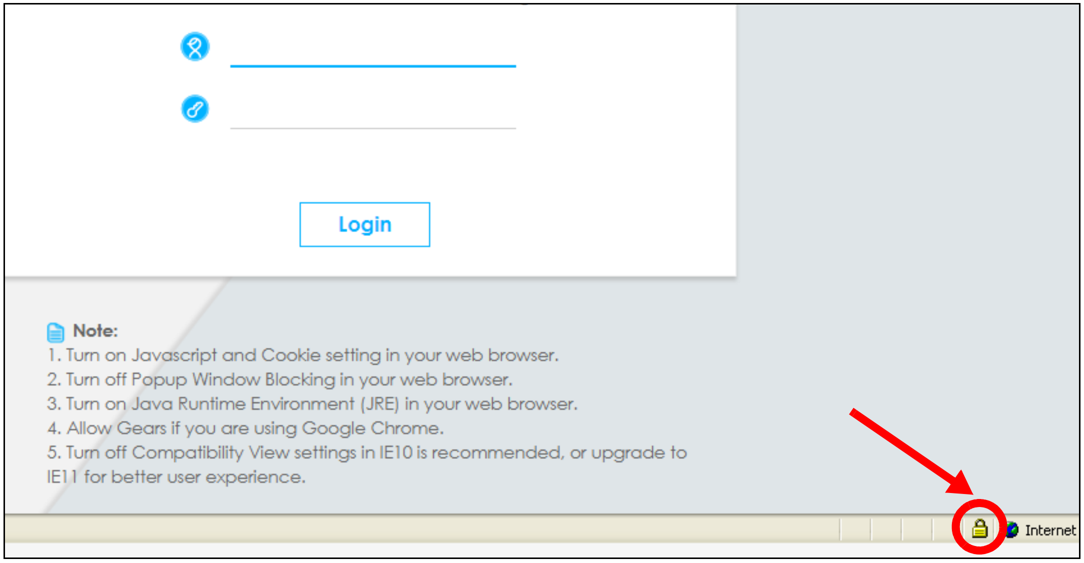
Here are the main reasons your browser displays warnings about the Zyxel Device's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the Zyxel Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Zyxel Device's factory default certificate is the Zyxel Device itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.

38.7.7.4 Login Screen

After you accept the certificate, the Zyxel Device login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 515 Login Screen (Internet Explorer)



Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.
5. Turn off Compatibility View settings in IE10 is recommended, or upgrade to IE11 for better user experience.

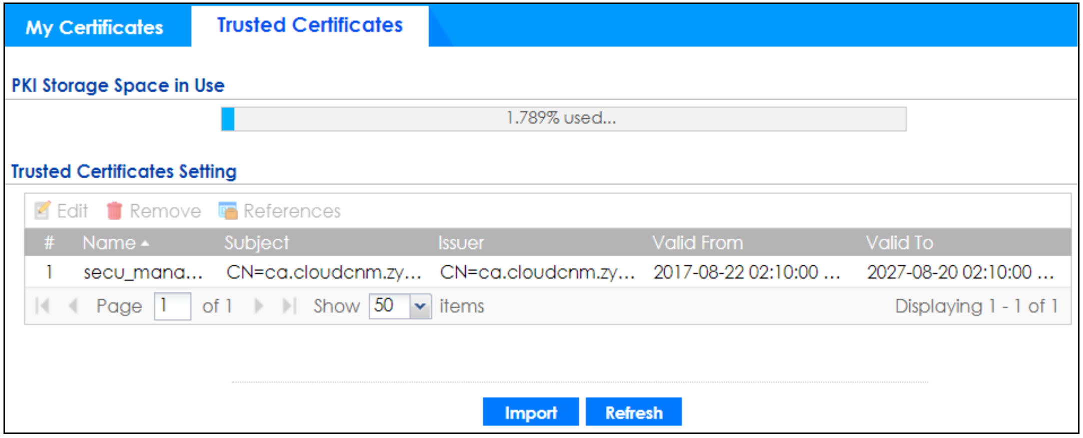
38.7.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Zyxel Device.

You must have imported at least one trusted CA to the Zyxel Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Zyxel Device (see the Zyxel Device's **Trusted CA** Web Configurator screen).

Figure 516 Zyxel Device Trusted CA Screen



PKI Storage Space in Use

1.789% used...

Trusted Certificates Setting

#	Name ▲	Subject	Issuer	Valid From	Valid To
1	secu_mana...	CN=ca.cloudcnm.zy...	CN=ca.cloudcnm.zy...	2017-08-22 02:10:00 ...	2027-08-20 02:10:00 ...

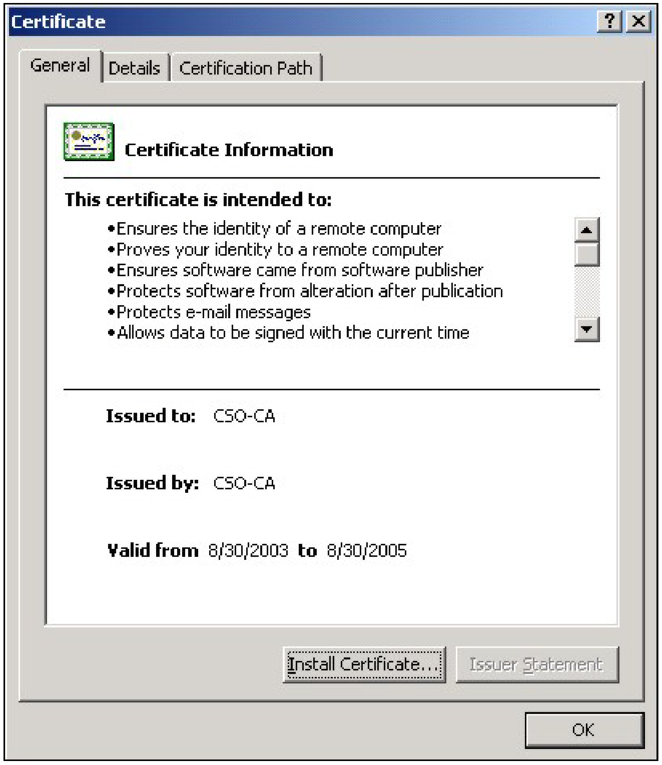
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

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

38.7.7.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 517 CA Certificate Example



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: CSO-CA

Issued by: CSO-CA

Valid from 8/30/2003 **to** 8/30/2005

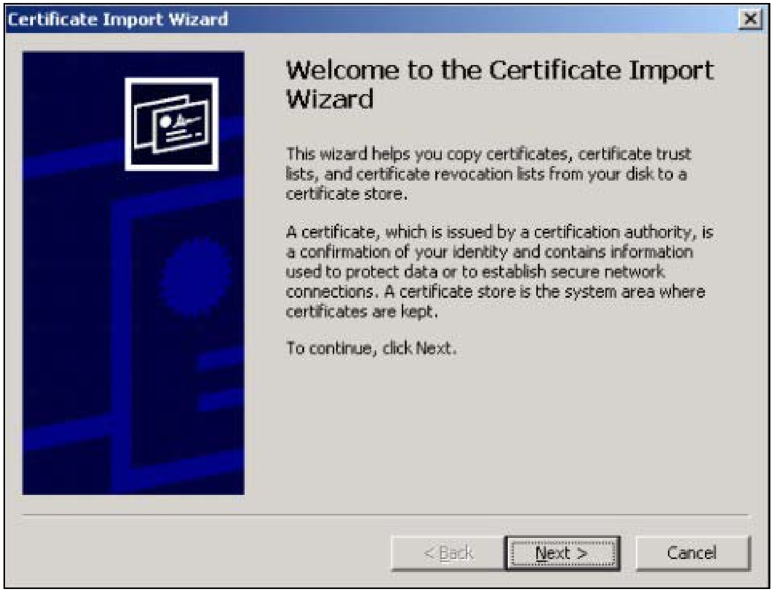
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

38.7.7.5.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 518 Personal Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

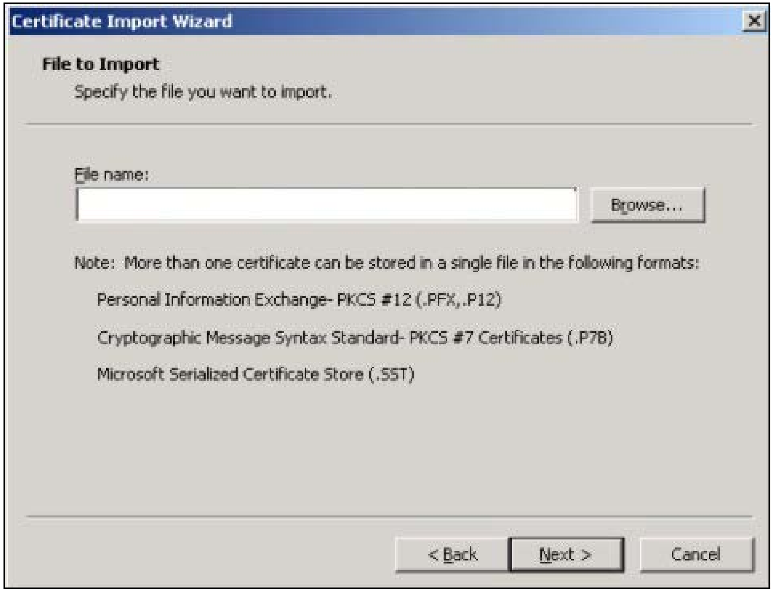
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 519 Personal Certificate Import Wizard 2



File to Import

Specify the file you want to import.

File name:

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

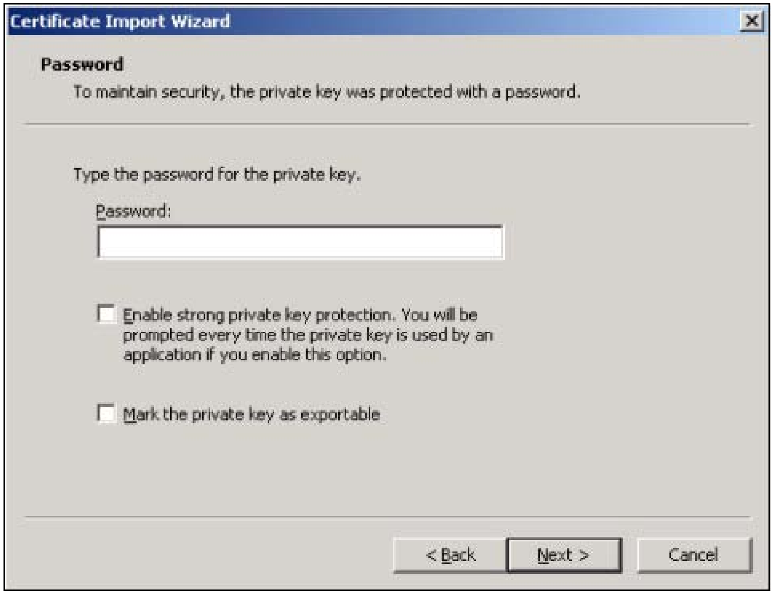
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

Figure 520 Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

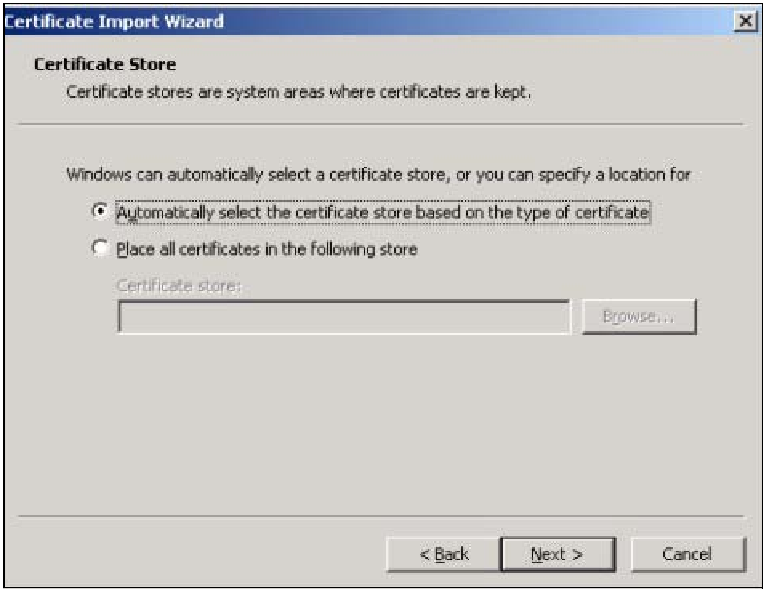
Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

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

Figure 521 Personal Certificate Import Wizard 4



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

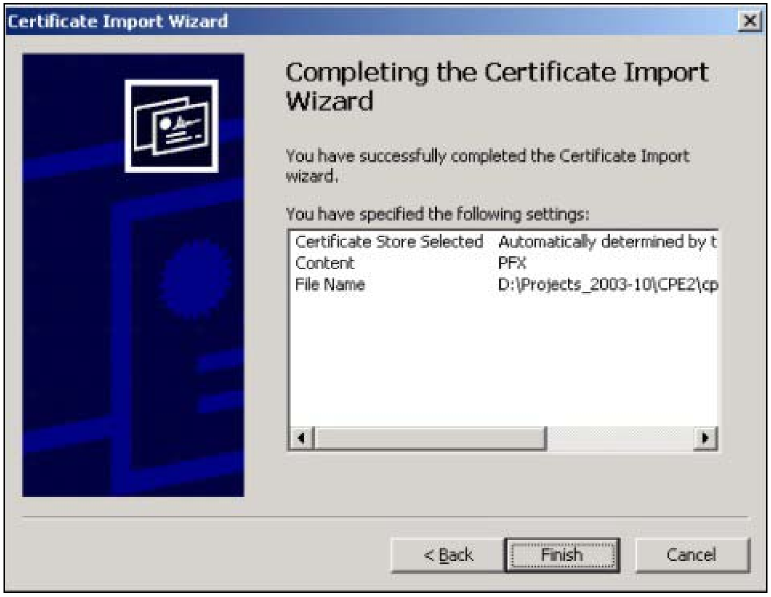
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

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

Figure 522 Personal Certificate Import Wizard 5



Completing the Certificate Import Wizard

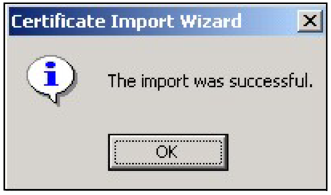
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

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

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

Figure 523 Personal Certificate Import Wizard 6



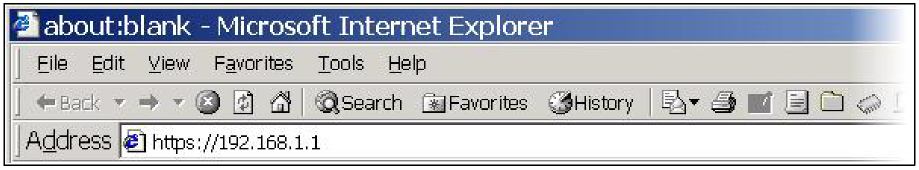
The import was successful.

38.7.7.6 Using a Certificate When Accessing the Zyxel Device Example

Use the following procedure to access the Zyxel Device via HTTPS.

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

Figure 524 Access the Zyxel Device Via HTTPS

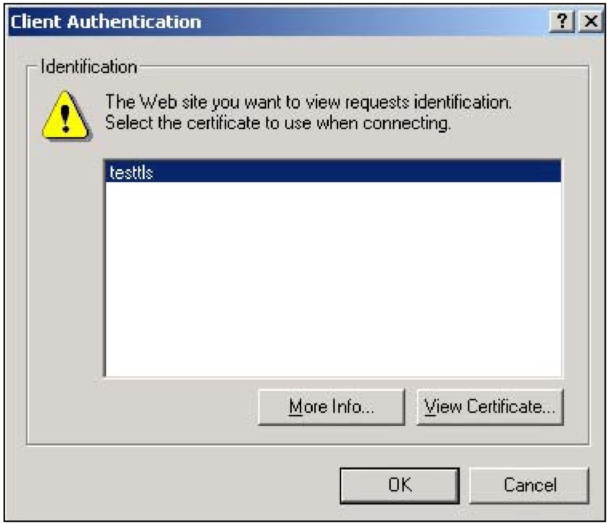


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address

https://192.168.1.1

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

Figure 525 SSL Client Authentication



Client Authentication

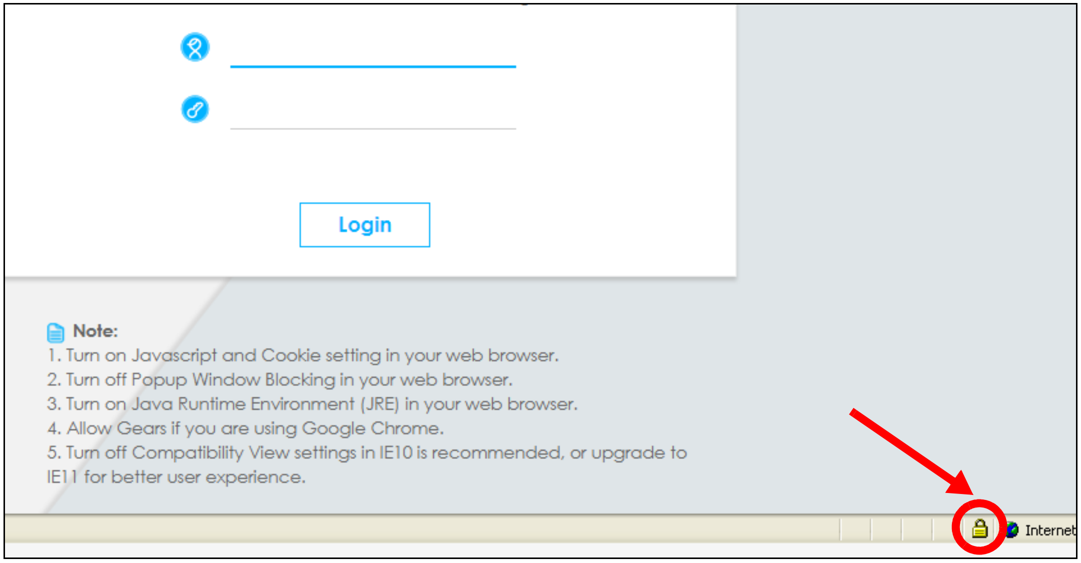
Identification

The Web site you want to view requests identification.
Select the certificate to use when connecting.

testtls

3 You next see the Web Configurator login screen.

Figure 526 Secure Web Configurator Login Screen



Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.
5. Turn off Compatibility View settings in IE10 is recommended, or upgrade to IE11 for better user experience.

38.8 SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

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

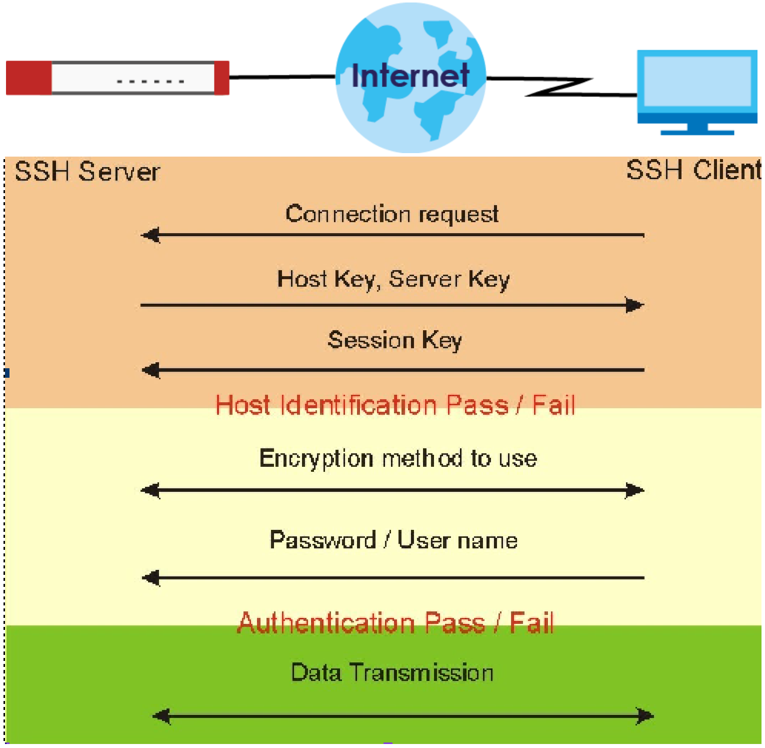
Figure 527 SSH Communication Over the WAN Example

Internet
Secure Connection
A

38.8.1 How SSH Works

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

Figure 528 How SSH v1 Works Example



1 Host Identification

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

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

2 Encryption Method

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

3 Authentication and Data Transmission

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

38.8.2 SSH Implementation on the Zyxel Device

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

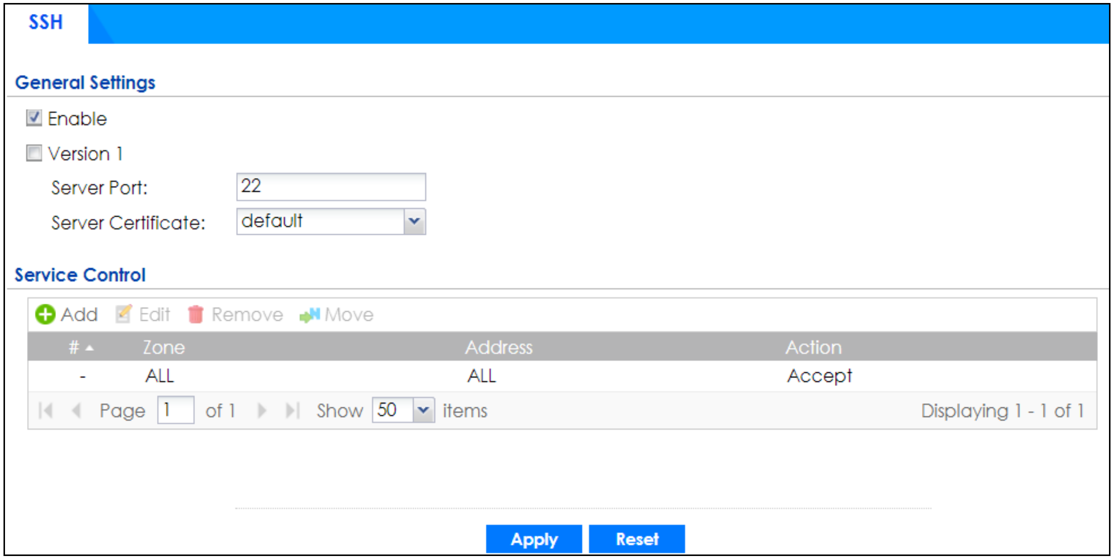
38.8.3 Requirements for Using SSH

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

38.8.4 Configuring SSH

Click **Configuration > System > SSH** to change your Zyxel Device's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 529 Configuration > System > SSH



SSH

General Settings

☑ Enable

□ Version 1

Server Port: 22

Server Certificate: default

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 327 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service.
Version 1	Select the check box to have the Zyxel Device use both SSH version 1 and version 2 protocols. If you clear the check box, the Zyxel Device uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

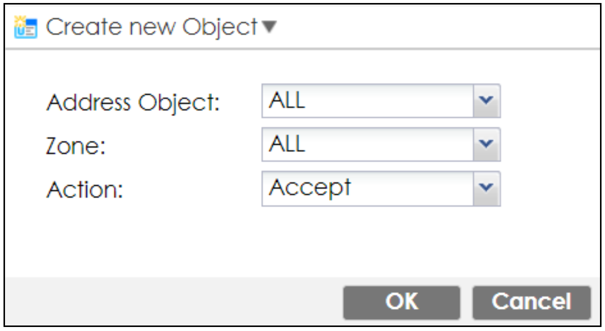
Table 327 Configuration > System > SSH (continued)

LABEL	DESCRIPTION
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. You must have certificates already configured in the **My Certificates** screen.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 325 on page 754 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.8.5 Service Control Rules

Click the **Add** or **Edit** icon in the **Service Control** table to add a service control rule.

Figure 530 Configuration > System > SSH > Service Control Rule Add/Edit



Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

Table 328 Configuration > System > SSH > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the Zyxel Device using SSH. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using SSH.
Zone	Select **ALL** to allow or prevent any Zyxel Device zones from being accessed using SSH. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.

Table 328 Configuration > System > SSH > Service Control Rule Add/Edit (continued)

LABEL	DESCRIPTION
Action	Select **Accept** to allow the user to access the Zyxel Device from the specified computers. Select **Deny** to block the user's access to the Zyxel Device from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.8.6 Secure Telnet Using SSH Examples

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

38.8.6.1 Example 1: Microsoft Windows

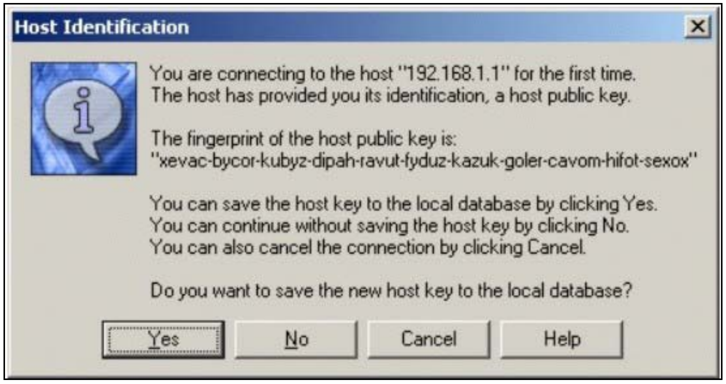
This section describes how to access the Zyxel Device using the Secure Shell Client program.

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

2 Configure the SSH client to accept connection using SSH version 1.

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

Figure 531 SSH Example 1: Store Host Key



Host Identification

You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

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

38.8.6.2 Example 2: Linux

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

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

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the Zyxel Device (using the default IP address of 192.168.1.1).

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

Figure 532 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the Zyxel Device using SSH version 1. If this is the first time you are connecting to the Zyxel Device using SSH, a message displays prompting you to save the host information of the Zyxel Device. Type "`yes`" and press [ENTER].

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

Figure 533 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

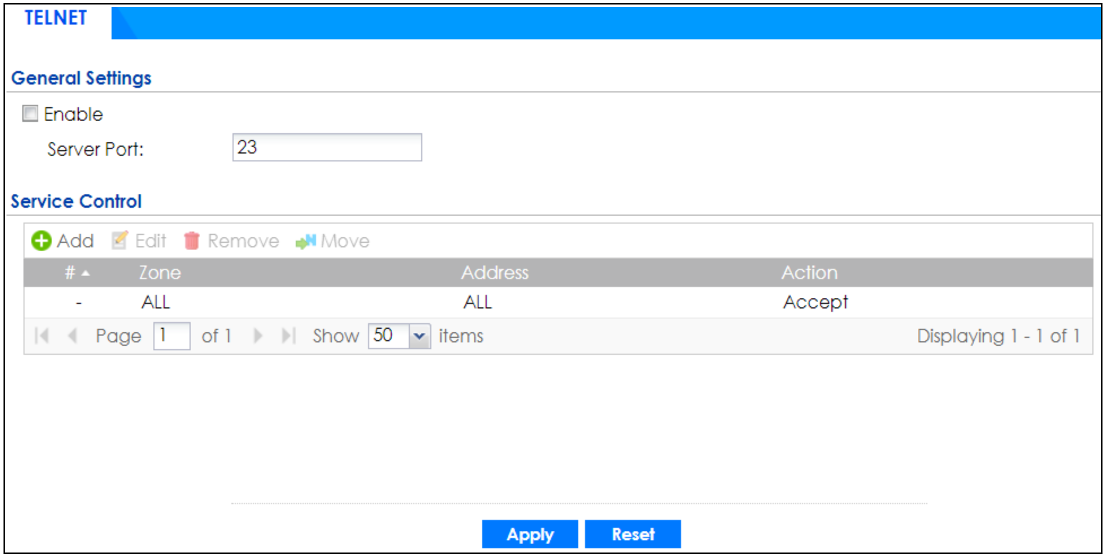
38.9 Telnet

You can use Telnet to access the Zyxel Device's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

38.9.1 Configuring Telnet

Click **Configuration > System > TELNET** to configure your Zyxel Device for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 534 Configuration > System > TELNET



The following table describes the labels in this screen.

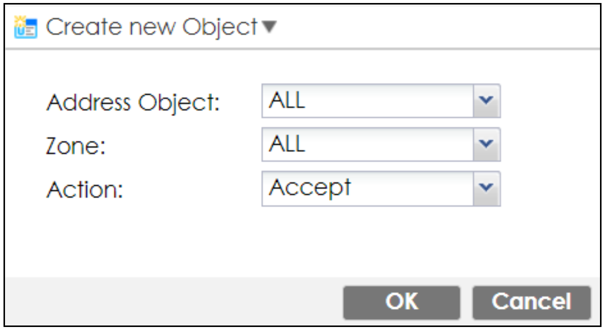
Table 329 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 325 on page 754 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.9.2 Service Control Rules

Click the **Add** or **Edit** icon in the **Service Control** table to add a service control rule.

Figure 535 Configuration > System > TELNET > Service Control Rule Add/Edit



Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

Table 330 Configuration > System > TELNET > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the Zyxel Device using Telnet. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using Telnet.
Zone	Select **ALL** to allow or prevent any Zyxel Device zones from being accessed using Telnet. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the Zyxel Device from the specified computers. Select **Deny** to block the user's access to the Zyxel Device from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

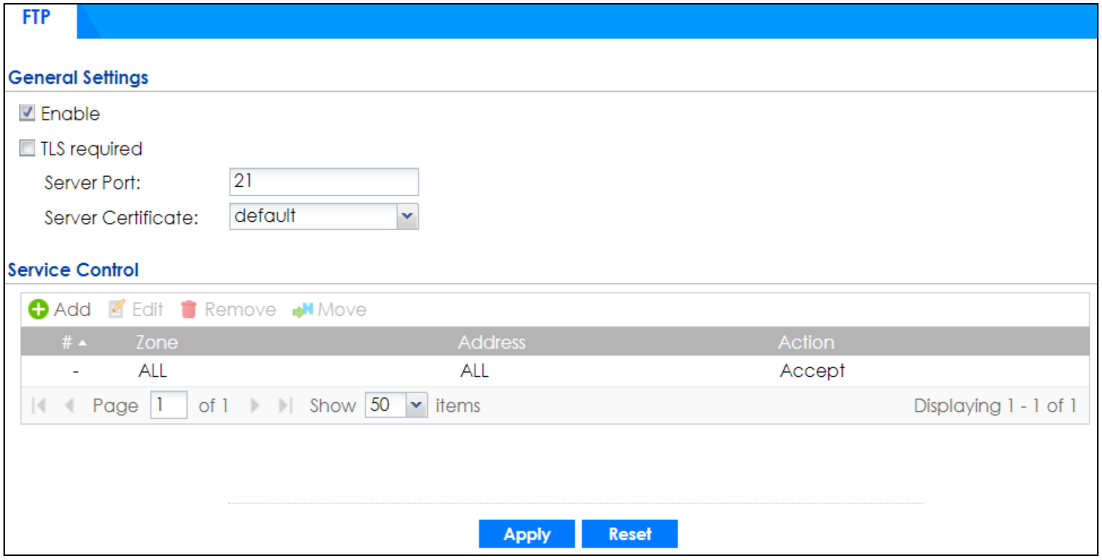
38.10 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

38.10.1 Configuring FTP

To change your Zyxel Device's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 536 Configuration > System > FTP



General Settings

☑ Enable

□ TLS required

Server Port: 21

Server Certificate: default

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 331 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections. You must have certificates already configured in the **My Certificates** screen.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 325 on page 754 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).

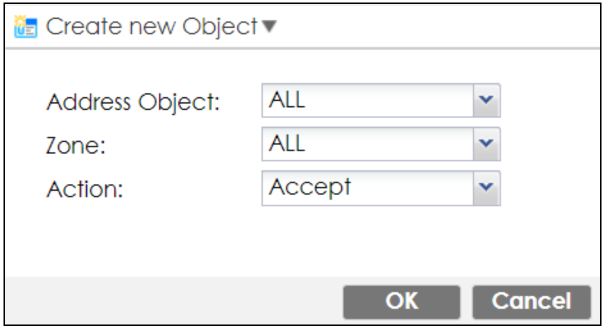
Table 331 Configuration > System > FTP (continued)

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

38.10.2 Service Control Rules

Click the **Add** or **Edit** icon in the **Service Control** table to add a service control rule.

Figure 537 Configuration > System > FTP > Service Control Rule Add/Edit



Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

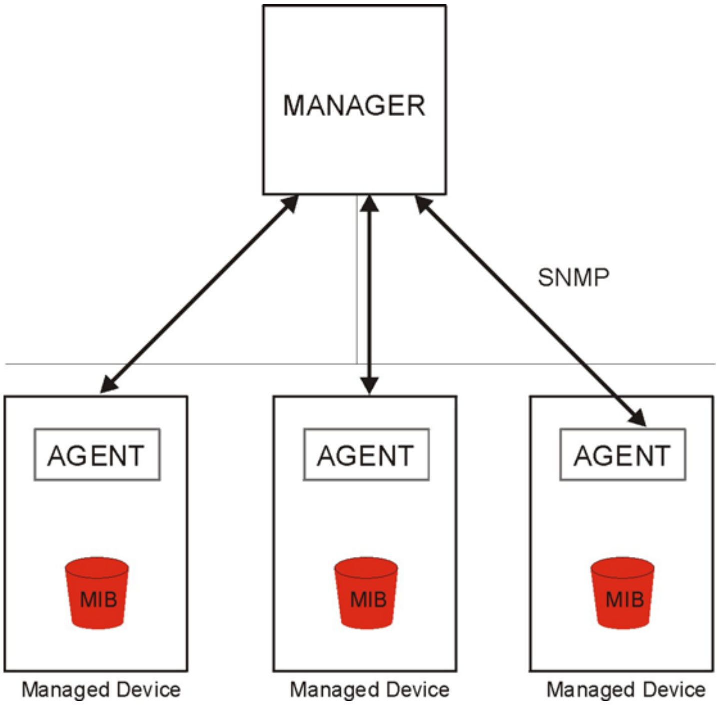
Table 332 Configuration > System > FTP > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the Zyxel Device using FTP. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using FTP.
Zone	Select **ALL** to allow or prevent any Zyxel Device zones from being accessed using FTP. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the Zyxel Device from the specified computers. Select **Deny** to block the user's access to the Zyxel Device from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1), version two (SNMPv2c) and version 3 (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 538 SNMP Management Model



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

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

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

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

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

38.11.1 SNMPv3 and Security

SNMPv3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

38.11.2 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

38.11.3 SNMP Traps

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

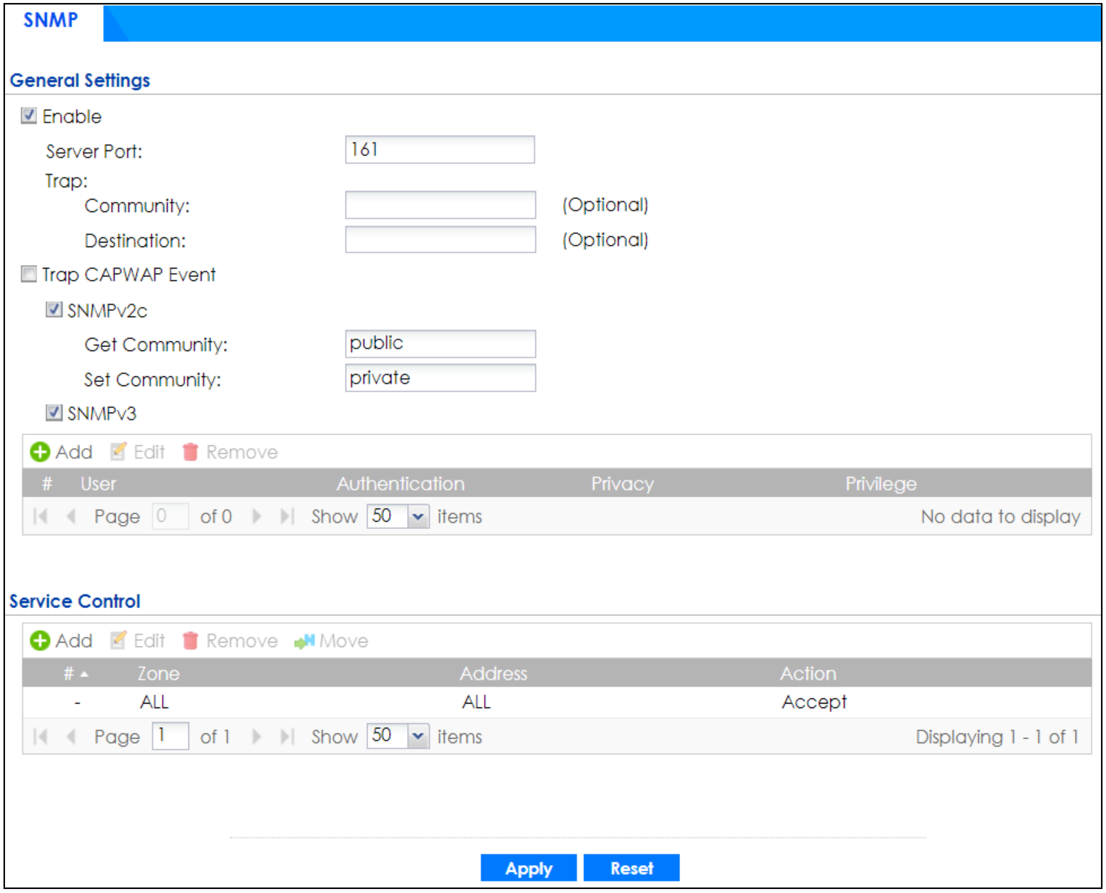
Table 333 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Zyxel Device is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

38.11.4 Configuring SNMP

To change your Zyxel Device's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 539 Configuration > System > SNMP



SNMP

General Settings

☑ Enable

Server Port: 161

Trap:

Community: (Optional)

Destination: (Optional)

☐ Trap CAPWAP Event

☑ SNMPv2c

Get Community: public

Set Community: private

☑ SNMPv3

#	User	Authentication	Privacy	Privilege

Page 0 of 0 Show 50 items No data to display

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 334 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Trap CAPWAP Event	Select this option to have the Zyxel Device send a trap to the SNMP manager when a managed AP is connected to or disconnected from the Zyxel Device.
SNMPv2c	Select the SNMP version for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.

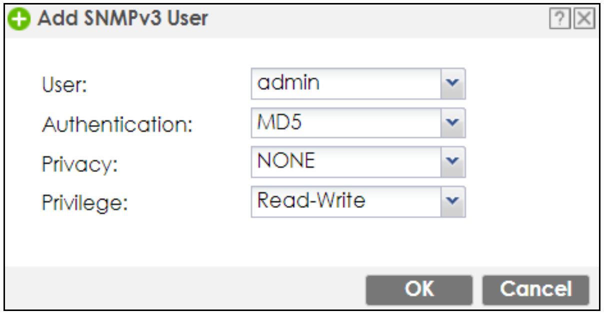
Table 334 Configuration > System > SNMP (continued)

LABEL	DESCRIPTION
SNMPv3	Select the SNMP version for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager. SNMPv3 (RFCs 3413 to 3415) provides secure access by authenticating and encrypting data packets over the network. The Zyxel Device uses your login password as the SNMPv3 authentication and encryption passphrase. Note: Your login password must consist of at least 8 printable characters for SNMPv3. An error message will display if your login password has fewer characters.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the entry.
User	This displays the name of the user object to be sent to the SNMP manager along with the SNMP v3 trap.
Authentication	This displays the authentication algorithm used for this entry. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	This displays the encryption method for SNMP communication from this user. Methods available are: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Privilege	This displays the access rights to MIBs. • **Read-Write** - The associated user can create and edit the MIBs on the Zyxel Device, except the user account. • **Read-Only** - The associated user can only collect information from the Zyxel Device MIBs.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 325 on page 754 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.11.5 Add SNMPv3 User

Click **Add** under SNMPv3 in **Configuration > System > SNMP** to create an SNMPv3 user for authentication with managers using SNMP v3. Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.

Figure 540 Configuration > System > SNMP(v3) > Add



Add SNMPv3 User

User: admin

Authentication: MD5

Privacy: NONE

Privilege: Read-Write

The following table describes the labels in this screen.

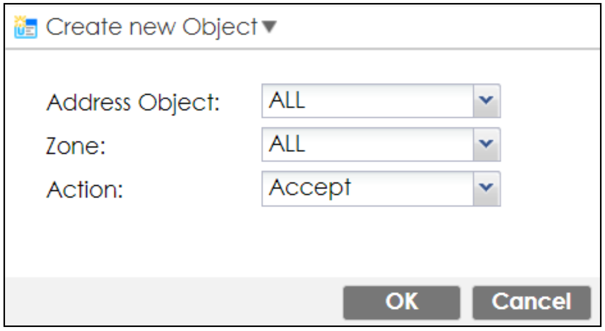
Table 335 Configuration > System > SNMP(v3) > Add

LABEL	DESCRIPTION
User	Specify the username of a login account on the Zyxel Device. The associated password is used in authentication algorithms and encryption methods.
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Privilege	Select the access rights to MIBs. • **Read-Write** - The associated user can create and edit the MIBs on the Zyxel Device, except the user account. • **Read-Only** - The associated user can only collect information from the Zyxel Device MIBs.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38.11.6 Service Control Rules

Click the **Add** or **Edit** icon in the **Service Control** table to add a service control rule.

Figure 541 Configuration > System > SNMP > Service Control Rule Add/Edit



Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

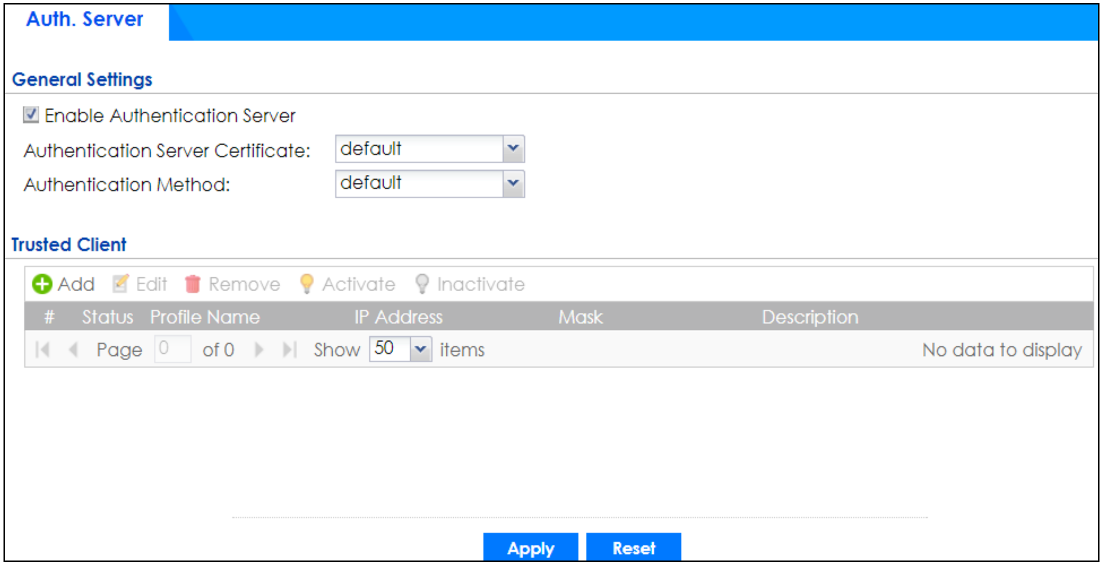
Table 336 Configuration > System > SNMP > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the Zyxel Device using SNMP. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using SNMP.
Zone	Select **ALL** to allow or prevent any Zyxel Device zones from being accessed using SNMP. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the Zyxel Device from the specified computers. Select **Deny** to block the user's access to the Zyxel Device from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.12 Authentication Server

You can set the Zyxel Device to work as a RADIUS server to exchange messages with a RADIUS client, such as an AP for user authentication and authorization. Click **Configuration > System > Auth. Server** tab. The screen appears as shown. Use this screen to enable the authentication server feature of the Zyxel Device and specify the RADIUS client's IP address.

Figure 542 Configuration > System > Auth. Server



Auth. Server

General Settings

☑ Enable Authentication Server

Authentication Server Certificate: default

Authentication Method: default

Trusted Client

#	Status	Profile Name	IP Address	Mask	Description

Page 0 of 0 Show 50 items No data to display

The following table describes the labels in this screen.

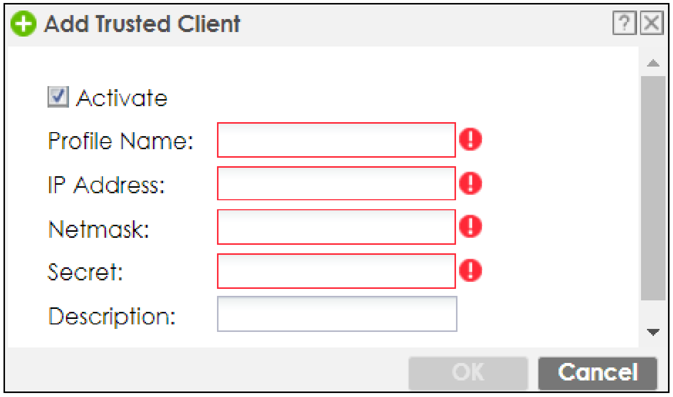
Table 337 Configuration > System > Auth. Server

LABEL	DESCRIPTION
Enable Authentication Server	Select the check box to have the Zyxel Device act as a RADIUS server.
Authentication Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device to the RADIUS client. You must have certificates already configured in the **My Certificates** screen.
Authentication Method	Select an authentication method if you have created any in the **Configuration > Object > Auth. Method** screen.
Trusted Client	Use this section to configure trusted clients in the Zyxel Device RADIUS server database.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This is the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the profile.
IP Address	This is the IP address of the RADIUS client that is allowed to exchange messages with the Zyxel Device.
Mask	This is the subnet mask of the RADIUS client.
Description	This is the description of the RADIUS client.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.12.1 Add/Edit Trusted RADIUS Client

Click **Configuration > System > Auth. Server** to display the **Auth. Server** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new entry or edit an existing one.

Figure 543 Configuration > System > Auth. Server > Add/Edit



The following table describes the labels in this screen.

Table 338 Configuration > System > Auth. Server > Add/Edit

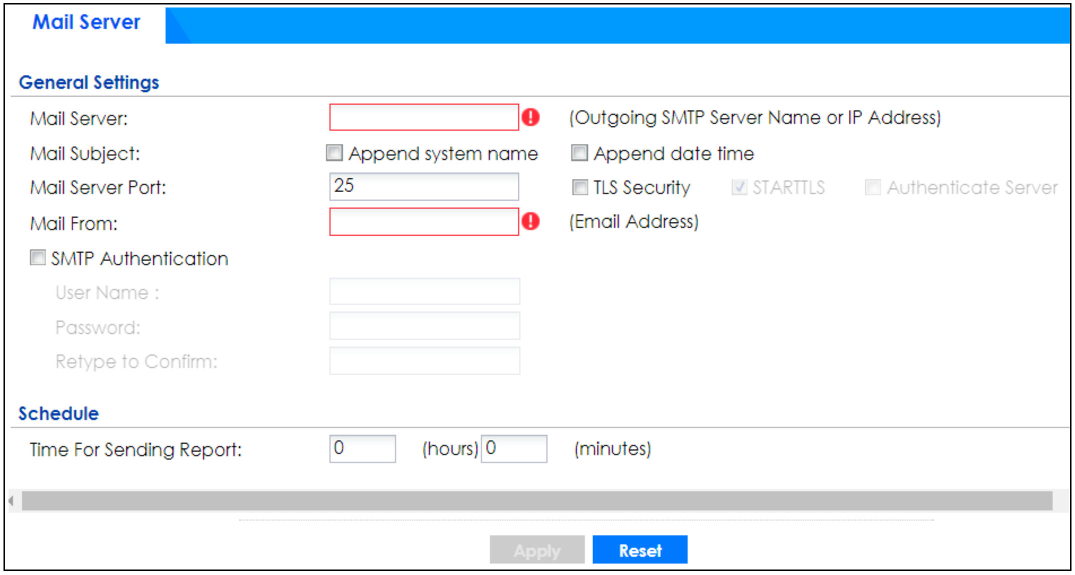
LABEL	DESCRIPTION
Activate	Select this check box to make this profile active.
Profile Name	Enter a descriptive name (up to 31 alphanumerical characters) for identification purposes.
IP Address	Enter the IP address of the RADIUS client that is allowed to exchange messages with the Zyxel Device.
Netmask	Enter the subnet mask of the RADIUS client.
Secret	Enter a password (up to 64 alphanumeric characters) as the key to be shared between the Zyxel Device and the RADIUS client. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

38.13 Notification > Mail Server

Use this screen to configure a mail server so you can receive reports and notification emails such as when your password is about to expire. After you configure the screen, you can test the settings in **Maintenance > Diagnostics > Network Tool** and then select **Test Email Server**. See **Configuration > Log & Report > Email Daily Report** to configure what reports to send and to whom.

Click **Configuration > System > Notification** to display the **Mail Server** screen.

Figure 544 Configuration > System > Notification



Mail Server

General Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: (Email Address)

□ SMTP Authentication

User Name :

Password:

Retype to Confirm:

Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

The following table describes the labels in this screen.

Table 339 Configuration > System > Notification

LABEL	DESCRIPTION
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Go to **Configuration > Log & Report > Email Daily Report** to type a subject line for outgoing email from the Zyxel Device.
Append system name	Select **Append system name** to add the Zyxel Device's system name to the subject.
Append date time	Select **Append date time** to add the Zyxel Device's system date and time to the subject.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select this option if the mail server uses Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
STARTTLS	Select this option if the mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device.
Authenticate Server	Select this if the Zyxel Device authenticates the mail server in the TLS handshake.
Mail From	Type the email address from which the outgoing email is delivered. This address is used in replies.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type a password of up to 63 characters to provide to the SMTP server when the log is emailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Time for sending report	Select the time of day (hours and minutes) when the log is emailed. Use 24-hour notation.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

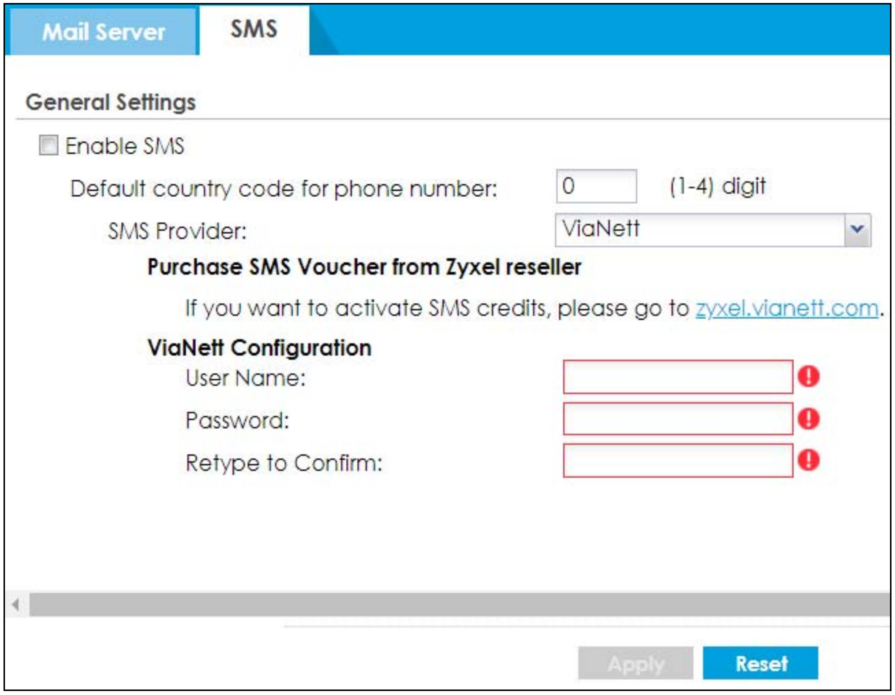
38.14 Notification > SMS

The Zyxel Device supports Short Message Service (SMS) to send short text messages to mobile phone devices. At the time of writing, the Zyxel Device uses ViaNett as the SMS gateway to help forward SMS messages. You must already have a ViaNett account in order to use the SMS service.

Click **Configuration > System > Notification > SMS** to open the following screen.

Configure the settings according to your SMS service provider's format. Different SMS service providers may have different format.

Figure 545 Configuration > System > Notification > SMS



General Settings

□ Enable SMS

Default country code for phone number: 0 (1-4) digit

SMS Provider: ViaNett

Purchase SMS Voucher from Zyxel reseller

If you want to activate SMS credits, please go to zyxel.vianett.com.

ViaNett Configuration

User Name:

Password:

Retype to Confirm:

The following table describes the labels in this screen.

Table 340 Configuration > System > Notification > SMS

LABEL	DESCRIPTION
General Settings	
Enable SMS	Select the check box to turn on the SMS service.
Default country code for phone number	Enter the default country code for the mobile phone number to which you want to send SMS messages.
SMS Provider	Select **ViaNett** if you use ViaNett to help forward SMS messages. Select **Email-to-SMS Provider** if you use another SMS gateway to help forward SMS messages.
These fields are available when the **SMS Provider** is **Email-to-SMS Provider**. Note: Go to the **Configuration** > **System** > **Notification** > **Mail Server** screen to configure a mail server first, so the Zyxel Device can send SMS messages to the SMS service provider via emails. Thus, the SMS service provider will send the SMS messages.	

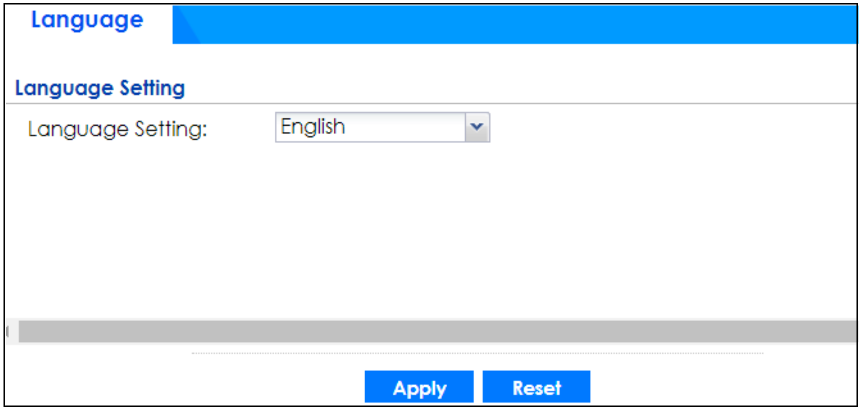
Table 340 Configuration > System > Notification > SMS (continued)

LABEL	DESCRIPTION
Provider Domain	Enter the domain name of your SMS service provider. The domain name can be of up to 252 characters. Select **auto append to "Mail to"** to add the domain name of your SMS service provider after the mobile phone number in the **Mail To** field.
Mail Subject	Type the subject line of up to 128 characters for outgoing e-mail from the Zyxel Device.
Mail From	Enter the sender's email address of up to 64 characters. This email address needs to be in your SMS provider's allowed sender address list. If you leave this field blank, the Zyxel Device will use the IP address or domain name of the **Mail Server** field in the **Configuration** > **System** > **Notification** > **Mail Server** screen.
Mail To	Enter the mobile phone number of up to 80 characters. You can only have one receiver. Use this variable in brackets [$mobile_number$], and the Zyxel Device will use the mobile phone number of the user logging in. Go to the **Configuration** > **Object** > **User/Group** > **User** screen to add a valid mobile telephone number for a user.
ViaNett Configuration	These fields are available when the **SMS Provider** is **ViaNett**.
User Name	Enter the user name for your ViaNett account.
Password	Type the Password associated with the user name.
Retype to Confirm	Type your password again for confirmation.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

38.15 Language Screen

Click **Configuration > System > Language** to open the following screen. Use this screen to select a display language for the Zyxel Device's Web Configurator screens.

Figure 546 Configuration > System > Language



Language

Language Setting

Language Setting: English

The following table describes the labels in this screen.

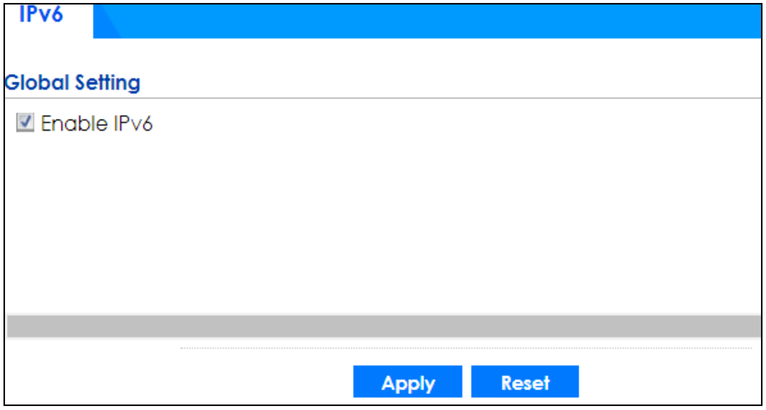
Table 341 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the Zyxel Device's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.16 IPv6 Screen

Click **Configuration > System > IPv6** to open the following screen. Use this screen to enable IPv6 support for the Zyxel Device's Web Configurator screens.

Figure 547 Configuration > System > IPv6



The following table describes the labels in this screen.

Table 342 Configuration > System > IPv6

LABEL	DESCRIPTION
Enable IPv6	Select this to have the Zyxel Device support IPv6 and make IPv6 settings be available on the screens that the functions support, such as the **Configuration** > **Network** > **Interface** > **Ethernet**, **VLAN**, and **Bridge** screens. The Zyxel Device discards all IPv6 packets if you clear this check box.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.17 Zyxel One Network (ZON) Utility

The Zyxel One Network (ZON) utility uses the Zyxel Discovery Protocol (ZDP) for discovering and configuring ZDP-aware Zyxel devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the Zyxel device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

38.17.1 Requirements

Before installing the ZON Utility on your computer, please make sure it meets the requirements listed below.

Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)
- Window 10 (both 32-bit / 64-bit versions)

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

Hardware

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

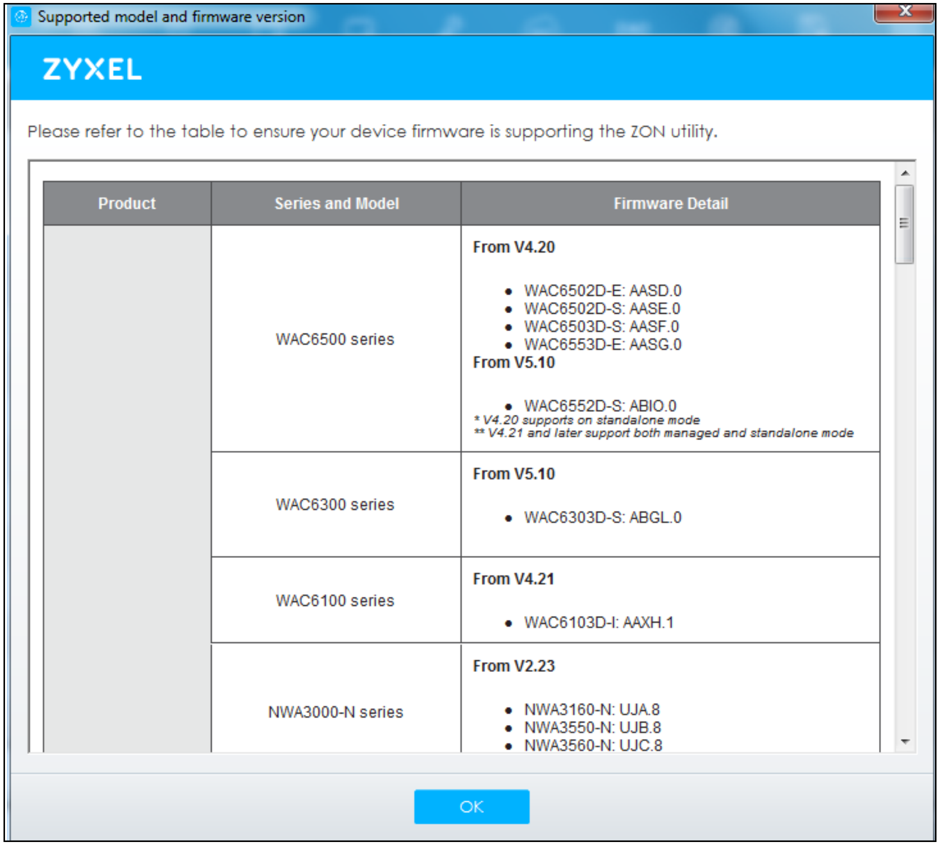
- Core i3 processor
- 2GB RAM
- 100MB free hard disk
- WXGA (Wide XGA 1280x800)

38.17.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

2 The first time you run the ZON Utility you will see if your Zyxel Device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 548 Supported Devices and Versions



Supported model and firmware version

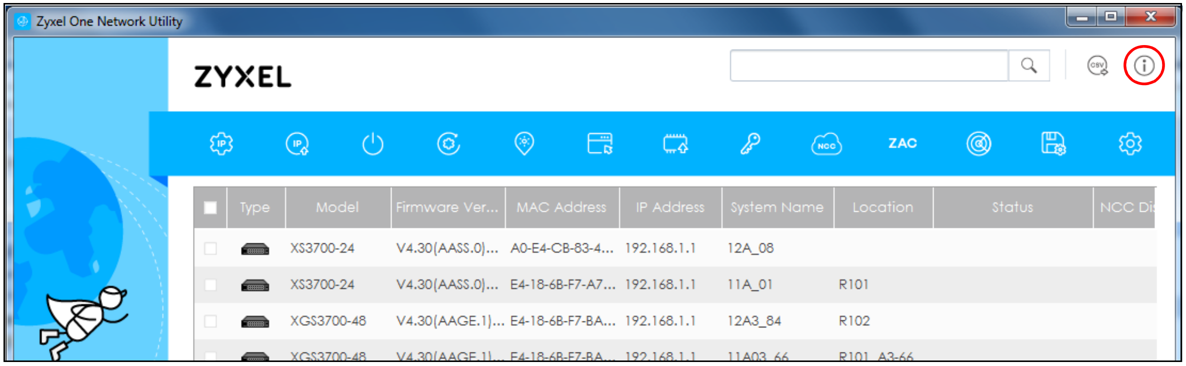
ZYXEL

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

Product	Series and Model	Firmware Detail
	WAC6500 series	**From V4.20** • WAC6502D-E: AASD.0 • WAC6502D-S: AASE.0 • WAC6503D-S: AASF.0 • WAC6553D-E: AASG.0 **From V5.10** • WAC6552D-S: ABIO.0 ** V4.20 supports on standalone mode* *** V4.21 and later support both managed and standalone mode*
	WAC6300 series	**From V5.10** • WAC6303D-S: ABGL.0
	WAC6100 series	**From V4.21** • WAC6103D-I: AAXH.1
	NWA3000-N series	**From V2.23** • NWA3160-N: UJA.8 • NWA3550-N: UJB.8 • NWA3560-N: UJC.8

If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON utility support. The release notes are in the firmware zip file on the Zyxel web site.

Figure 549 ZON Utility Screen



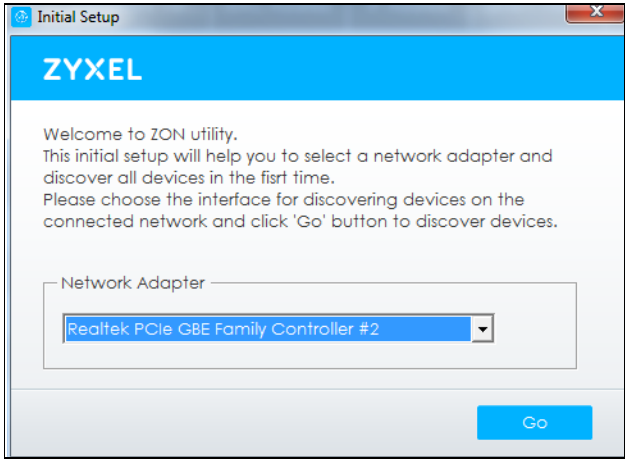
Zyxel One Network Utility

ZYXEL

□	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	NCC Di
□		XS3700-24	V4.30(AASS.0)...	A0-E4-CB-83-4...	192.168.1.1	12A_08			
□		XS3700-24	V4.30(AASS.0)...	E4-18-6B-F7-A7...	192.168.1.1	11A_01	R101		
□		XGS3700-48	V4.30(AAGE.1)...	E4-18-6B-F7-BA...	192.168.1.1	12A3_84	R102		
□		XGS3700-48	V4.30(AAGE.1)...	E4-18-6B-F7-BA...	192.168.1.1	11A03_66	R101_A3-66		

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

Figure 550 Network Adapter

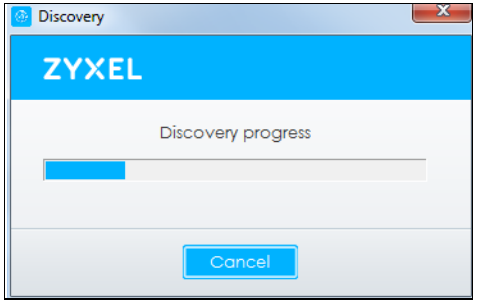


Welcome to ZON utility.
This initial setup will help you to select a network adapter and discover all devices in the fisrt time.
Please choose the interface for discovering devices on the connected network and click 'Go' button to discover devices.

Network Adapter: Realtek PCIe GBE Family Controller #2

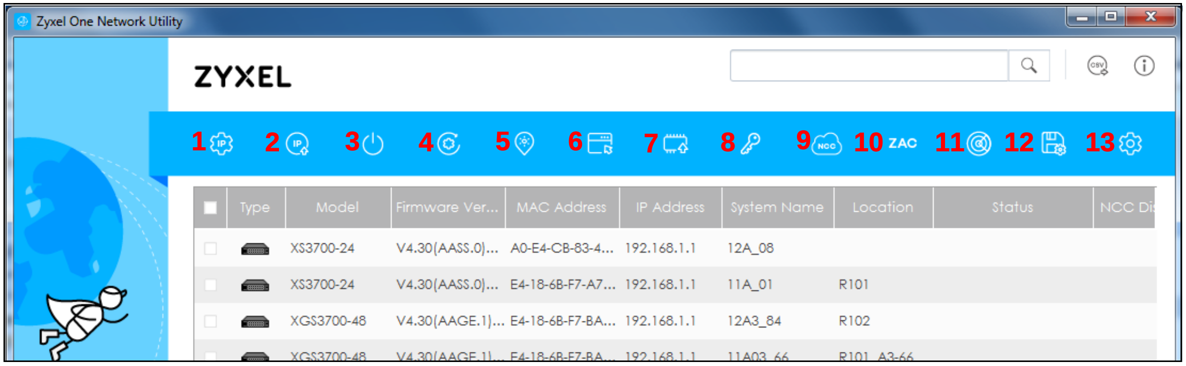
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 551 Discovery



5 The ZON Utility screen shows the devices discovered.

Figure 552 ZON Utility Screen



☐	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	NCC Di
☐		XS3700-24	V4.30(AASS.0)...	A0-E4-CB-83-4...	192.168.1.1	12A_08			
☐		XS3700-24	V4.30(AASS.0)...	E4-18-6B-F7-A7...	192.168.1.1	11A_01	R101		
☐		XGS3700-48	V4.30(AAGE.1)...	E4-18-6B-F7-BA...	192.168.1.1	12A3_84	R102		
☐		XGS3700-48	V4.30(AAGE.1)...	E4-18-6B-F7-BA...	192.168.1.1	11A03_66	R101_A3-66		

6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

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

Table 343 ZON Utility Icons

ICON	DESCRIPTION
1 IP configuration	Change the selected device’s IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.

Table 343 ZON Utility Icons

ICON	DESCRIPTION
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	If you forget your password or cannot access the Web Configurator, you can use this icon to reload the factory-default configuration file. This means that you will lose all configurations that you had previously.
5 Locator LED	Use this icon to locate the selected device by causing its Locator LED to blink.
6 Web GUI	Use this to access the selected device web configurator from your browser. You will need a username and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance. If your Zyxel Device supports dual firmware images, the standby image will be upgraded. After the new firmware is uploaded, you Zyxel Device will reboot, and the new firmware will be the running firmware.
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the cloud management mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adaptor for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 344 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support **IP Configuration**, **Renew IP address** and **Flash Locator LED**, this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.
NCC Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the cloud management mode.

Table 344 ZON Utility Fields

LABEL	DESCRIPTION
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.

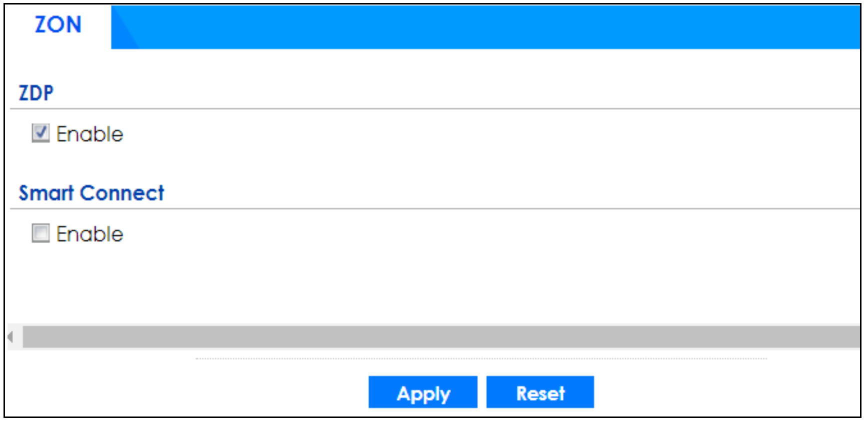
38.17.3 Zyxel One Network (ZON) System Screen

Enable **ZDP** (ZON) and **Smart Connect** (Ethernet Neighbor) in the **System > ZON** screen.

See **Monitor > System Status > Ethernet Neighbor** for information on using **Smart Connect** (Link Layer Discovery Protocol (LLDP)) for discovering and configuring LLDP-aware devices in the same broadcast domain as the Zyxel Device that you're logged into using the web configurator.

The following figure shows the **System > ZON** screen.

Figure 553 Configuration > System > ZON



ZON

ZDP

☑ Enable

Smart Connect

□ Enable

The following table describes the labels in this screen.

Table 345 Configuration > System > ZON

LABEL	DESCRIPTION
ZDP	Zyxel Discovery Protocol (ZDP) is the protocol that the Zyxel One Network (ZON) utility uses for discovering and configuring ZDP-aware Zyxel devices in the same broadcast domain as the computer on which ZON is installed.
Enable	Select to activate ZDP discovery on the Zyxel Device.
Smart Connect	**Smart Connect** uses Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the Zyxel Device that you're logged into using the web configurator.
Enable	Select to activate LLDP discovery on the Zyxel Device. See also **Monitor > System Status > Ethernet Discovery.**
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 39
Log and Report

39.1 Overview

Use these screens to configure daily reporting and log settings.

39.1.1 What You Can Do In this Chapter

- Use the **Email Daily Report** screen (Section 39.2 on page 793) to configure where and how to send daily reports and what reports to send.
- Use the **Log Setting** screens (Section 39.3 on page 795) to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers.

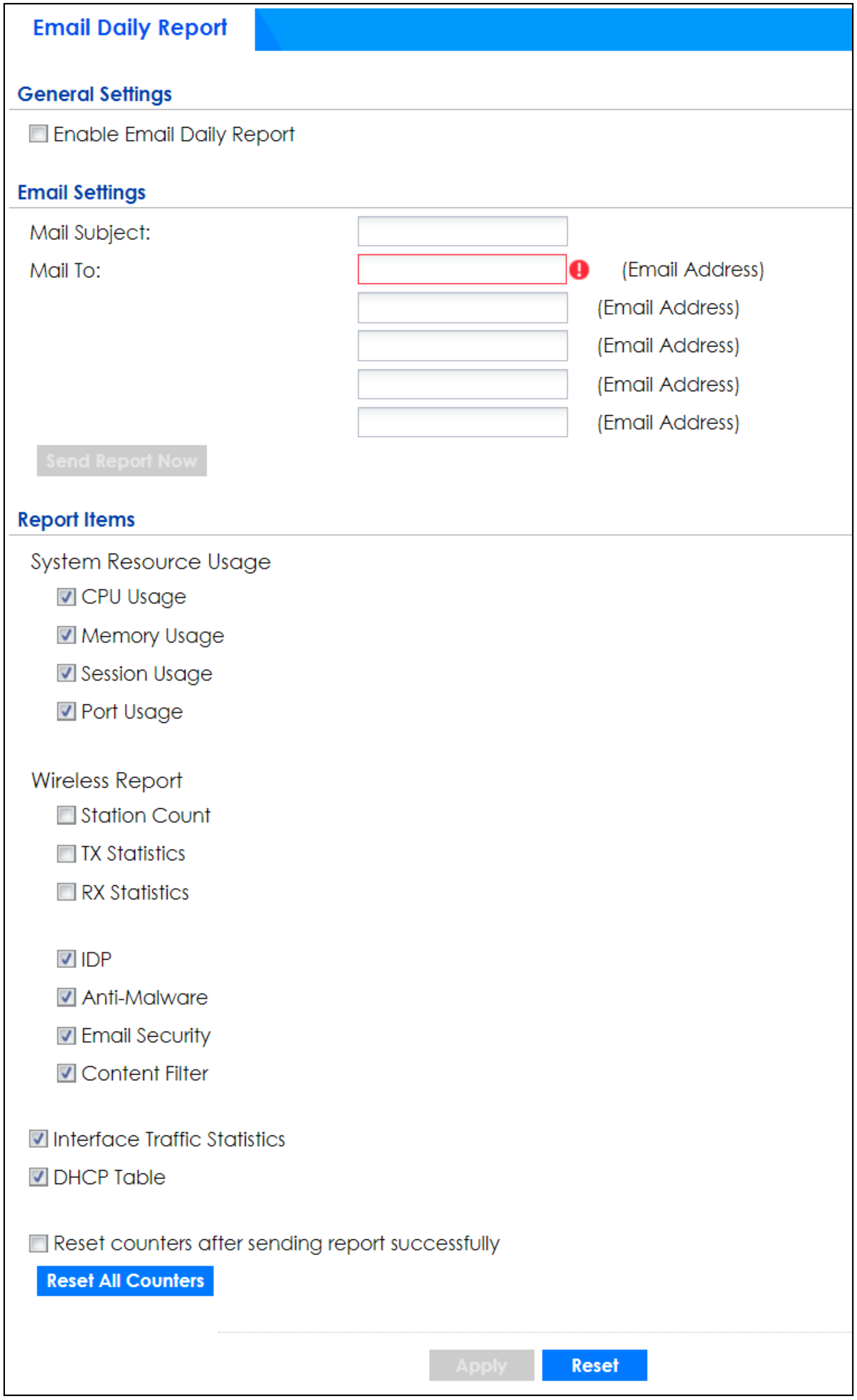
39.2 Email Daily Report

Use the **Email Daily Report** screen to start or stop data collection and view various statistics about traffic passing through your Zyxel Device. See **Configuration > System > Notification** to set up the mail server.

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

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

Figure 554 Configuration > Log & Report > Email Daily Report



Email Daily Report

General Settings

□ Enable Email Daily Report

Email Settings

Mail Subject:		
Mail To:		(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)

Report Items

System Resource Usage

☑ CPU Usage

☑ Memory Usage

☑ Session Usage

☑ Port Usage

Wireless Report

□ Station Count

□ TX Statistics

□ RX Statistics

☑ IDP

☑ Anti-Malware

☑ Email Security

☑ Content Filter

☑ Interface Traffic Statistics

☑ DHCP Table

□ Reset counters after sending report successfully

The following table describes the labels in this screen.

Table 346 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by email every day.
Mail Subject	Type the subject line for outgoing email from the Zyxel Device.

Table 346 Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
Mail To	Type the email address (or addresses) to which the outgoing email is delivered.
Send Report Now	Click this button to have the Zyxel Device send the daily email report immediately.
Report Items	Select the information to include in the report. Types of information include **System Resource Usage**, **Wireless Report**, **Interface Traffic Statistics** and **DHCP Table**. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

39.3 Log Setting Screens

The **Log Setting** screens control log messages and alerts. A log message stores the information for viewing or regular emailing later, and an alert is emailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The Zyxel Device provides a system log and supports email profiles and remote syslog servers. View the system log in the **MONITOR > Log** screen. Use the email profiles to mail log messages to the specific destinations. You can also have the Zyxel Device store system logs on a connected USB storage device. The other four logs are stored on specified syslog servers.

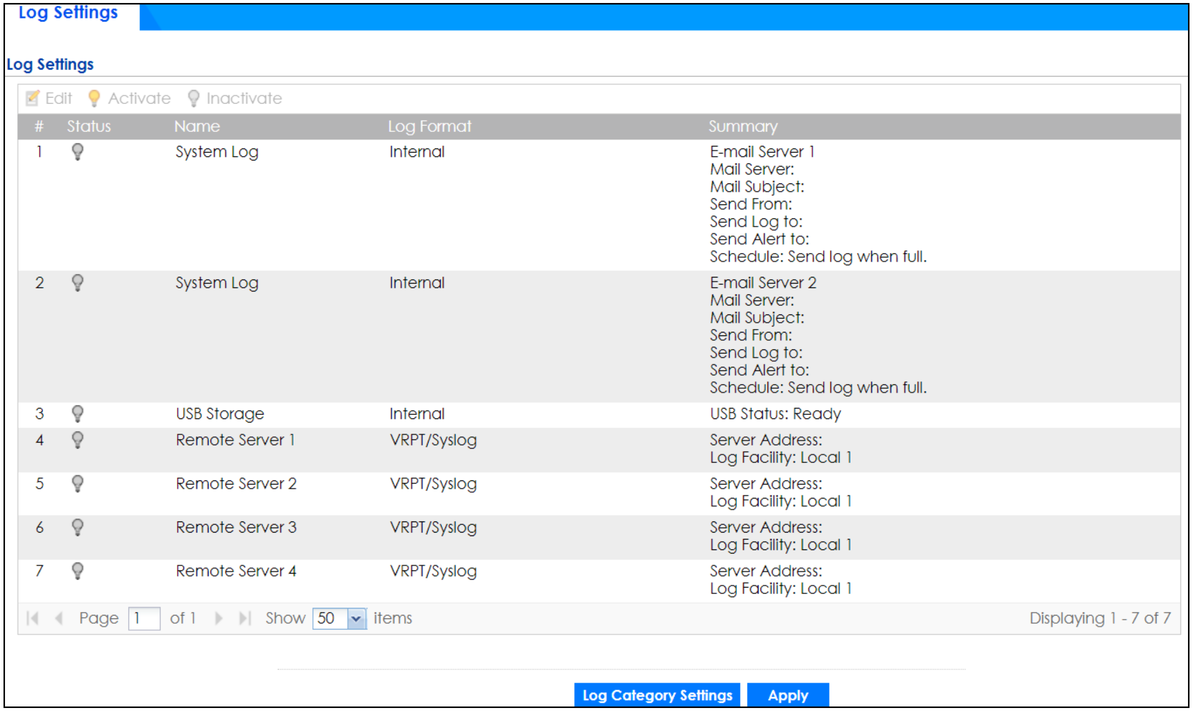
The **Log Setting** screens control what information the Zyxel Device saves in each log. You can also specify which log messages to email for the system log, and where and how often to email them. These screens also set for which events to generate alerts and where to email the alerts.

The first **Log Setting** screen provides a settings summary. Use the **Edit** screens to configure settings such as log categories, email addresses, and server names for any log. Use the **Log Category Settings** screen to edit what information is included in the system log, USB storage, email profiles, and remote servers.

39.3.1 Log Setting Summary

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

Figure 555 Configuration > Log & Report > Log Setting



#	Status	Name	Log Format	Summary
1	💡	System Log	Internal	E-mail Server 1 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
2	💡	System Log	Internal	E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3	💡	USB Storage	Internal	USB Status: Ready
4	💡	Remote Server 1	VRPT/Syslog	Server Address: Log Facility: Local 1
5	💡	Remote Server 2	VRPT/Syslog	Server Address: Log Facility: Local 1
6	💡	Remote Server 3	VRPT/Syslog	Server Address: Log Facility: Local 1
7	💡	Remote Server 4	VRPT/Syslog	Server Address: Log Facility: Local 1

The following table describes the labels in this screen.

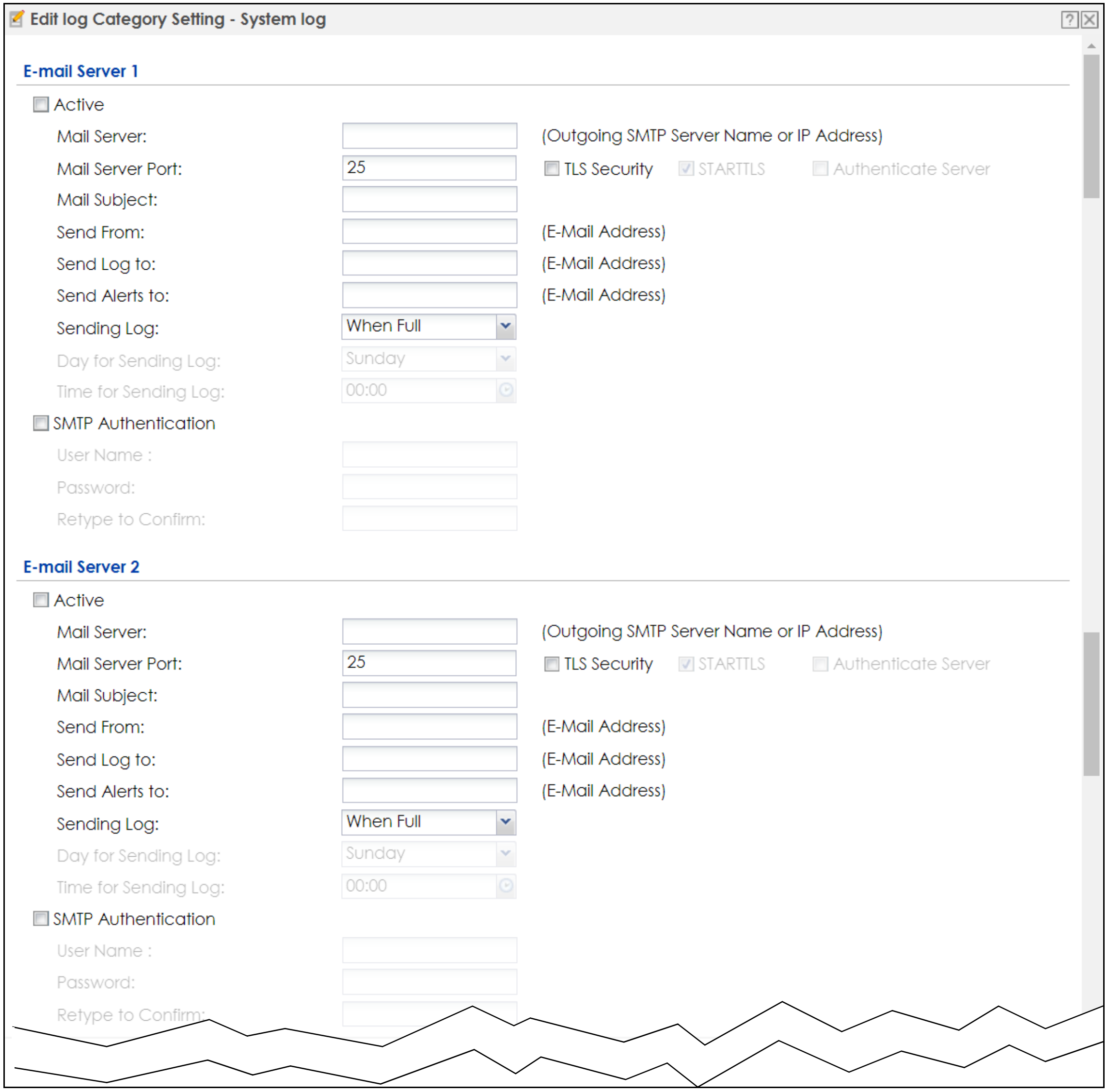
Table 347 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the Zyxel Device, or one of the remote servers).
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 39.3.2 on page 796 for more information.
Log Category Settings	Click this button to open the **Log Category Settings Edit** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

39.3.2 Edit System Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the email profiles). Go to the **Log Settings Summary** screen (see Section 39.3.1 on page 795), and click the system log **Edit** icon.

Figure 556 Configuration > Log & Report > Log Setting > Edit (System Log - E-mail Servers)



Edit log Category Setting - System log

E-mail Server 1

☐ Active

Mail Server:		(Outgoing SMTP Server Name or IP Address)
Mail Server Port:	25	☐ TLS Security ☑ STARTTLS ☐ Authenticate Server
Mail Subject:		
Send From:		(E-Mail Address)
Send Log to:		(E-Mail Address)
Send Alerts to:		(E-Mail Address)
Sending Log:	When Full	
Day for Sending Log:	Sunday	
Time for Sending Log:	00:00	

☐ SMTP Authentication

User Name :	
Password:	
Retype to Confirm:	

E-mail Server 2

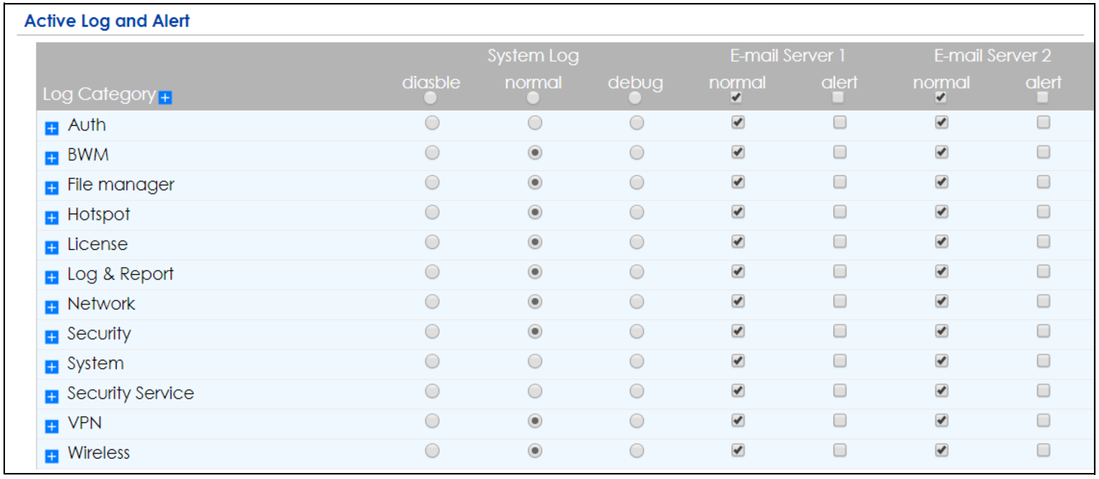
☐ Active

Mail Server:		(Outgoing SMTP Server Name or IP Address)
Mail Server Port:	25	☐ TLS Security ☑ STARTTLS ☐ Authenticate Server
Mail Subject:		
Send From:		(E-Mail Address)
Send Log to:		(E-Mail Address)
Send Alerts to:		(E-Mail Address)
Sending Log:	When Full	
Day for Sending Log:	Sunday	
Time for Sending Log:	00:00	

☐ SMTP Authentication

User Name :	
Password:	
Retype to Confirm:	

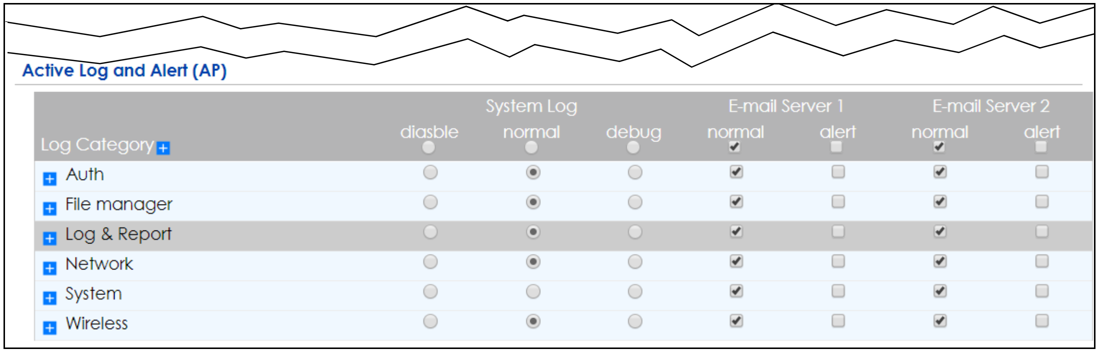
Figure 557 Configuration > Log & Report > Log Setting > Edit (System Log)



Active Log and Alert

	System Log			E-mail Server 1		E-mail Server 2	
Log Category	diasble ○	normal ○	debug ○	normal ☑	alert ☐	normal ☑	alert ☐
Auth	○	○	○	☑	☐	☑	☐
BWM	○	●	○	☑	☐	☑	☐
File manager	○	●	○	☑	☐	☑	☐
Hotspot	○	●	○	☑	☐	☑	☐
License	○	●	○	☑	☐	☑	☐
Log & Report	○	●	○	☑	☐	☑	☐
Network	○	●	○	☑	☐	☑	☐
Security	○	●	○	☑	☐	☑	☐
System	○	○	○	☑	☐	☑	☐
Security Service	○	○	○	☑	☐	☑	☐
VPN	○	●	○	☑	☐	☑	☐
Wireless	○	●	○	☑	☐	☑	☐

Figure 558 Configuration > Log & Report > Log Setting > Edit (System Log - AP)



Active Log and Alert (AP)

	System Log			E-mail Server 1		E-mail Server 2	
Log Category	diasble ○	normal ○	debug ○	normal ☑	alert □	normal ☑	alert □
Auth	○	●	○	☑	□	☑	□
File manager	○	●	○	☑	□	☑	□
Log & Report	○	●	○	☑	□	☑	□
Network	○	●	○	☑	□	☑	□
System	○	○	○	☑	□	☑	□
Wireless	○	●	○	☑	□	☑	□

The following table describes the labels in this screen.

Table 348 Configuration > Log & Report > Log Setting > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing email.
Send From	Type the email address from which the outgoing email is delivered. This address is used in replies.
Send Log To	Type the email address to which the outgoing email is delivered.
Send Alerts To	Type the email address to which alerts are delivered.
Sending Log	Select how often log information is emailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is emailed weekly. Select the day of the week the log is emailed.
Time for Sending Log	This field is available if the log is emailed weekly or daily. Select the time of day (hours and minutes) when the log is emailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password of up to 63 characters to provide to the SMTP server when the log is emailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Active Log and Alert	
System Log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.

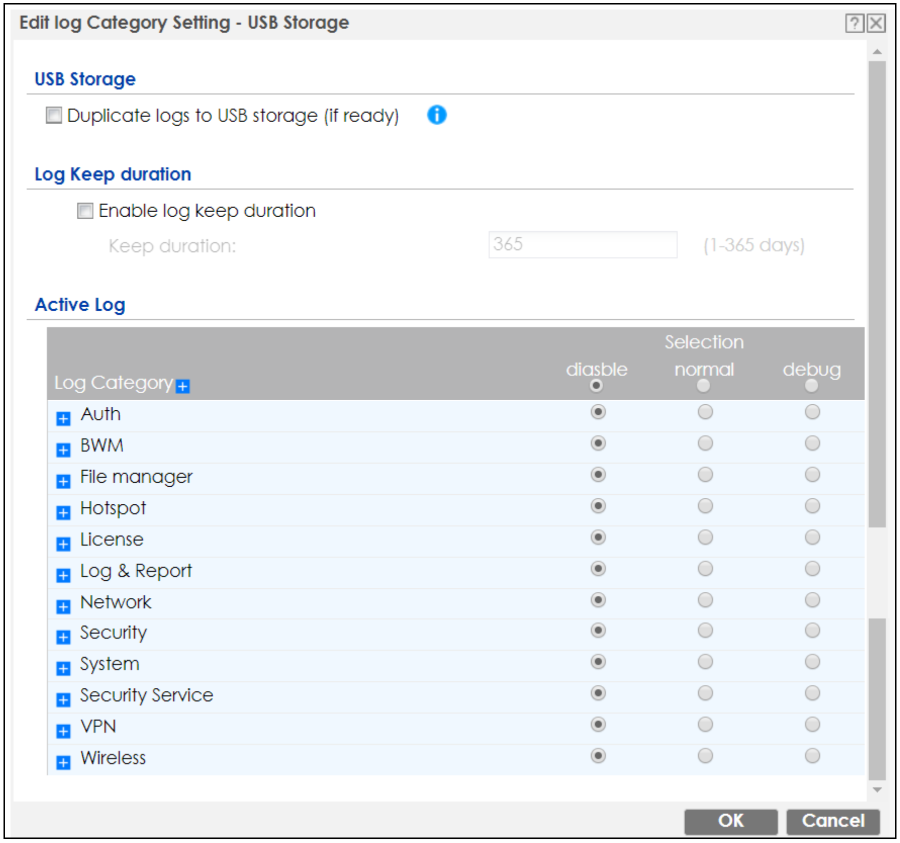
Table 348 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

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

39.3.3 Edit Log on USB Storage Setting

The **Edit Log on USB Storage Setting** screen controls the detailed settings for saving logs to a connected USB storage device. Go to the **Log Setting Summary** screen (see Section 39.3.1 on page 795), and click the USB storage **Edit** icon.

Figure 559 Configuration > Log & Report > Log Setting > Edit (USB Storage)



Edit log Category Setting - USB Storage

USB Storage

□ Duplicate logs to USB storage (if ready)

Log Keep duration

□ Enable log keep duration

Keep duration: 365 (1-365 days)

Active Log

Log Category	diasble	Selection normal	debug
	○	○	○
Auth	●	○	○
BWM	●	○	○
File manager	●	○	○
Hotspot	●	○	○
License	●	○	○
Log & Report	●	○	○
Network	●	○	○
Security	●	○	○
System	●	○	○
Security Service	●	○	○
VPN	●	○	○
Wireless	●	○	○

The following table describes the labels in this screen.

Table 349 Configuration > Log & Report > Log Setting > Edit (USB Storage)

LABEL	DESCRIPTION
Duplicate logs to USB storage (if ready)	Select this to have the Zyxel Device save a copy of its system logs to a connected USB storage device. Use the **Active Log** section to specify what kinds of messages to include.
Enable log keep duration	Select this checkbox to enter a value in the **Keep Duration** field.
Keep Duration	Enter a number of days that the Zyxel Device keeps this log.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.

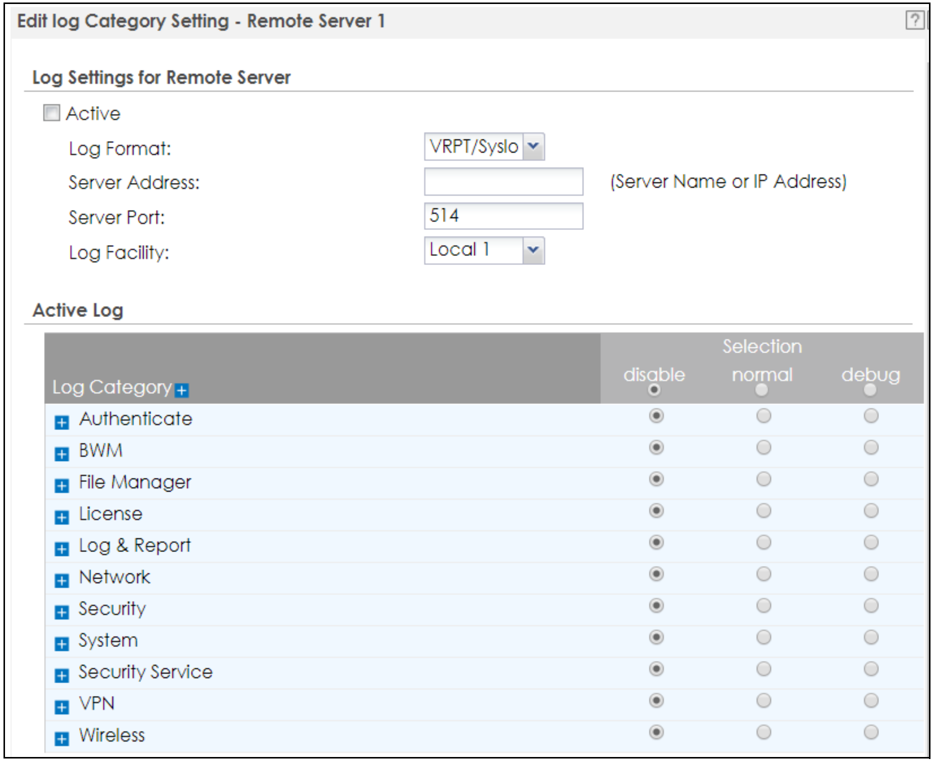
Table 349 Configuration > Log & Report > Log Setting > Edit (USB Storage) (continued)

LABEL	DESCRIPTION
Log Category	This field displays each category of messages. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

39.3.4 Edit Remote Server Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see Section 39.3.1 on page 795), and click a remote server **Edit** icon.

Figure 560 Configuration > Log & Report > Log Setting > Edit (Remote Server - AC)



Edit log Category Setting - Remote Server 1

Log Settings for Remote Server

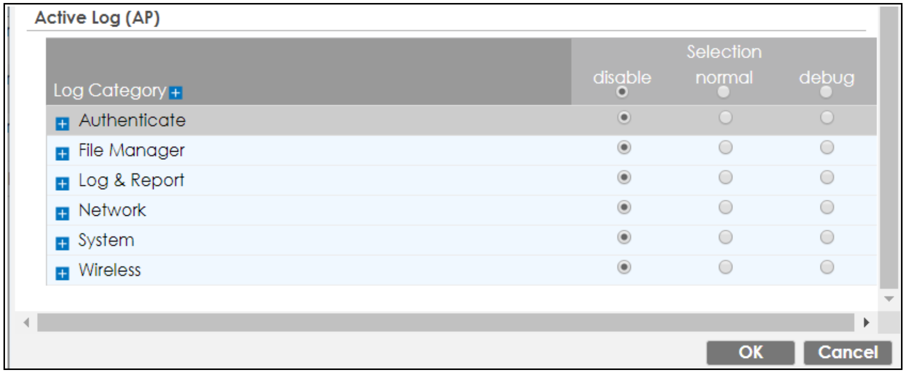
□ Active

Log Format:	VRPT/Syslo	
Server Address:		(Server Name or IP Address)
Server Port:	514	
Log Facility:	Local 1	

Active Log

Log Category	Selection disable ●	 normal ○	 debug ○
Authenticate	●	○	○
BWM	●	○	○
File Manager	●	○	○
License	●	○	○
Log & Report	●	○	○
Network	●	○	○
Security	●	○	○
System	●	○	○
Security Service	●	○	○
VPN	●	○	○
Wireless	●	○	○

Configuration > Log & Report > Log Setting > Edit (Remote Server - AP)



Active Log (AP)

Log Category	Selection disable ●	 normal ○	 debug ○
Authenticate	●	○	○
File Manager	●	○	○
Log & Report	●	○	○
Network	●	○	○
System	●	○	○
Wireless	●	○	○

The following table describes the labels in this screen.

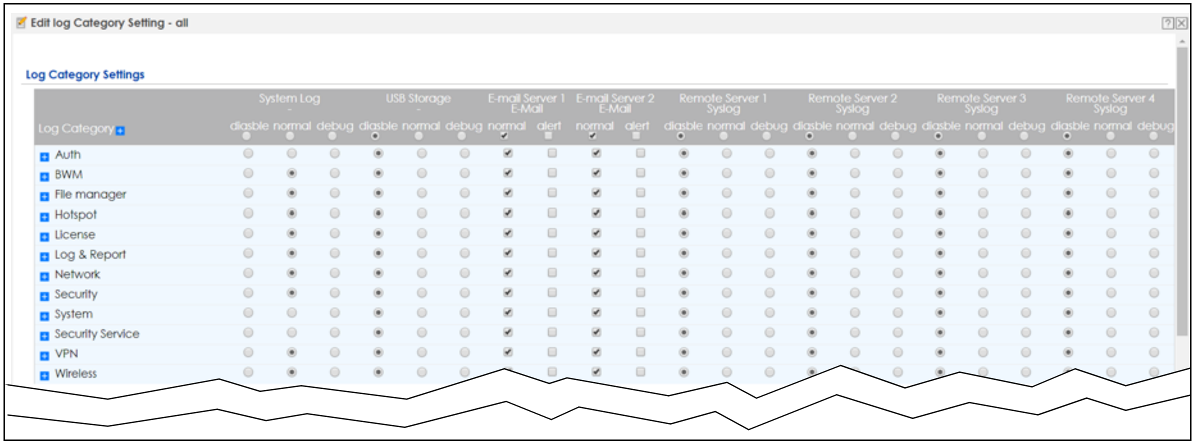
Table 350 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Server Port	Type the service port number used by the remote server.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

39.3.5 Log Category Settings Screen

The **Log Category Settings** screen allows you to view and to edit what information is included in the system log, USB storage, email profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is emailed or remote server names). To access this screen, go to the **Log Settings Summary** screen (see Section 39.3.1 on page 795), and click the **Log Category Settings** button.

Figure 561 Log Category Settings AC

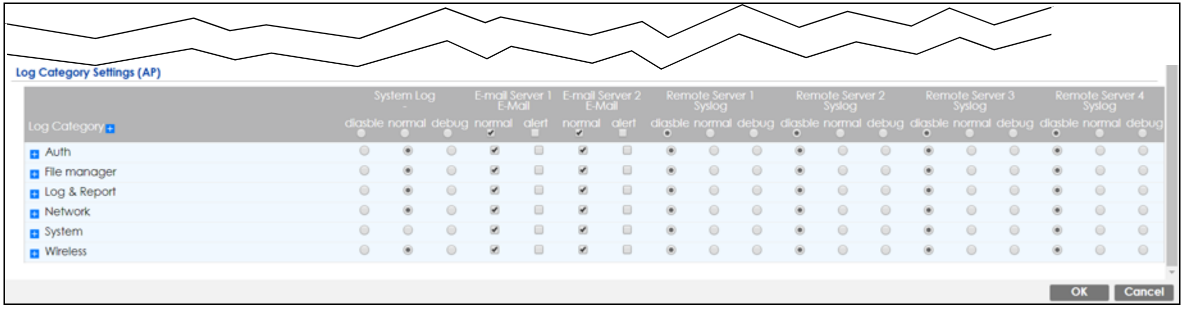


Edit log Category Setting - all

Log Category Settings

	System Log -			USB Storage -			E-mail Server 1 E-Mail		E-mail Server 2 E-Mail		Remote Server 1 Syslog			Remote Server 2 Syslog			Remote Server 3 Syslog			Remote Server 4 Syslog		
	diasble	normal	debug	diasble	normal	debug	normal	alert	normal	alert	diasble	normal	debug	diasble	normal	debug	diasble	normal	debug	diasble	normal	debug
Log Category	○	○	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Auth	○	○	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
BWM	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
File manager	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Hotspot	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
License	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Log & Report	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Network	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Security	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
System	○	○	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Security Service	○	○	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
VPN	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Wireless	○	●	○	●	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○

Figure 562 Log Category Settings AP



Log Category Settings (AP)

	System Log -			E-mail Server 1 E-Mail		E-mail Server 2 E-Mail		Remote Server 1 Syslog			Remote Server 2 Syslog			Remote Server 3 Syslog			Remote Server 4 Syslog		
	diasble	normal	debug	normal	alert	normal	alert	diasble	normal	debug	diasble	normal	debug	diasble	normal	debug	diasble	normal	debug
Log Category	○	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Auth	○	●	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
File manager	○	●	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Log & Report	○	●	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Network	○	●	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
System	○	○	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○
Wireless	○	●	○	☑	□	☑	□	●	○	○	●	○	○	●	○	○	●	○	○

This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 39.3.2 on page 796, where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 351 Configuration > Log & Report > Log Setting > Log Category Settings

LABEL	DESCRIPTION
System Log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.
USB Storage	Use the **USB Storage** drop-down list to change the log settings for saving logs to a connected USB storage device. **disable all logs** (red X) - do not log any information for any category to a connected USB storage device. **enable normal logs** (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.
E-mail Server 1 E-mail	Use the **E-Mail Server 1** drop-down list to change the settings for emailing logs to email server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your email server 1 settings. **enable normal logs** (green check mark) - email log messages for all categories to email server 1. **enable alert logs** (red exclamation point) - email alerts for all categories to email server 1.
E-mail Server 2 E-mail	Use the **E-Mail Server 2** drop-down list to change the settings for emailing logs to email server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your email server 2 settings. **enable normal logs** (green check mark) - email log messages for all categories to email server 2. **enable alert logs** (red exclamation point) - email alerts for all categories to email server 2.
Remote Server 1~4 Syslog	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System Log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.

Table 351 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

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

CHAPTER 40
File Manager

40.1 Overview

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

40.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see Section 40.2 on page 808) to store and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.
- Use the **Firmware Package** screen (see Section 40.3 on page 812) to check your current firmware version and upload firmware to the Zyxel Device.
- Use the **Shell Script** screen (see Section 40.4 on page 818) to store, name, download, upload and run shell script files.

40.1.2 What you Need to Know

Configuration Files and Shell Scripts

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

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

Figure 563 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

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

Table 352 Configuration Files and Shell Scripts in the Zyxel Device

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

You have to run the example in Figure 563 on page 807 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the Zyxel Device treat the line as a comment.

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

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

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface ge1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

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

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

40.2 The Configuration File Screen

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

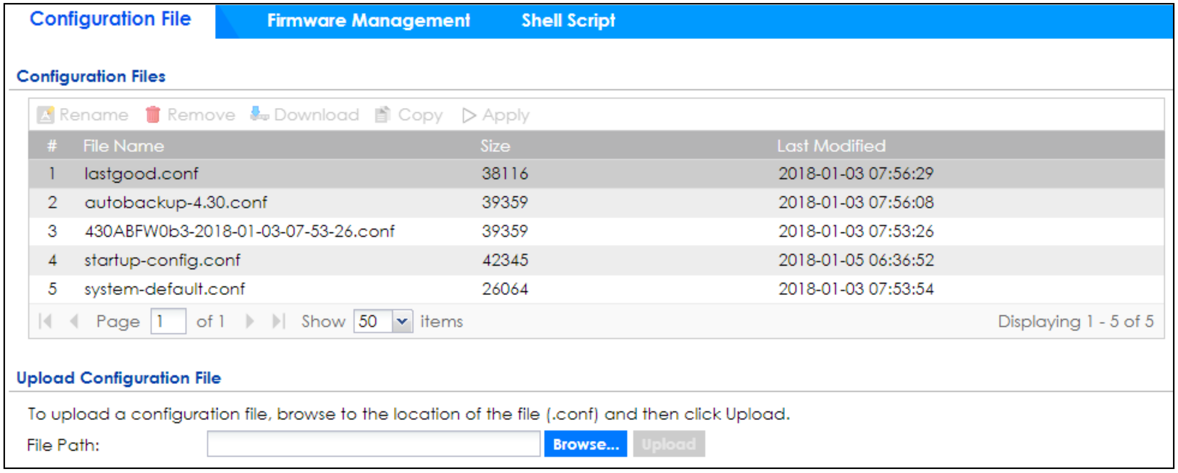
Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Filenames beginning with autoback are automatic configuration files created when new firmware is uploaded. backup-yyyy-mm-dd-hh-mm-ss.conf is the name of the automatic backup when a secure policy is added or changed. Select a configuration file, then click **Apply** to apply the file to the Zyxel Device .

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Figure 564 Maintenance > File Manager > Configuration File



#	File Name	Size	Last Modified
1	lastgood.conf	38116	2018-01-03 07:56:29
2	autobackup-4.30.conf	39359	2018-01-03 07:56:08
3	430ABFW0b3-2018-01-03-07-53-26.conf	39359	2018-01-03 07:53:26
4	startup-config.conf	42345	2018-01-05 06:36:52
5	system-default.conf	26064	2018-01-03 07:53:54

Page 1 of 1 Show 50 items Displaying 1 - 5 of 5

Upload Configuration File

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path:

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

The following table describes the labels in this screen.

Table 353 Maintenance > File Manager > Configuration File

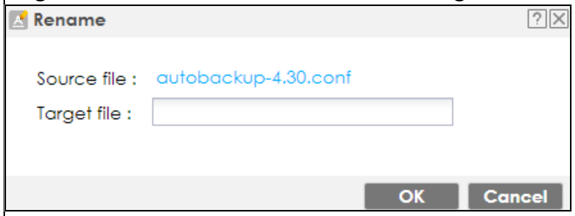
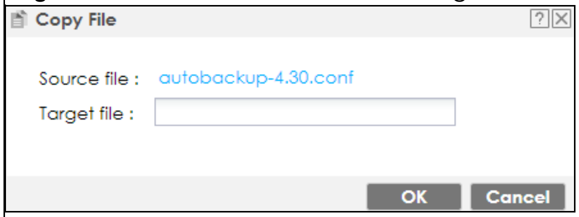
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the Zyxel Device. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen. **Figure 565** Maintenance > File Manager > Configuration File > Rename  Rename Source file : autobackup-4.30.conf Target file : Specify the new name for the configuration file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen. **Figure 566** Maintenance > File Manager > Configuration File > Copy  Copy File Source file : autobackup-4.30.conf Target file : Specify a name for the duplicate configuration file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 353 Maintenance > File Manager > Configuration File (continued)

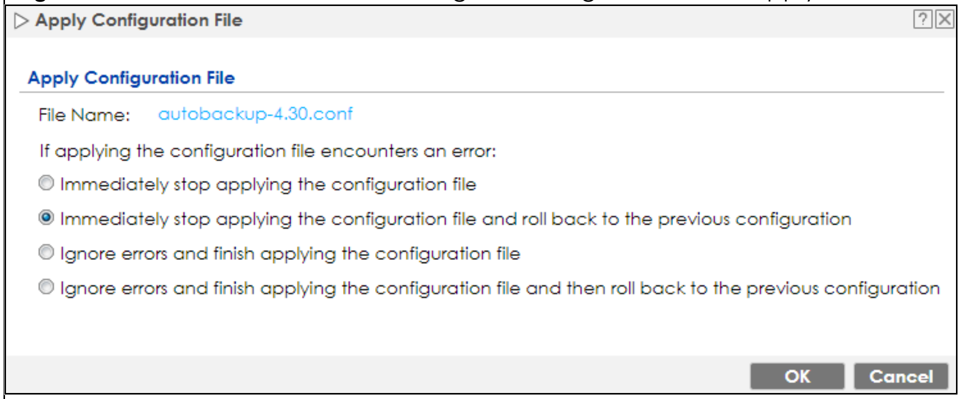
LABEL	DESCRIPTION
Apply	Use this button to have the Zyxel Device use a specific configuration file. Click a configuration file’s row to select it and click **Apply** to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file. **Figure 567** Maintenance > File Manager > Configuration File > Apply  ▷ Apply Configuration File Apply Configuration File File Name: autobackup-4.30.conf If applying the configuration file encounters an error: ○ Immediately stop applying the configuration file ● Immediately stop applying the configuration file and roll back to the previous configuration ○ Ignore errors and finish applying the configuration file ○ Ignore errors and finish applying the configuration file and then roll back to the previous configuration **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file’s errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file’s errors, and starts the Zyxel Device with a fully valid configuration file. Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the Zyxel Device’s default settings. Select this file and click **Apply** to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.

Table 353 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

40.3 Firmware Management

Use the **Firmware Management** screen to check your current firmware version and upload firmware to the Zyxel Device. You can upload firmware to be the **Running** firmware or **Standby** firmware.

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

Find the firmware file in a folder that (usually) uses the system model name with the model code and a bin extension. For example, a firmware for ZyWALL VPN100 is "430ABFV0b2s1.bin".

The Zyxel Device's firmware package cannot go through the Zyxel Device when you enable the anti-malware **Destroy compressed files that could not be decompressed** option. The Zyxel Device classifies the firmware package as not being able to be decompressed and deletes it. You can upload the firmware package to the Zyxel Device with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 28.2 on page 548 for more on the anti-malware **Destroy compressed files that could not be decompressed** option.

The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!

If your Zyxel Device has two firmware images installed, and one fails to boot (kernel crash, kernel panic, out-of-memory etc.), then the Zyxel Device will automatically use the (good) backup image to boot.

40.3.1 Cloud Helper

Cloud Helper lets you know if there is a later firmware available on the Cloud Helper server and lets you download it if there is.

Note: Go to myZyxel, create an account and register your Zyxel Device first. Then you will be able to see links to and get notifications on new firmware available.

At the time of writing, the Firmware Upgrade license providing Cloud Helper new firmware notifications is free when you register your Zyxel Device. The license does not expire if you have firmware version 4.32 patch 1 and later.

The following table explains the **Upgrade** icons in the web configurator.

Table 354 Cloud Helper Firmware Icons

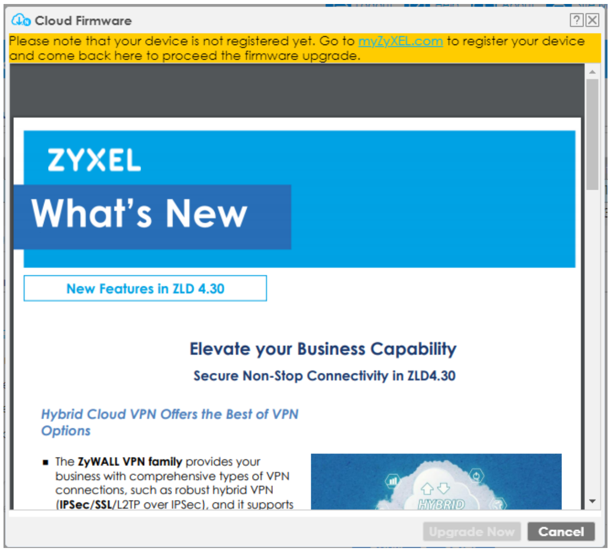
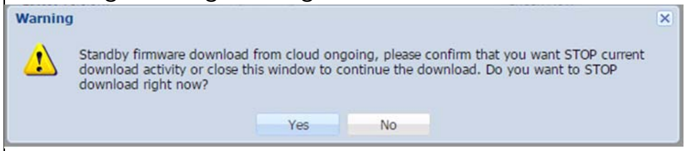
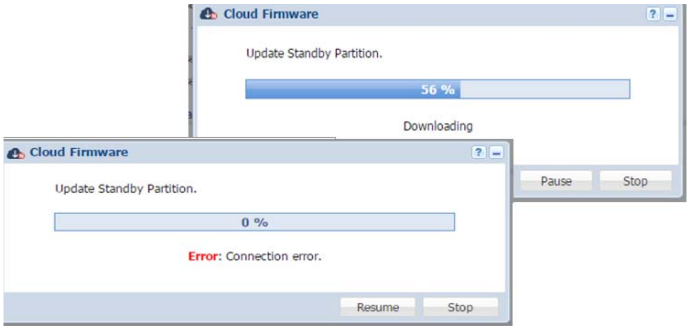
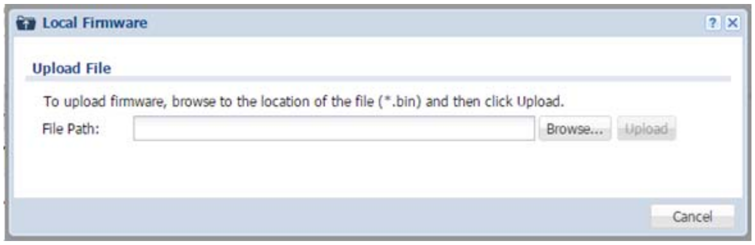
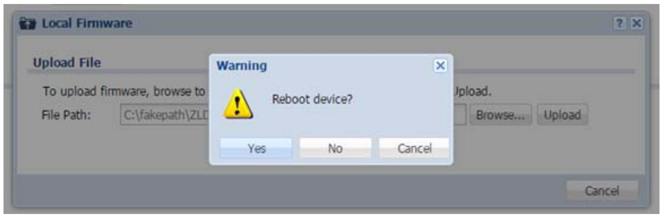
Cloud Helper New	A later firmware is available on the Cloud Helper Server. Click this icon to display a **What's New** pop-up screen. You need a Firmware Upgrade license to upgrade the firmware. If you do not have a license, **Upgrade Now** is grayed out. If you have a license, click **Upgrade Now** to directly upgrade firmware to the standby partition and have the Zyxel Device reboot automatically so that the new standby firmware becomes the running firmware. The previous running firmware becomes the standby firmware. If you haven't registered the Zyxel Device, a message will appear and remind you to register it. Also, **Upgrade Now** is grayed out.  Cloud Firmware Please note that your device is not registered yet. Go to myZyXEL.com to register your device and come back here to proceed the firmware upgrade. ZYXEL What's New New Features in ZLD 4.30 Elevate your Business Capability Secure Non-Stop Connectivity in ZLD4.30 *Hybrid Cloud VPN Offers the Best of VPN Options* ■ The **ZyWALL VPN family** provides your business with comprehensive types of VPN connections, such as robust hybrid VPN (**IPSec**/**SSL**/L2TP over IPSec), and it supports

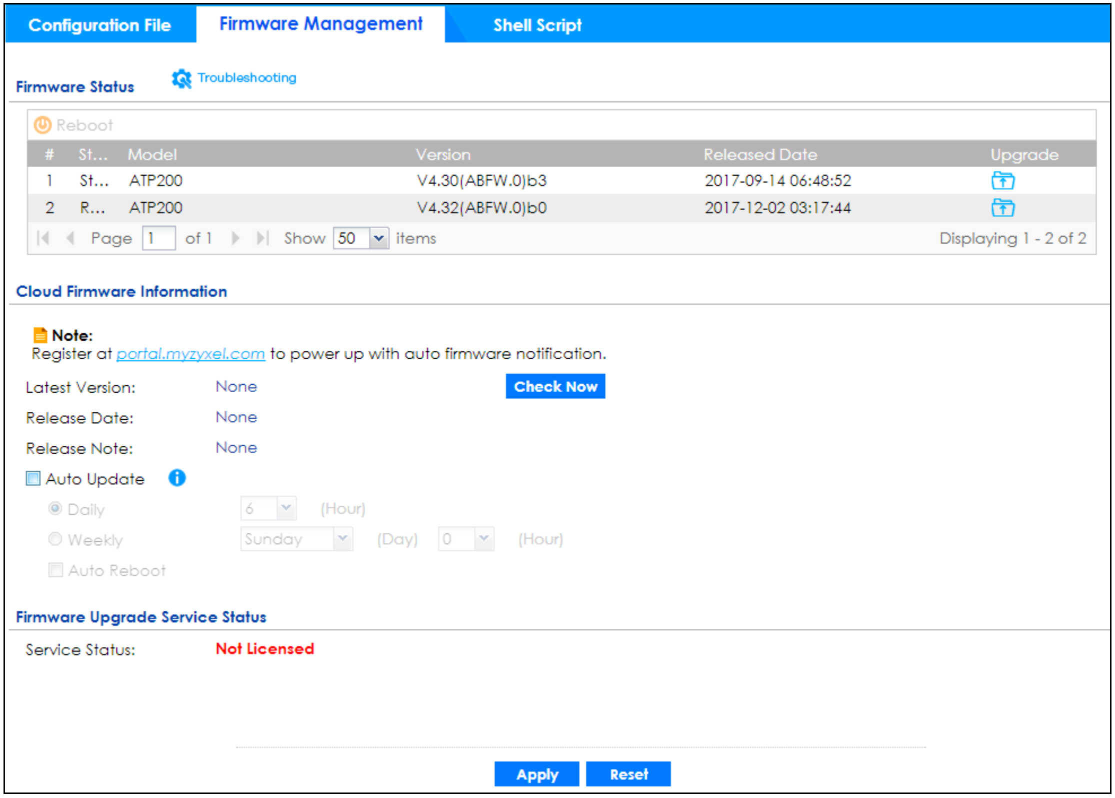
Table 354 Cloud Helper Firmware Icons

Cloud Helper Downloading	Cloud firmware is being downloaded from the Cloud Helper Server. If you select another partition or the local firmware upgrade icon, you will see the following warning message.  Warning Standby firmware download from cloud ongoing, please confirm that you want STOP current download activity or close this window to continue the download. Do you want to STOP download right now? When firmware is downloading, you can pause, resume, stop or retry the firmware download.  Cloud Firmware Update Standby Partition. 56 % Downloading Cloud Firmware Update Standby Partition. 0 % Error: Connection error.
Local Firmware	Use this if you have already downloaded the latest firmware from the Zyxel website to your computer and unzipped it. Click the icon and then browse to the location of the unzipped files.  Local Firmware Upload File To upload firmware, browse to the location of the file (*.bin) and then click Upload. File Path: If you upload the latest firmware to the running partition, the Zyxel Device will reboot automatically when it finishes uploading. If you upload the latest firmware to the standby partition, a message will appear to ask if you want to reboot the Zyxel Device.  Local Firmware Upload File To upload firmware, browse to ... Upload. File Path: C:\fakepath\ZLD Warning Reboot device?

40.3.2 The Firmware Management Screen

Click **Maintenance > File Manager > Firmware Management** to open the **Firmware Management** screen.

Figure 568 Maintenance > File Manager > Firmware Management



Firmware Status

#	St...	Model	Version	Released Date	Upgrade
1	St...	ATP200	V4.30(ABFW.0)b3	2017-09-14 06:48:52	
2	R...	ATP200	V4.32(ABFW.0)b0	2017-12-02 03:17:44	

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Cloud Firmware Information

Note:
Register at portal.myzyxel.com to power up with auto firmware notification.

Latest Version: None

Release Date: None

Release Note: None

□ Auto Update

● Daily 6 (Hour)

○ Weekly Sunday (Day) 0 (Hour)

□ Auto Reboot

Firmware Upgrade Service Status

Service Status: Not Licensed

The following table describes the labels in this screen.

Table 355 Maintenance > File Manager > Firmware Management

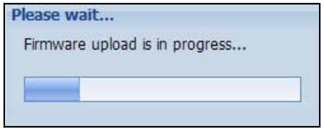
LABEL	DESCRIPTION
Firmware Status	
Reboot	Click the **Reboot** icon to restart the Zyxel Device. If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot. If you want the **Standby** firmware to be the **Running** firmware, then select the **Standby** firmware row and click **Reboot**. Wait a few minutes until the login screen appears. If the login screen does not appear, clear your browser cache and refresh the screen or type the IP address of the Zyxel Device in your Web browser again. You can also use the CLI command `reboot` to restart the Zyxel Device.
#	This displays the system space (partition) index number where the firmware is located. The firmware can be either **Standby** or **Running**; only one firmware can be running at any one time.
Status	This indicates whether the firmware is **Running**, or not running but already uploaded to the Zyxel Device and is on **Standby**. It displays **N/A** if there is no firmware uploaded to that system space.
Model	This is the model name of the device which the firmware is running on.
Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.

Table 355 Maintenance > File Manager > Firmware Management (continued)

LABEL	DESCRIPTION
Upgrade	A cloud helper icon displays if there is a later firmware on the Cloud Server than the firmware in the partition. Click the cloud helper icon to download a later firmware from the Cloud Helper Server. Use the local firmware icon if you have already downloaded the latest firmware from the Zyxel website to your computer and unzipped it.
Cloud Firmware Information	You must register your Zyxel Device at myZyxel first to use cloud firmware.
Latest Version	This displays the latest firmware version at the Cloud Helper Server. Click **Check Now** to see if there is a later firmware at the Cloud Server.
Release Date	This displays the date the latest firmware version was made available.
Release Note	The release note contains details of latest firmware version such as new features and bug fixes.
Auto Update	Select this check box to have the Zyxel Device automatically check for and download new firmware to the standby partition at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Daily	Select this option to have the Zyxel Device check for new firmware every day at the specified time. The time format is the 24 hour clock, so '0' means midnight for example.
Weekly	Select this option to have the Zyxel Device check for new firmware once a week on the day and at the time specified.
Auto Reboot	Select this to have the newly downloaded firmware in the standby partition become the running firmware after the Zyxel Device automatically restarts.
Firmware Upgrade Service Status	
Service Status	This field displays whether the firmware license service is activated at myZyxel (**Activated**) or not (**Not Activated**).

After you see the **Firmware Upload in Process** screen, wait a few minutes before logging into the Zyxel Device again.

Figure 569 Firmware Upload In Process



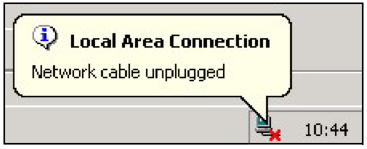
Please wait...

Firmware upload is in progress...

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

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

Figure 570 Network



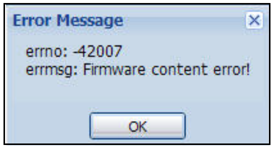
Local Area Connection

Network cable unplugged

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

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 571 Firmware Upload Error



Error Message

errno: -42007
errmsg: Firmware content error!

40.3.3 Firmware Upgrade via USB Stick

In addition to uploading firmware via the web configurator or console port (see the CLI Reference Guide), you can also upload firmware directly from a USB stick connected to the Zyxel Device.

1 Create a folder on the USB stick called '/[ProductName_dir]/firmware'. For example, if your Zyxel Device is USG110, then create a '/usg110_dir/firmware/' folder on the stick.

2 Put one firmware 'bin' file into the firmware folder. Make sure the firmware ID and version number are correct for your model (the firmware ID is in brackets after the firmware version number - for USG100 it is AAPH).

Note: Do not put more than one firmware 'bin' file into the firmware folder.

The firmware version in the USB stick must be different to the currently running firmware. If the firmware on the USB stick is older, then the Zyxel Device will 'upgrade' to the older version. It is recommended that the firmware on the USB stick be the latest firmware version.

3 Insert the USB stick into the Zyxel Device. The firmware uploads to the standby system space.

4 The **SYS** LED blinks when the Zyxel Device automatically reboots making the upgraded firmware in standby become the running firmware.

Note: If the **startup-config.conf** configuration file has problems and you are upgrading to 4.25 or later firmware, then the Zyxel Device will revert (failover) to the previously running firmware.

If the **startup-config.conf** configuration file has problems and you are upgrading to earlier than 4.25 firmware, then the Zyxel Device uses the new earlier firmware, but generates a log and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.

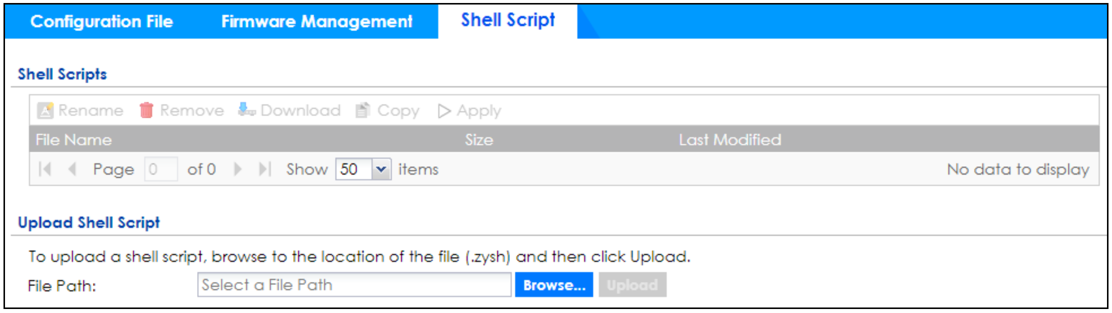
40.4 The Shell Script Screen

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

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

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

Figure 572 Maintenance > File Manager > Shell Script



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

Each field is described in the following table.

Table 356 Maintenance > File Manager > Shell Script

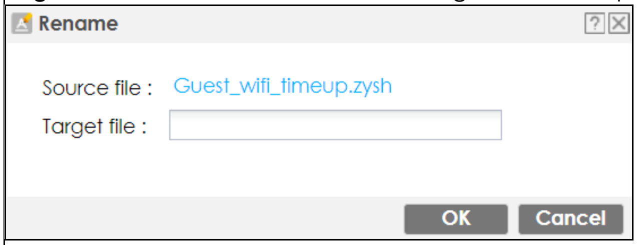
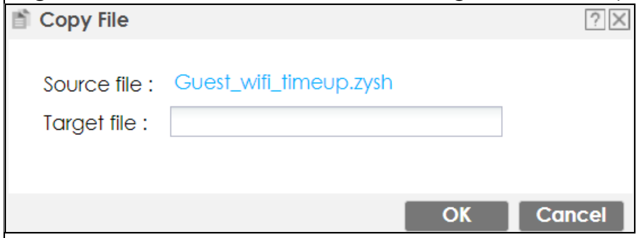
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. **Figure 573** Maintenance > File Manager > Shell Script > Rename  Source file : Guest_wifi_timeup.zysh Target file : Specify the new name for the shell script file. Use up to 63 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Remove** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.

Table 356 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. **Figure 574** Maintenance > File Manager > Shell Script > Copy Copy File Source file : Guest_wifi_timeup.zysh Target file : Specify a name for the duplicate file. Use up to 63 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click **Apply** to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

CHAPTER 41 Diagnostics

41.1 Overview

Use the diagnostics screens for troubleshooting.

41.1.1 What You Can Do in this Chapter

- Use the **Diagnostics** screens (see Section 41.2 on page 821) to generate a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the **Packet Capture** screens (see Section 41.3 on page 825) to capture packets going through the Zyxel Device.
- Use the **CPU / Memory Status** screens (see Section 41.4 on page 832) to view the CPU and memory performance of various applications on the Zyxel Device.
- Use the **System Logs** screen (see Section 41.5 on page 834) to see system logs stored on a connected USB storage device on the Zyxel Device.
- Use the **Remote Assistance** screens (see Section 41.6 on page 834) to configure and schedule external access to the Zyxel Device for troubleshooting.
- Use the **Network Tool** screen (see Section 41.7 on page 836) to ping an IP address or trace the route packets take to a host.
- Use the **Routing Traces** screens (see Section 41.8 on page 838) to configure traceroute to identify where packets are dropped for troubleshooting.
- Use the **Wireless Frame Capture** screens (see Section 41.9 on page 839) to capture network traffic going through the AP interfaces connected to your Zyxel Device.

41.2 The Diagnostics Screens

The **Diagnostics** screens provide an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics** to open the **Diagnostics** screens.

41.2.1 The Diagnostics Collect Screen

When you click **Collect Now**, a series of commands are run to display information about the Zyxel Device. This is an example of a default script with interface diagnostic commands.

```
debug interface ifconfig
debug interface show event_sink
debug interface show interface_obj
debug switch table
debug switch port_groupping
show ping-check status
debug system netstat interface
show interface all
show port status
```

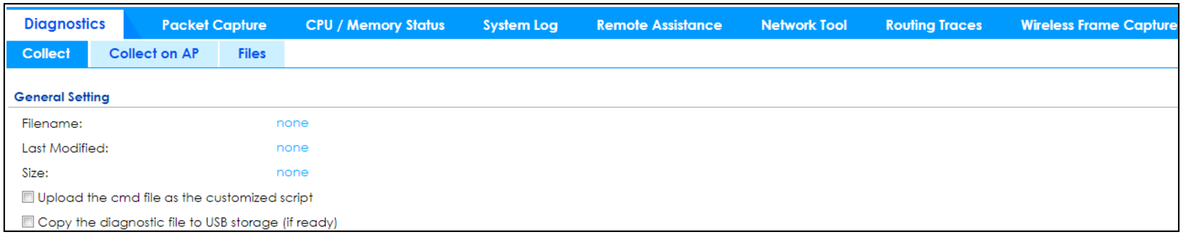
You can also create your own script to display information about the Zyxel Device. This is an example of a customized **Diagnostics > Collect** script.

```
show service-register status all
show myzyxel-service get-cloud-timezone
show cloud-helper firmware
show cloud-helper remind
```

Note: A script created in **File Manager > Shell Script** is used to run commands on the Zyxel Device. A script created in **Diagnostics > Collect** is used to display information about the Zyxel Device only. Both use a ".zysh" filename extension with a file name of up to 25 characters (including a-z, A-Z, 0-9 and ;'~!@#$%^&()_+[]{}',.=-). Spaces are allowed.

Click **Maintenance > Diagnostics > Collect** to open the **Collect** screen.

Figure 575 Maintenance > Diagnostics > Collect



General Setting

Filename: none

Last Modified: none

Size: none

□ Upload the cmd file as the customized script

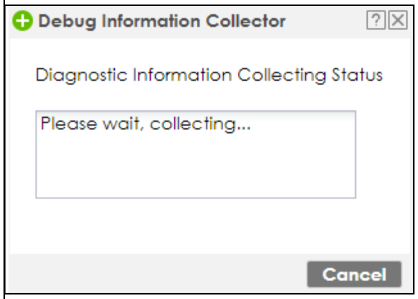
□ Copy the diagnostic file to USB storage (if ready)

The following table describes the labels in this screen.

Table 357 Maintenance > Diagnostics > Collect

LABEL	DESCRIPTION
General Setting	
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Upload the cmd file as the customized script	Select this to upload a customized shell script to display information about the Zyxel Device. Use a text editor to create the shell script files. They must use a ".zysh" filename extension. Specify the new name for the shell script file. Use up to 25 characters (including a-z, A-Z, 0-9 and ;'~!@#$%^&()_+[]{}',.=-). Spaces are allowed.

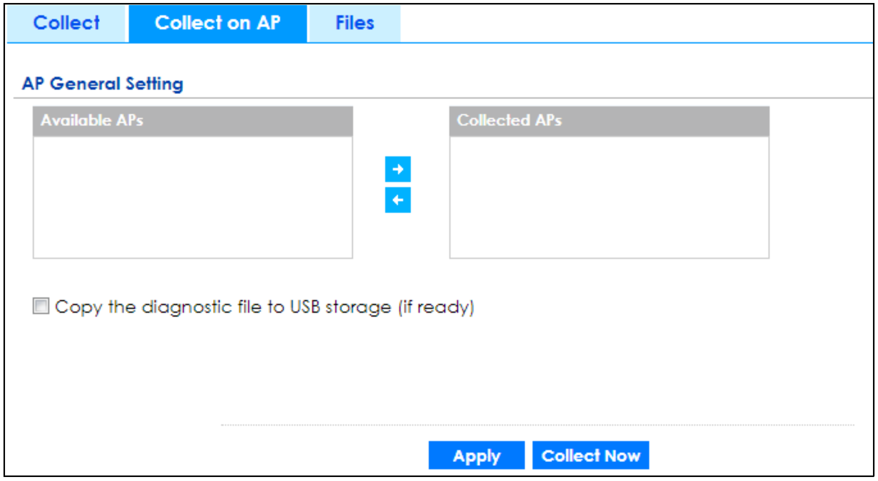
Table 357 Maintenance > Diagnostics > Collect (continued)

LABEL	DESCRIPTION
Copy the diagnostic file to USB storage (if ready)	Select this to have the Zyxel Device create an extra copy of the diagnostic file to a connected USB storage device.
Select **Upload the cmd file as the customized script** to display the following fields.	
Shell Scripts	
Filename	This displays the names of the customized shell script you created.
Upload Shell Script	
File Path	Click **Browse** to find the location of the file you want to upload in this field. Click **Upload** to begin the upload process. This process may take a few minutes.
Apply	Click **Apply** to save your changes.
Collect Now	Click this to have the Zyxel Device create a new diagnostic file. Wait while information is collected.  Debug Information Collector Diagnostic Information Collecting Status Please wait, collecting... Cancel

41.2.2 The Diagnostics Collect on AP Screen

This screen provides an easy way for you to generate a file containing the selected managed AP's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. Click **Maintenance > Diagnostics > Collect on AP** to open the **Collect on AP** screen.

Figure 576 Maintenance > Diagnostics > Collect on AP



☐ Copy the diagnostic file to USB storage (if ready)

The following table describes the labels in this screen.

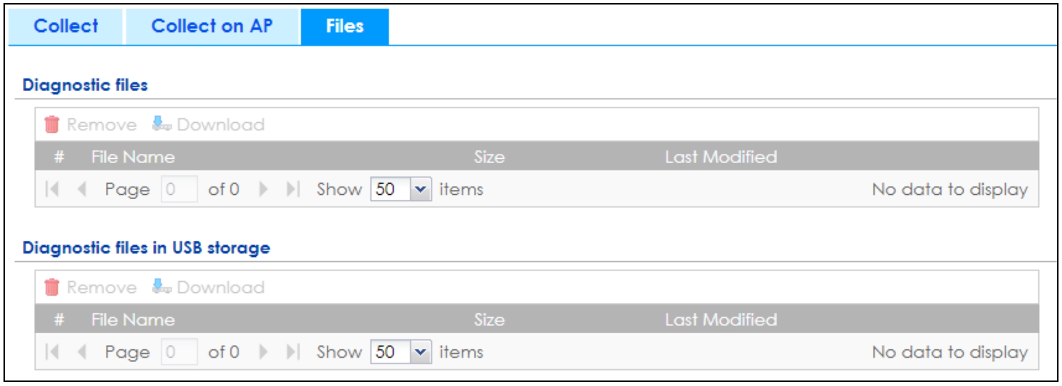
Table 358 Maintenance > Diagnostics > Collect on AP

LABEL	DESCRIPTION
AP General Setting	
Available APs	This text box lists the managed APs that are connected and available. Select the managed APs that you want the Zyxel Device to generate a diagnostic file containing their configuration, and click the right arrow button to add them.
Collected APs	This text box lists the managed APs that you allow the Zyxel Device to generate a diagnostic file containing their configuration. Select any managed APs that you want to prevent the Zyxel Device from generating a diagnostic file for them, and click the left arrow button to remove them.
Copy the diagnostic file to USB storage (if ready)	Select this to have the Zyxel Device create an extra copy of the diagnostic file to a connected USB storage device.
Apply	Click **Apply** to save your changes.
Collect Now	Click this to have the Zyxel Device create a new diagnostic file.

41.2.3 The Diagnostics Files Screen

Click **Maintenance > Diagnostics > Files** to open the diagnostic files screen. This screen lists the files of diagnostic information the Zyxel Device has collected and stored on the Zyxel Device or in a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 577 Maintenance > Diagnostics > Files



The following table describes the labels in this screen.

Table 359 Maintenance > Diagnostics > Files

LABEL	DESCRIPTION
Diagnostic files	This lists the files of diagnostic information stored on the Zyxel Device.
Diagnostic files in USB storage	This lists the files of diagnostic information stored in a connected USB storage device.
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.

Table 359 Maintenance > Diagnostics > Files (continued)

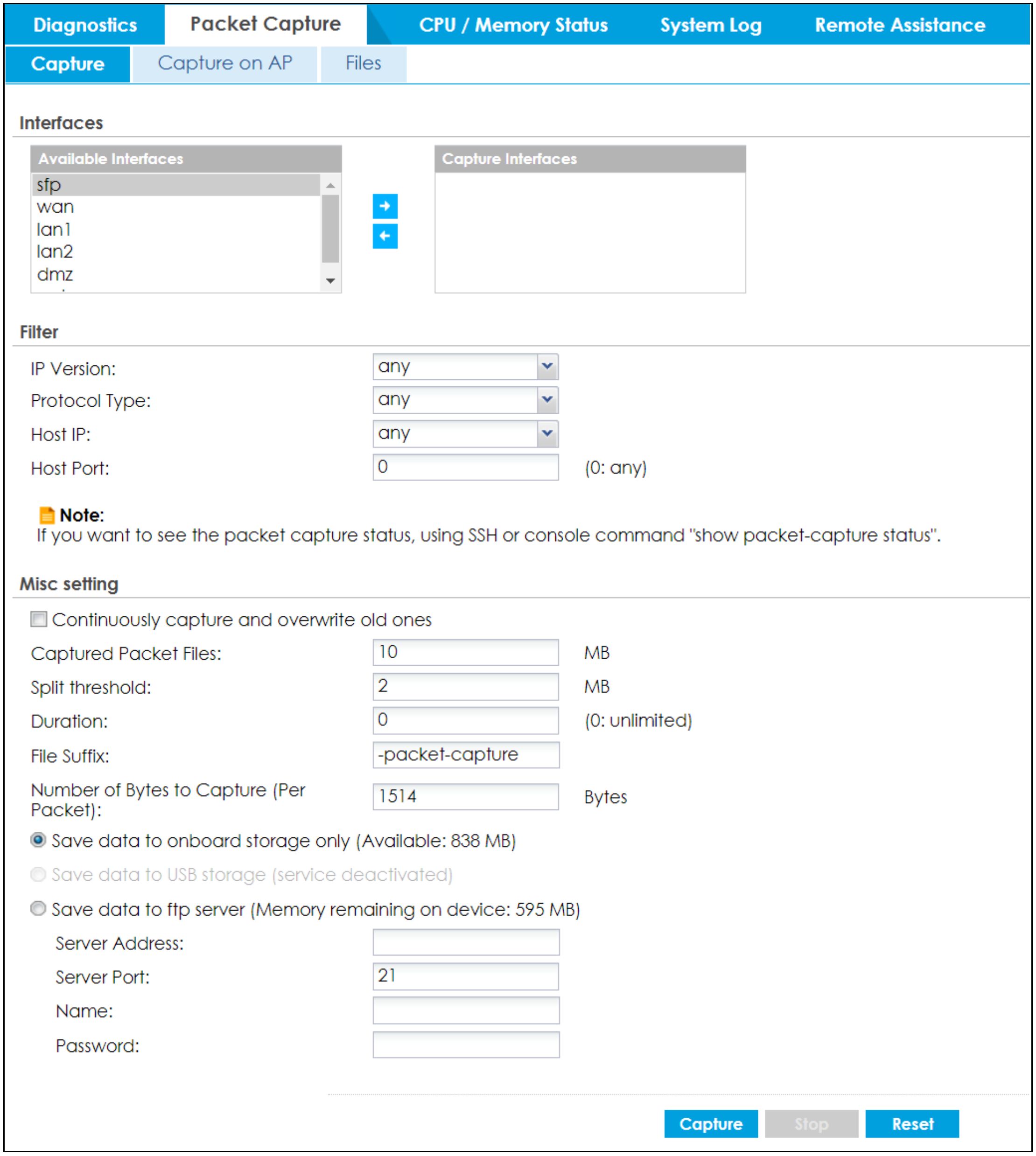
LABEL	DESCRIPTION
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

41.3 The Packet Capture Screen

Use this screen to capture network traffic going through the Zyxel Device’s interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostics > Packet Capture** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the **File Suffix** field’s setting to avoid this.

Figure 578 Maintenance > Diagnostics > Packet Capture



Interfaces

Filter

IP Version: any

Protocol Type: any

Host IP: any

Host Port: 0 (0: any)

Note:
If you want to see the packet capture status, using SSH or console command "show packet-capture status".

Misc setting

□ Continuously capture and overwrite old ones

Captured Packet Files: 10 MB

Split threshold: 2 MB

Duration: 0 (0: unlimited)

File Suffix: -packet-capture

Number of Bytes to Capture (Per Packet): 1514 Bytes

● Save data to onboard storage only (Available: 838 MB)

○ Save data to USB storage (service deactivated)

○ Save data to ftp server (Memory remaining on device: 595 MB)

Server Address:

Server Port: 21

Name:

Password:

The following table describes the labels in this screen.

Table 360 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under **Available Interfaces**. Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
IP Version	Select the version of IP for which to capture packets. Select **any** to capture packets for all IP versions.
Protocol Type	Select the protocol of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.

Table 360 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Host IP	Select a host IP address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.
Host Port	This field is configurable when you set the **IP Type** to **any**, **tcp**, or **udp**. Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the Zyxel Device keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.
Captured Packet Files	When saving packet captures only to the Zyxel Device's on board storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the Zyxel Device. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the **Continuously capture and overwrite old ones** option, you may need to set this size larger or delete existing capture files. The valid range depends on the available on board/USB storage size. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified in the **Duration** field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
Duration	Set a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the **File Size** field. 0 means there is no time limit.
File Suffix	Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
Save data to onboard storage only	Select this to have the Zyxel Device only store packet capture entries on the Zyxel Device. The available storage size is displayed as well. Note: The Zyxel Device reserves some on board storage space as a buffer.
Save data to USB storage	Select this to have the Zyxel Device store packet capture entries only on a USB storage device connected to the Zyxel Device if the Zyxel Device allows this. Status: **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the Zyxel Device cannot mount it. **none** - no USB storage device is connected. **service deactivated** - USB storage feature is disabled (in **Configuration > System > USB Storag**e), so the Zyxel Device cannot use a connected USB device to store system logs and other diagnostic information. **available** - you can have the Zyxel Device use the USB storage device. The available storage capacity also displays. Note: The Zyxel Device reserves some USB storage space as a buffer.

Table 360 Maintenance > Diagnostics > Packet Capture (continued)

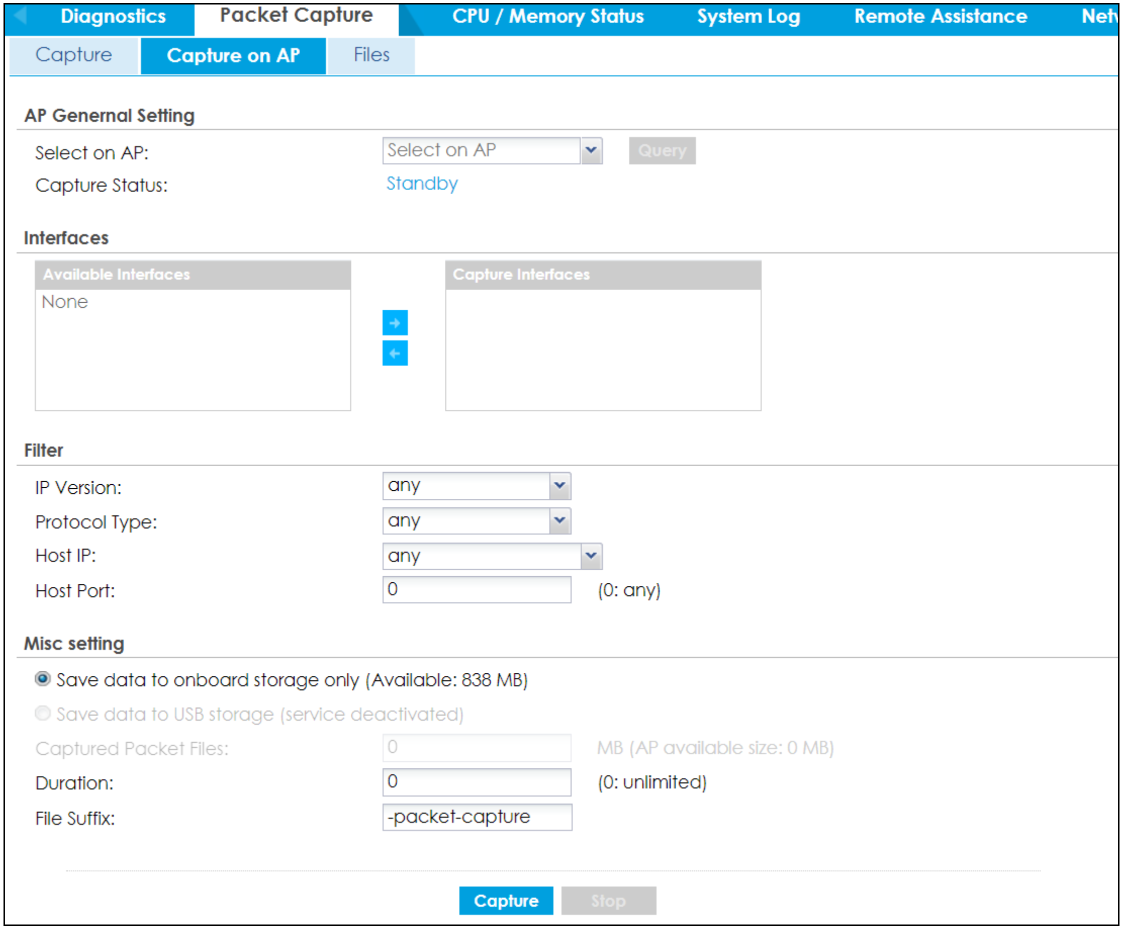
LABEL	DESCRIPTION
Save data to ftp server (available: xx MB)	Select this to have the Zyxel Device store packet capture entries on the defined FTP site. The available storage size is displayed as well.
Server Address	Type the IP address of the FTP server.
Server Port	Type the port this server uses for FTP traffic. The default FTP port is 21.
Name	Type the login username to access the FTP server.
Password	Type the associated login password to access the FTP server.
Capture	Click this button to have the Zyxel Device capture packets according to the settings configured in this screen. You can configure the Zyxel Device while a packet capture is in progress although you cannot modify the packet capture settings. The Zyxel Device's throughput or performance may be affected while a packet capture is in progress. After the Zyxel Device finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

41.3.1 The Packet Capture on AP Screen

Use this screen to capture network traffic going through the connected APs' interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostics > Packet Capture > Capture on AP** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the **File Suffix** field's setting to avoid this.

Figure 579 Maintenance > Diagnostics > Packet Capture > Capture on AP



AP Genernal Setting

Select on AP: Select on AP

Capture Status: Standby

Interfaces

Available Interfaces: None

Capture Interfaces:

Filter

IP Version: any

Protocol Type: any

Host IP: any

Host Port: 0 (0: any)

Misc setting

● Save data to onboard storage only (Available: 838 MB)

○ Save data to USB storage (service deactivated)

Captured Packet Files: 0 MB (AP available size: 0 MB)

Duration: 0 (0: unlimited)

File Suffix: -packet-capture

The following table describes the labels in this screen.

Table 361 Maintenance > Diagnostics > Packet Capture > Capture on AP

LABEL	DESCRIPTION
Select on AP	This lists the managed APs that are connected and available. Select the managed AP that you want the Zyxel Device to capture network traffic going through it.
Query	After you select an AP, click this button to update and display the interfaces, filter configuration and storage size available for the selected AP in the screen. Note: You need to use the **Query** button before packet capturing on an AP if the AP has rebooted or the applied AP profile settings have been changed.
Capture Status	This shows **Standby** when the Zyxel Device is ready to or have finished capturing network traffic going through the selected AP's interface(s). This shows **Preparing** when the Zyxel Device is sending the capture command to the AP's interface(s). This shows **Capturing** when the AP is capturing network traffic going through the selected AP's interface(s). This shows **File Receiving** when the Zyxel Device starts to receive capture files from the AP's interface(s) after you press the Stop button.
Interfaces	Enabled interfaces (except for virtual interfaces) appear under **Available Interfaces**. Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list. Use the [Shift] and/or [Ctrl] key to select multiple objects.

Table 361 Maintenance > Diagnostics > Packet Capture > Capture on AP (continued)

LABEL	DESCRIPTION
IP Version	Select the version of IP for which to capture packets. Select **any** to capture packets for all IP versions.
Protocol Type	Select the protocol of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.
Host Port	This field is configurable when you set the **IP Type** to **any**, **tcp**, or **udp**. Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the Zyxel Device keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.
Captured Packet Files	When saving packet captures only to the Zyxel Device's on board storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the Zyxel Device. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the **Continuously capture and overwrite old ones** option, you may need to set this size larger or delete existing capture files. The valid range depends on the available on board/USB storage size. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified in the **Duration** field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
Duration	Set a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the **File Size** field. 0 means there is no time limit.
File Suffix	Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
Save data to onboard storage only	Select this to have the Zyxel Device only store packet capture entries on the Zyxel Device. The available storage size is displayed as well. Note: The Zyxel Device reserves some on board storage space as a buffer.

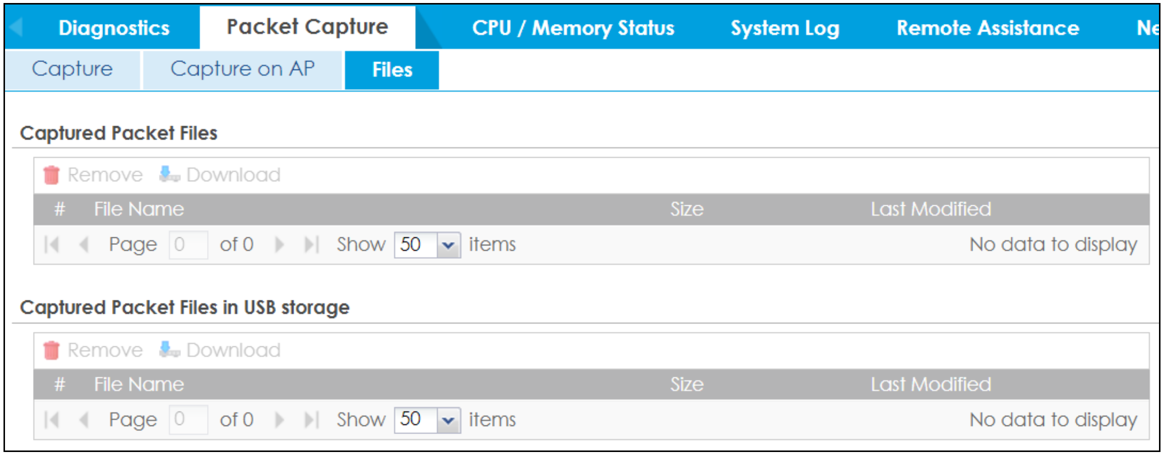
Table 361 Maintenance > Diagnostics > Packet Capture > Capture on AP (continued)

LABEL	DESCRIPTION
Save data to USB storage	Select this to have the Zyxel Device store packet capture entries only on a USB storage device connected to the Zyxel Device if the Zyxel Device allows this. Status: **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the Zyxel Device cannot mount it. **none** - no USB storage device is connected. **service deactivated** - USB storage feature is disabled (in **Configuration > System > USB Storag**e), so the Zyxel Device cannot use a connected USB device to store system logs and other diagnostic information. **available** - you can have the Zyxel Device use the USB storage device. The available storage capacity also displays. Note: The Zyxel Device reserves some USB storage space as a buffer.
Save data to ftp server (available: xx MB)	Select this to have the Zyxel Device store packet capture entries on the defined FTP site. The available storage size is displayed as well.
Server Address	Type the IP address of the FTP server.
Server Port	Type the port this server uses for FTP traffic. The default FTP port is 21.
Name	Type the login username to access the FTP server.
Password	Type the associated login password to access the FTP server.
Capture	Click this button to have the Zyxel Device capture packets according to the settings configured in this screen. You can configure the Zyxel Device while a packet capture is in progress although you cannot modify the packet capture settings. The Zyxel Device's throughput or performance may be affected while a packet capture is in progress. After the Zyxel Device finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

41.3.2 The Packet Capture Files Screen

Click **Maintenance > Diagnostics > Packet Capture > Files** to open the packet capture files screen. This screen lists the files of packet captures stored on the Zyxel Device or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 580 Maintenance > Diagnostics > Packet Capture > Files



Captured Packet Files

Remove Download

#	File Name	Size	Last Modified

Page 0 of 0 Show 50 items No data to display

Captured Packet Files in USB storage

Remove Download

#	File Name	Size	Last Modified

Page 0 of 0 Show 50 items No data to display

The following table describes the labels in this screen.

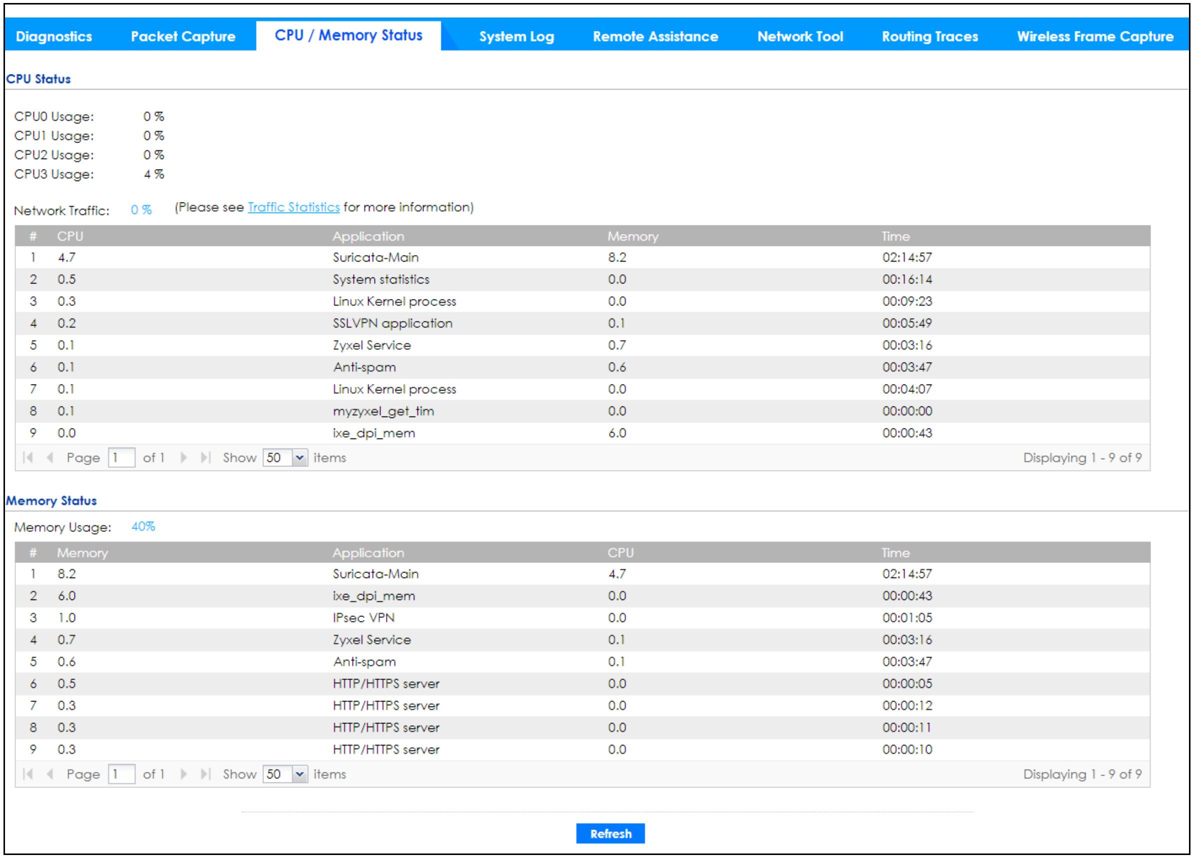
Table 362 Maintenance > Diagnostics > Packet Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

41.4 The CPU / Memory Status Screen

Click **Maintenance > Diagnostics > CPU / Memory Status** to open the **CPU/Memory Status** screen. Use this screen to view the CPU and memory performance of various applications on the Zyxel Device.

Figure 581 Maintenance > Diagnostics > CPU / Memory Status



CPU Status

CPU0 Usage: 0 %
CPU1 Usage: 0 %
CPU2 Usage: 0 %
CPU3 Usage: 4 %

Network Traffic: 0 % (Please see Traffic Statistics for more information)

#	CPU	Application	Memory	Time
1	4.7	Suricata-Main	8.2	02:14:57
2	0.5	System statistics	0.0	00:16:14
3	0.3	Linux Kernel process	0.0	00:09:23
4	0.2	SSLVPN application	0.1	00:05:49
5	0.1	Zyxel Service	0.7	00:03:16
6	0.1	Anti-spam	0.6	00:03:47
7	0.1	Linux Kernel process	0.0	00:04:07
8	0.1	myzyxel_get_tim	0.0	00:00:00
9	0.0	ixe_dpi_mem	6.0	00:00:43

Page 1 of 1 Show 50 items Displaying 1 - 9 of 9

Memory Status

Memory Usage: 40%

#	Memory	Application	CPU	Time
1	8.2	Suricata-Main	4.7	02:14:57
2	6.0	ixe_dpi_mem	0.0	00:00:43
3	1.0	IPsec VPN	0.0	00:01:05
4	0.7	Zyxel Service	0.1	00:03:16
5	0.6	Anti-spam	0.1	00:03:47
6	0.5	HTTP/HTTPS server	0.0	00:00:05
7	0.3	HTTP/HTTPS server	0.0	00:00:12
8	0.3	HTTP/HTTPS server	0.0	00:00:11
9	0.3	HTTP/HTTPS server	0.0	00:00:10

Page 1 of 1 Show 50 items Displaying 1 - 9 of 9

The following table describes the labels in this screen.

Table 363 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
CPU Status This table displays the applications that use the most Zyxel Device CPU processing.	
CPUn Usage	CPU usage shows how much processing power the Zyxel Device is using. This field displays the current percentage usage of a CPU (where n is the number of the CPU) as a percentage of total processing power.
Network Traffic	This field displays the current percentage of network traffic through the Zyxel Device.
#	This field is a sequential value, and it is not associated with any entry.
CPU	This field displays the current CPU utilization percentage for each application used on the Zyxel Device.
Application	This field displays the name of the application consuming the related processing power on the Zyxel Device.
Memory	This field displays the current DRAM memory utilization percentage for each application used on the Zyxel Device.
Time	This field displays each application’s running time in hours - minutes - seconds.
Memory Status This table displays the applications that use the most Zyxel Device DRAM memory.	
Memory Usage	Memory usage shows how much DRAM memory the Zyxel Device is using. This field displays the current percentage of memory utilization.
#	This field is a sequential value, and it is not associated with any entry.

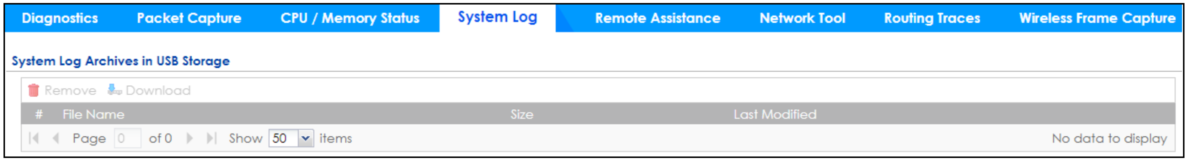
Table 363 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
Memory	This field displays the current DRAM memory utilization percentage for each application used on the Zyxel Device.
Application	This field displays the name of the application consuming the related memory on the Zyxel Device.
CPU	This field displays the current CPU utilization percentage for each application used on the Zyxel Device.
Time	This field displays each application's running time.
Refresh	Click this to update the information in this screen.

41.5 The System Log Screen

Click **Maintenance > Diagnostics > System Log** to open the **System Log** screen. This screen lists the files of Zyxel Device system logs stored on a connected USB storage device. The files are in comma separated value (csv) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 582 Maintenance > Diagnostics > System Log



#	File Name	Size	Last Modified

No data to display

The following table describes the labels in this screen.

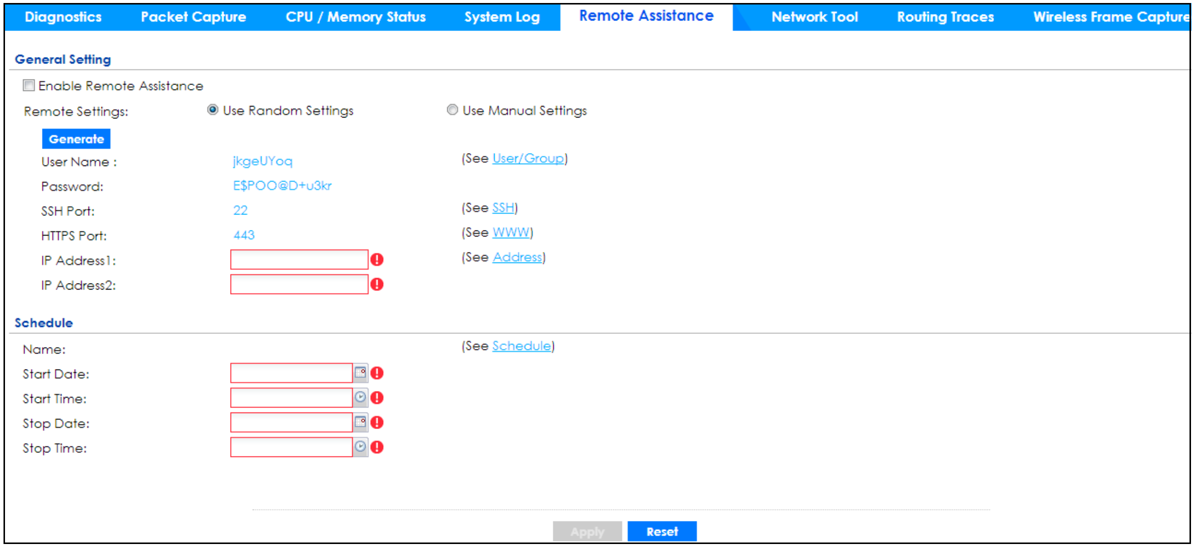
Table 364 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the Zyxel Device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

41.6 The Remote Assistance Screen

Click **Maintenance > Diagnostics > Remote Assistance** to open the **Remote Assistance** screen. Use this screen to configure and schedule external access to the Zyxel Device for troubleshooting. You can also specify the port numbers the services must use to connect to the Zyxel Device. Remote assistance is disabled by default.

Figure 583 Maintenance > Diagnostics > Remote Assistance - Random



General Setting

□ Enable Remote Assistance

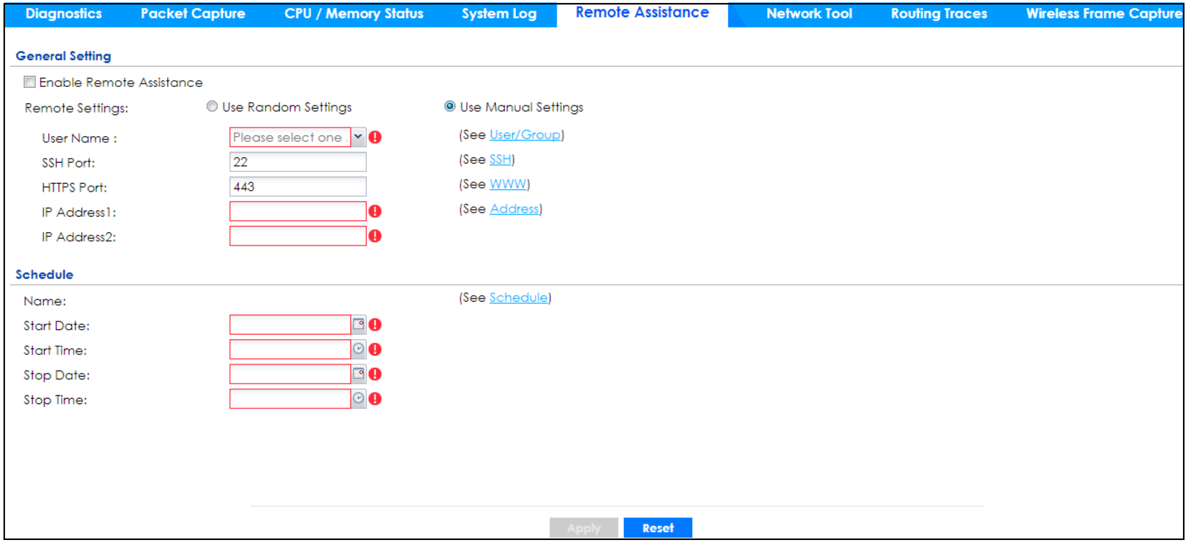
Remote Settings: ● Use Random Settings ○ Use Manual Settings

User Name :	jkgeUYoq	(See User/Group)
Password:	E$POO@D+u3kr	
SSH Port:	22	(See SSH)
HTTPS Port:	443	(See WWW)
IP Address1:		(See Address)
IP Address2:		

Schedule

Name:		(See Schedule)
Start Date:		
Start Time:		
Stop Date:		
Stop Time:		

Figure 584 Maintenance > Diagnostics > Remote Assistance - Manual



General Setting

□ Enable Remote Assistance

Remote Settings: ○ Use Random Settings ● Use Manual Settings

User Name :	Please select one	(See User/Group)
SSH Port:	22	(See SSH)
HTTPS Port:	443	(See WWW)
IP Address1:		(See Address)
IP Address2:		

Schedule

Name:		(See Schedule)
Start Date:		
Start Time:		
Stop Date:		
Stop Time:		

The following table describes the labels in this screen.

Table 365 Maintenance > Diagnostics > Remote Assistance

LABEL	DESCRIPTION
General Setting	
Enable Remote Assistance	Select this to enable an external person, such as customer support to access the Zyxel Device from a network outside the Zyxel Device local network for troubleshooting.
Remote Settings	Select **Use Random Settings** to access the Zyxel Device remotely by using a randomly generated user name and password pair. Select **Use Manual Settings** to access the Zyxel Device remotely by using a previously configured specific user account.
Generate	This button is displayed when you select **Use Random Settings** in the **Remote Settings** field. Click this button to generate a random user name and password pair.
User Name	Select a previously created user/group object that identifies who can have external access to the Zyxel Device for troubleshooting.

Table 365   Maintenance > Diagnostics > Remote Assistance (continued)

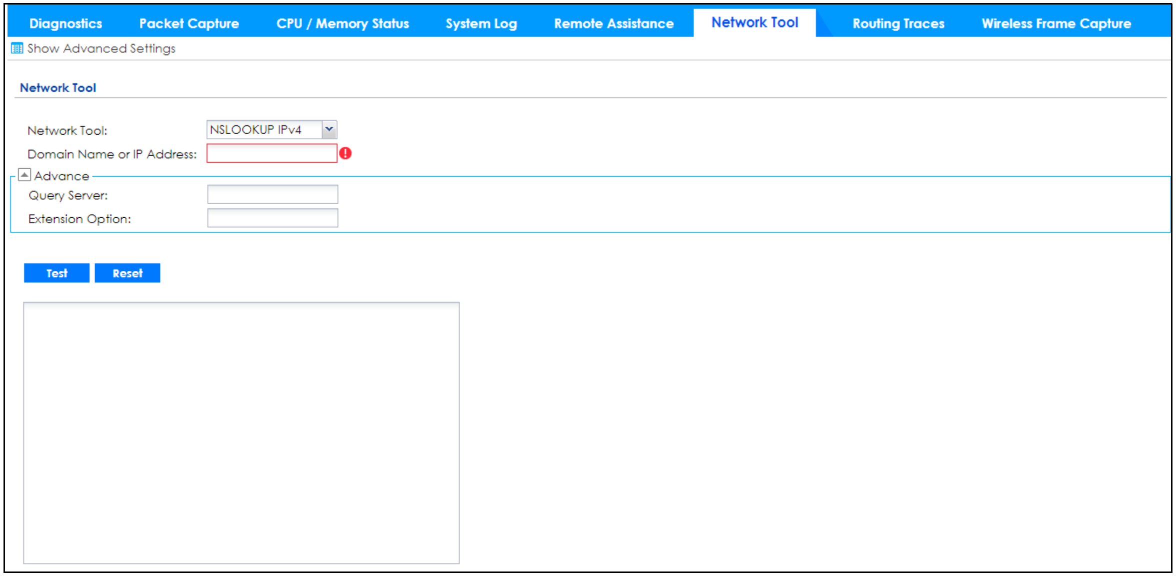
LABEL	DESCRIPTION
Password	Type a password for the selected user/group to allow external access.
SSH Port	This field displays the SSH port number for external access. It should be the same port number as the one configured in **Configuration > System > SSH**.
HTTPS Port	This field displays the HTTPS port number for external access. It should be the same port number as the one configured in **Configuration > System > WWW > Service Control**.
IP Address1	Enter the public IP address of the external user that is allowed to access the Zyxel Device remotely.
IP Address2	Enter the public IP address of the external user that is allowed to access the Zyxel Device remotely.
Schedule	
Name	This field displays the name of the schedule for allowed external access. The schedule must be first configured in **Object > Schedule**.
Start Date	This field displays the date on which the schedule begins.
Start Time	This field displays the time at which the schedule begins.
Stop Date	This field displays the date on which the schedule ends.
Stop Time	This field displays the time at which the schedule ends.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

41.7 The Network Tool Screen

Use this screen to perform various network tests.

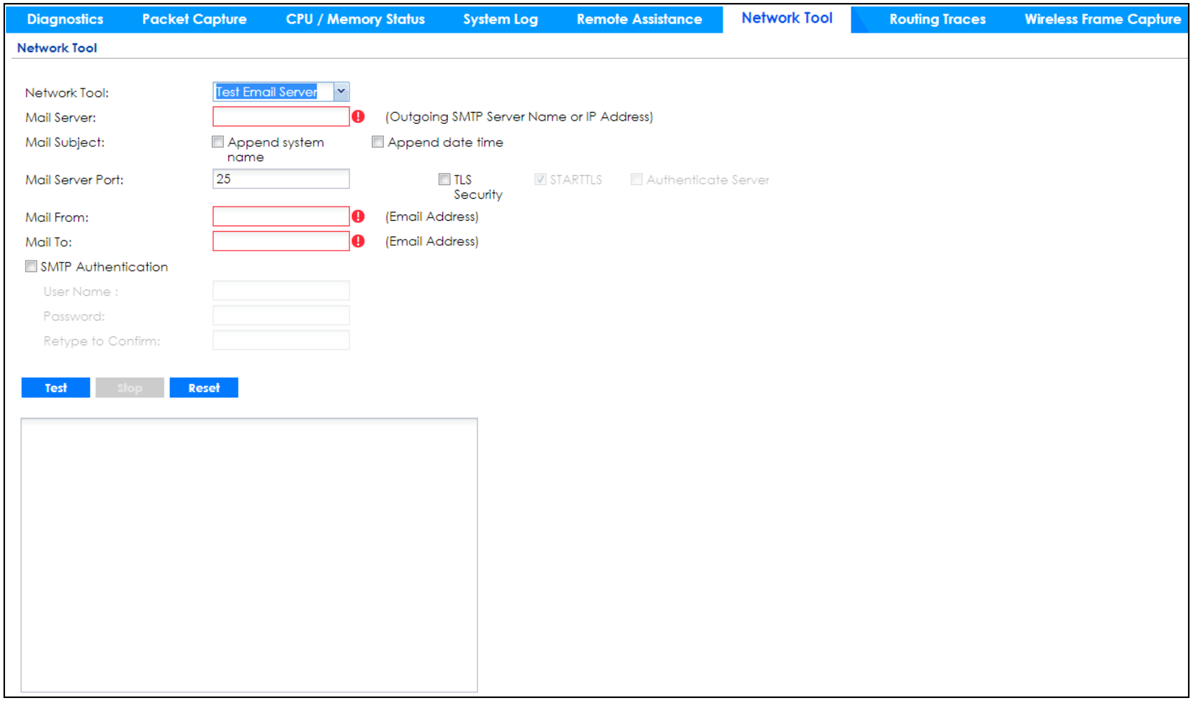
Click **Maintenance > Diagnostics > Network Tool** to display this screen.

Figure 585   Maintenance > Diagnostics > Network Tool



Network Tool: NSLOOKUP IPv4

Figure 586 Maintenance > Diagnostics > Network Tool - Test Email Server



Network Tool

Network Tool: Test Email Server

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: (Email Address)

Mail To: (Email Address)

□ SMTP Authentication

User Name :

Password:

Retype to Confirm:

The following table describes the labels in this screen.

Table 366 Maintenance > Diagnostics > Network Tool

LABEL	DESCRIPTION
Network Tool	Select a network tool: • Select **NSLOOKUP IPv4** or **NSLOOKUP IPv6** to perform name server lookup for querying the Domain Name System (DNS) to get the domain name or IP address mapping. • Select **PING IPv4** or **PING IPv6** to ping the IP address that you entered. • Select **TRACEROUTE IPv4** or **TRACEROUTE IPv6** to run the traceroute function. This determines the path a packet takes to the specified computer. • Select **Test Email Server** to test access to an SMTP email server.
Domain Name or IP Address	Type the IP address that you want to use to for the selected network tool.
Advance Click this to display the following fields.	
Query Server	Enter the IP address of a server to which the Zyxel Device sends queries for NSLOOKUP.
Interface	Select the interface through which the Zyxel Device sends queries for PING or TRACEROUTE.
Extension Option	Enter the extended option if you want to use an extended ping or traceroute command. For example, enter "`-c count`" (where *`count`* is the number of ping requests) to set how many times the Zyxel Device pings the destination IP address, or enter "`-w waittime`" (where *`waittime`* is a time period in seconds) to set how long the Zyxel Device waits for a response to a probe before running another traceroute.
The following fields display when you select **Test Email Server** in **Network Tool**.	
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing email. • Select **Append system name** to add the Zyxel Device system name to the subject. • Select **Append date time** to add the Zyxel Device date and time to the subject.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.

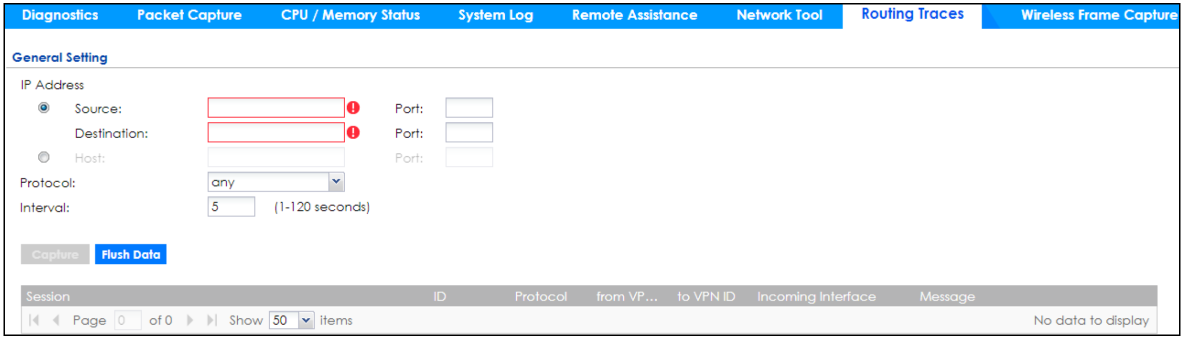
Table 366 Maintenance > Diagnostics > Network Tool (continued)

LABEL	DESCRIPTION
TLS Security	Select this option if the mail server uses Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
STARTTLS	Select this option if the mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device.
Authenticate Server	Select this if the Zyxel Device authenticates the mail server in the TLS handshake.
Mail From	Type the email address from which the outgoing email is delivered. This address is used in replies.
Mail To	Type the email address to which the outgoing email is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type a password of up to 63 characters to provide to the SMTP server when the log is emailed.
Retype to Confirm	Retype your new password for confirmation.
Test	Click this button to start the test.
Stop	Click this button to stop the test.
Reset	Click this button to return the screen to its last-saved settings.

41.8 The Routing Traces Screen

Click **Maintenance > Diagnostics > Routing Traces** to display this screen. Use this screen to configure a traceroute to identify where packets are dropped for troubleshooting.

Figure 587 Maintenance > Diagnostics > Routing Traces



IP Address

● Source: Port:

Destination: Port:

○ Host: Port:

Protocol: any

Interval: 5 (1-120 seconds)

Session	ID	Protocol	from VP...	to VPN ID	Incoming Interface	Message

Page 0 of 0 Show 50 items No data to display

The following table describes the labels in this screen.

Table 367 Maintenance > Diagnostics > Routing Traces

LABEL	DESCRIPTION
IP Address	You can trace traffic through the Zyxel Device from a specific source-to-destination stream or just from/to a specific host (source or destination).
Source	Enter the source IP address of traffic that you want to trace.
Port	Enter the source port number of traffic that you want to trace.
Destination	Enter the destination IP address of traffic that you want to trace.

Table 367 Maintenance > Diagnostics > Routing Traces (continued)

LABEL	DESCRIPTION
Port	Enter the destination port number of traffic that you want to trace.
Host	Enter the IP address of a specific source or destination host whose traffic you want to trace.
Port	Enter the port number for particular source traffic on the host that you want to trace.
Protocol	Select the protocol of traffic that you want to trace. **any** means any protocol.
Interval	Enter a time interval in seconds for renewing a route trace. The default time interval is 5 seconds.
Capture	Click this button to have the Zyxel Device capture frames according to the settings configured in this screen. You can configure the Zyxel Device while a frame capture is in progress although you cannot modify the frame capture settings.
Flush Data	Click this to clear all data on the screen.
Session	This field displays established sessions that passed through the Zyxel Device which matched the capture criteria.
ID	This field displays the packet ID for each active session.
Protocol	This field displays the protocol used in each active session.
from VPN ID	This field displays the tagged VLAN ID in ingress packets coming into the Zyxel Device.
to VPN ID	This field displays the tagged VLAN ID in egress packets going out from the Zyxel Device.
Incoming Interface	This is the source interface of packets to which this active session applies.
Message	This field displays traceroute information.

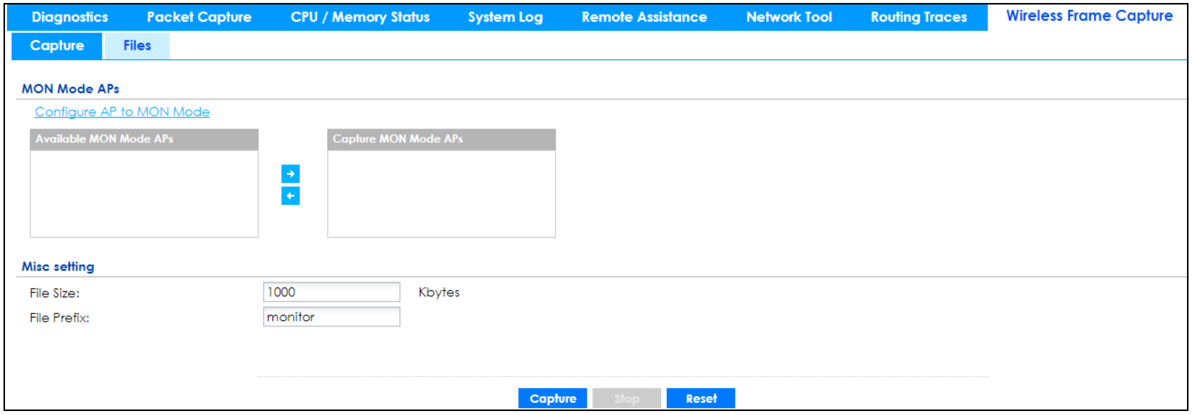
41.9 The Wireless Frame Capture Screen

Use this screen to capture wireless network traffic going through the AP interfaces connected to your Zyxel Device. Studying these frame captures may help you identify network problems.

Click **Maintenance > Diagnostics > Wireless Frame Capture** to display this screen.

Note: New capture files overwrite existing files of the same name. Change the **File Prefix** field's setting to avoid this.

Figure 588 Maintenance > Diagnostics > Wireless Frame Capture > Capture



File Size: 1000 Kbytes

File Prefix: monitor

The following table describes the labels in this screen.

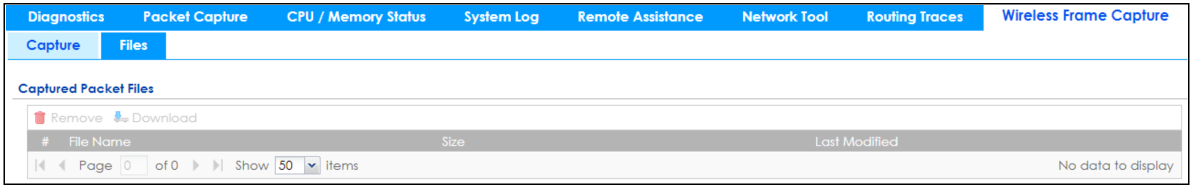
Table 368 Maintenance > Diagnostics > Wireless Frame Capture > Capture

LABEL	DESCRIPTION
MON Mode APs	
Configure AP to MON Mode	Click this to go the **Configuration > Wireless > AP Management** screen, where you can set one or more APs to monitor mode.
Available MON Mode APs	This column displays which APs on your wireless network are currently configured for monitor mode. Use the arrow buttons to move APs off this list and onto the **Captured MON Mode APs** list.
Capture MON Mode APs	This column displays the monitor-mode configured APs selected to for wireless frame capture.
Misc Setting	
File Size	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the Zyxel Device, including any existing capture files and any new capture files you generate. Note: If you have existing capture files you may need to set this size larger or delete existing capture files. The valid range is 1 to 50000. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size.
File Prefix	Specify text to add to the front of the file name in order to help you identify frame capture files. You can modify the prefix to also create new frame capture files each time you perform a frame capture operation. Doing this does no overwrite existing frame capture files. The file format is: [file prefix].cap. For example, “monitor.cap”.
Capture	Click this button to have the Zyxel Device capture frames according to the settings configured in this screen. You can configure the Zyxel Device while a frame capture is in progress although you cannot modify the frame capture settings. The Zyxel Device’s throughput or performance may be affected while a frame capture is in progress. After the Zyxel Device finishes the capture it saves a combined capture file for all APs. The total number of frame capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more frame captures will fail.
Stop	Click this button to stop a currently running frame capture and generate a combined capture file for all APs.
Reset	Click this button to return the screen to its last-saved settings.

41.9.1 The Wireless Frame Capture Files Screen

Click **Maintenance > Diagnostics > Wireless Frame Capture > Files** to open this screen. This screen lists the files of wireless frame captures the Zyxel Device has performed. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 589 Maintenance > Diagnostics > Wireless Frame Capture > Files



The following table describes the labels in this screen.

Table 369 Maintenance > Diagnostics > Wireless Frame Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the Zyxel Device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

CHAPTER 42
Packet Flow Explore

42.1 Overview

Use this to get a clear picture on how the Zyxel Device determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

42.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see Section 42.2 on page 842) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see Section 42.3 on page 846) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

42.2 The Routing Status Screen

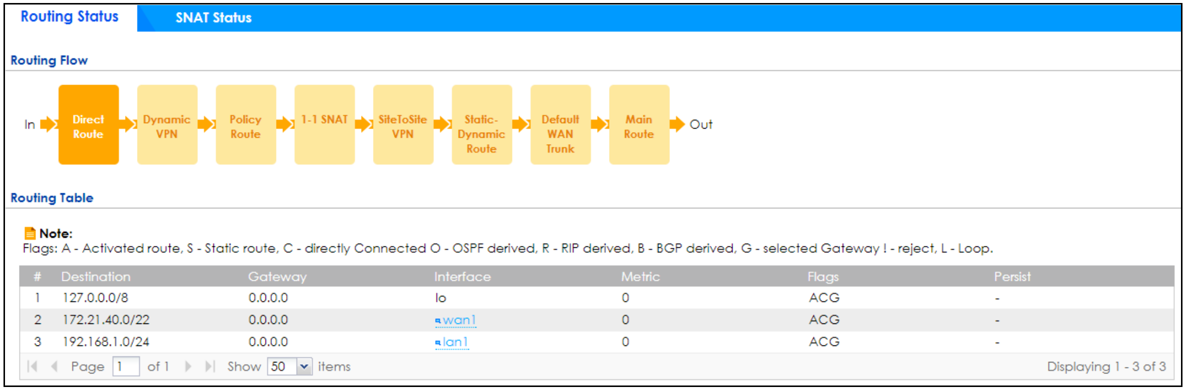
The **Routing Status** screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the **Routing Flow** section, the related routes (activated) will display in the **Routing Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore** > **Routing Status**.

The order of the routing flow may vary depending on whether you:

- Select **use policy route to override direct route** in the **CONFIGURATION > Network > Routing > Policy Route** screen.
- Use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- Select **use policy routes to control dynamic IPSec rules** in the **CONFIGURATION > VPN > IPSec VPN > VPN Connection** screen.

Note: Once a packet matches the criteria of a routing rule, the Zyxel Device takes the corresponding action and does not perform any further flow checking.

Figure 590 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

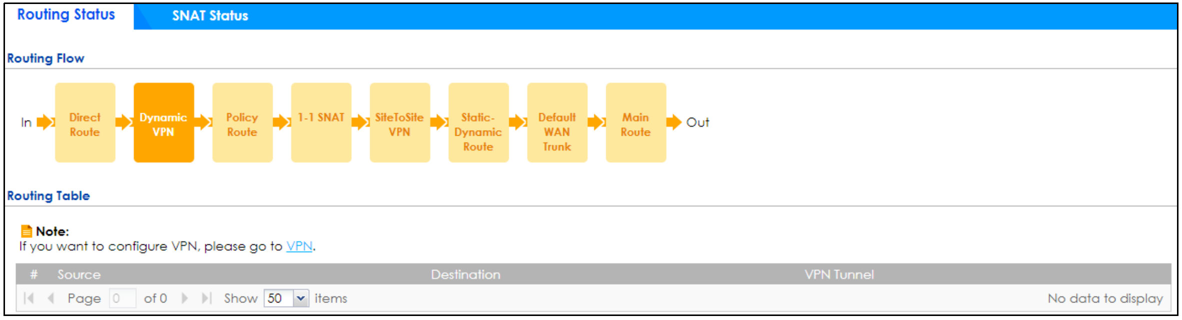


Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, B - BGP derived, G - selected Gateway ! - reject, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	Persist
1	127.0.0.0/8	0.0.0.0	lo	0	ACG	-
2	172.21.40.0/22	0.0.0.0	wan1	0	ACG	-
3	192.168.1.0/24	0.0.0.0	lan1	0	ACG	-

Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

Figure 591 Maintenance > Packet Flow Explore > Routing Status (Dynamic VPN)

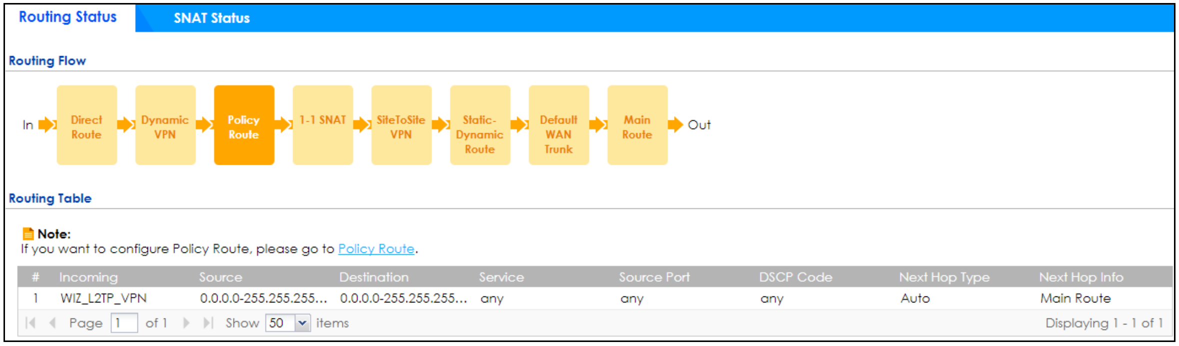


Note:
If you want to configure VPN, please go to VPN.

#	Source	Destination	VPN Tunnel

Page 0 of 0 Show 50 items No data to display

Figure 592 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

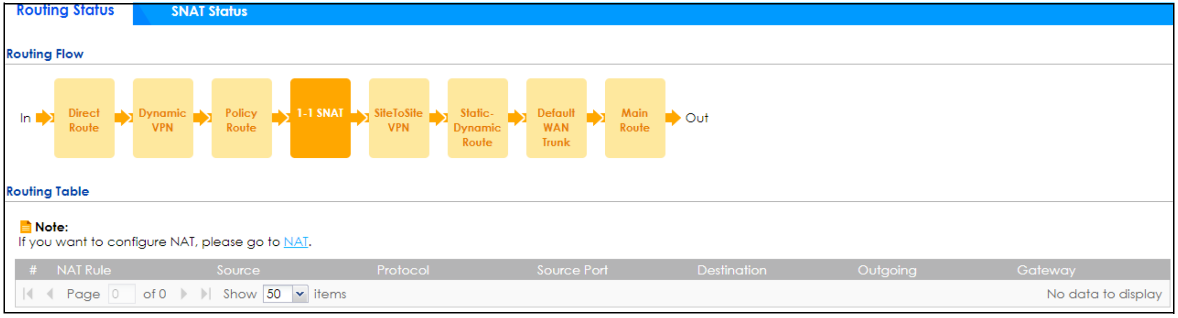


Note:
If you want to configure Policy Route, please go to Policy Route.

#	Incoming	Source	Destination	Service	Source Port	DSCP Code	Next Hop Type	Next Hop Info
1	WIZ_L2TP_VPN	0.0.0.0-255.255.255...	0.0.0.0-255.255.255...	any	any	any	Auto	Main Route

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Figure 593 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

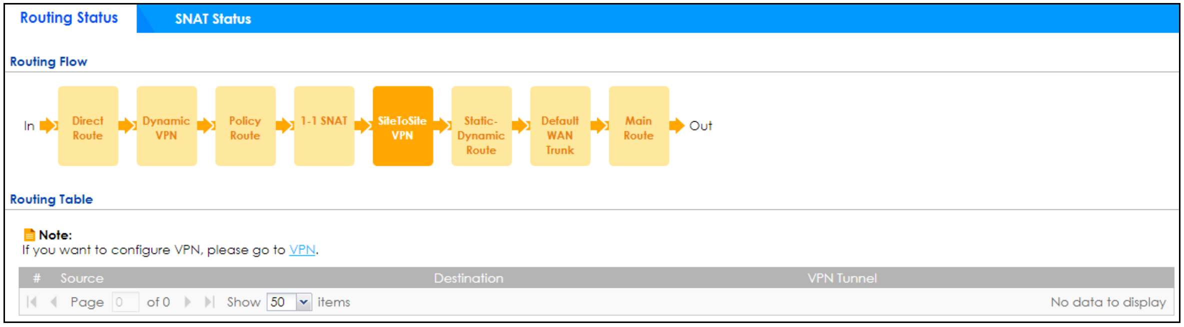


Note:
If you want to configure NAT, please go to NAT.

#	NAT Rule	Source	Protocol	Source Port	Destination	Outgoing	Gateway

Page 0 of 0 Show 50 items No data to display

Figure 594 Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)



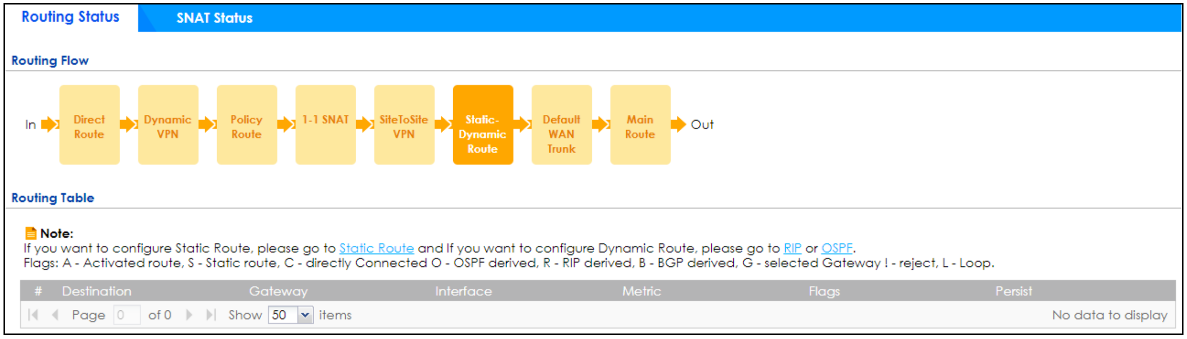
Routing Table

Note:
If you want to configure VPN, please go to VPN.

#	Source	Destination	VPN Tunnel

Page 0 of 0 Show 50 items No data to display

Figure 595 Maintenance > Packet Flow Explore > Routing Status (Static-Dynamic Route)



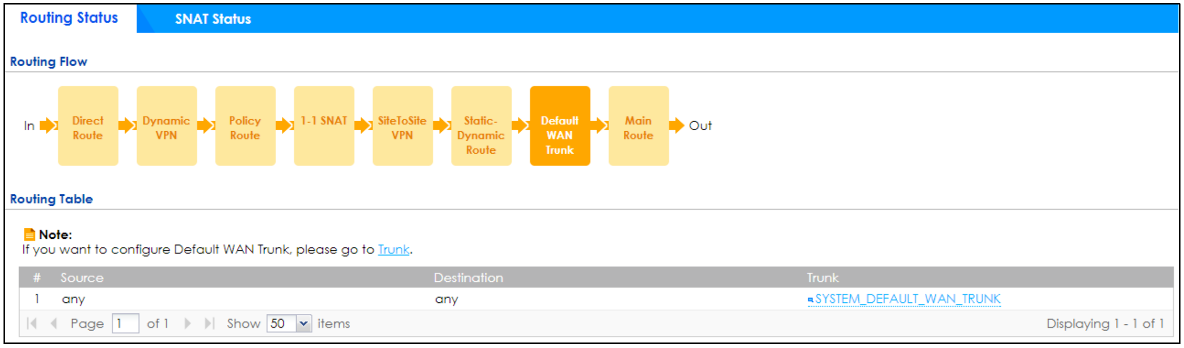
Routing Table

Note:
If you want to configure Static Route, please go to Static Route and If you want to configure Dynamic Route, please go to RIP or OSPF.
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, B - BGP derived, G - selected Gateway ! - reject, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	Persist

Page 0 of 0 Show 50 items No data to display

Figure 596 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)



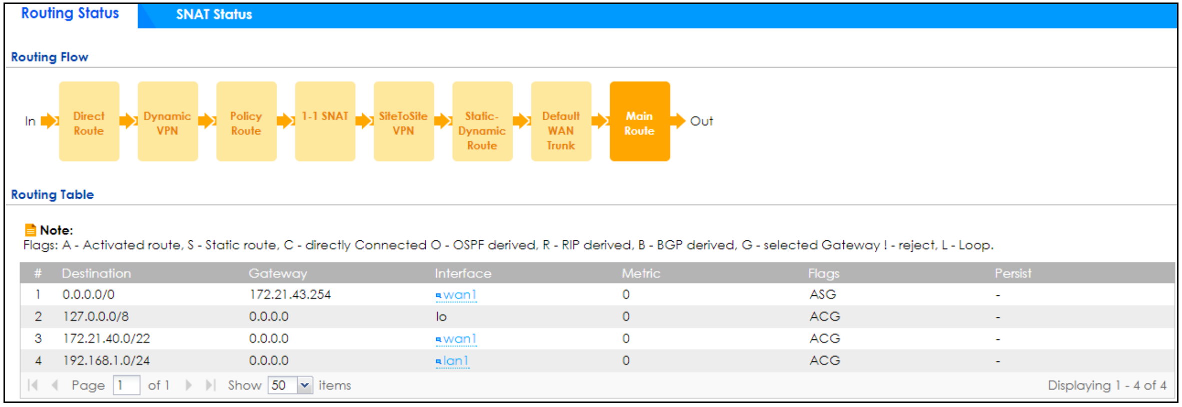
Routing Table

Note:
If you want to configure Default WAN Trunk, please go to Trunk.

#	Source	Destination	Trunk
1	any	any	SYSTEM_DEFAULT_WAN_TRUNK

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Figure 597 Maintenance > Packet Flow Explore > Routing Status (Main Route)



Routing Table

Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, B - BGP derived, G - selected Gateway ! - reject, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	Persist
1	0.0.0.0/0	172.21.43.254	wan1	0	ASG	-
2	127.0.0.0/8	0.0.0.0	lo	0	ACG	-
3	172.21.40.0/22	0.0.0.0	wan1	0	ACG	-
4	192.168.1.0/24	0.0.0.0	lan1	0	ACG	-

Page 1 of 1 Show 50 items Displaying 1 - 4 of 4

The following table describes the labels in this screen.

Table 370 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the Zyxel Device determines where to route a packet. Click a function box to display the related settings in the **Routing Table** section.
Routing Table	This section shows the corresponding settings according to the function box you click in the **Routing Flow** section.
The following fields are available if you click **Direct Route**, **Static-Dynamic Route**, or **Main Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: • **A** - this route is currently activated. • **S** - this is a static route. • **C** - this is a direct connected route. • **O** - this is a dynamic route learned through OSPF. • **R** - this is a dynamic route learned through RIP. • **B** - this is a dynamic route learned through BGP. • **G** - the route is to a gateway (router) in the same network. • **!** - this is a route which forces a route lookup to fail. • **B** - this is a route which discards packets. • **L** - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The Zyxel Device removes the route after this time period is counted down to zero.
The following fields are available if you click **Policy Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. **any** means all services.
Source Port	This is the source port(s) from which the packets are sent.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 10.2 on page 312 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	• This is the main route if the next hop type is **Auto**. • This is the interface name and gateway IP address if the next hop type is **Interface / GW**. • This is the tunnel name if the next hop type is **VPN Tunnel**. • This is the trunk name if the next hop type is **Trunk**.
The following fields are available if you click **1-1 SNAT** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the external source IP address(es).
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.

Table 370   Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Destination	This is the external destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click **Dynamic VPN or SiteToSite VPN** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click **Default WAN Trunk** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. **any** means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. **any** means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

42.3 The SNAT Status Screen

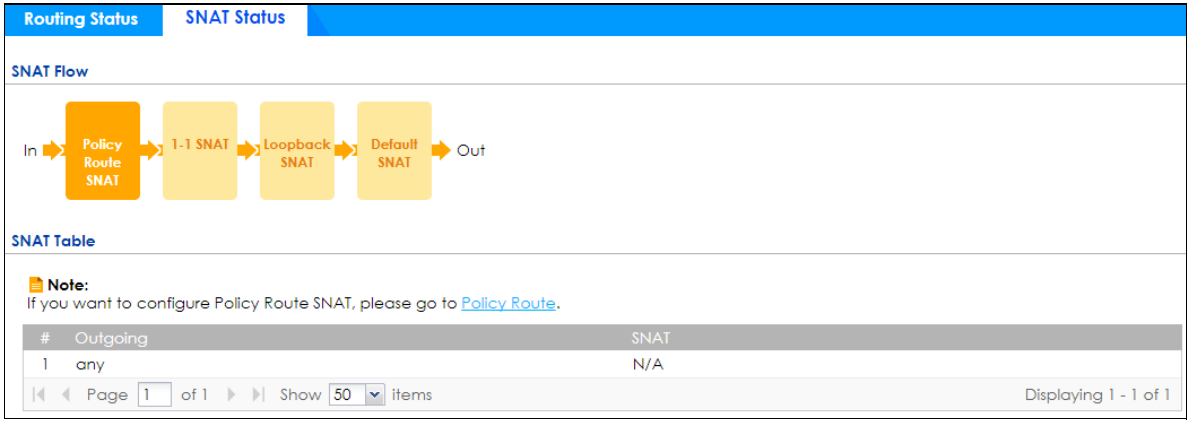
The **SNAT Status** screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the **SNAT Flow** section, the related SNAT rules (activated) will display in the **SNAT Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore** > **SNAT Status**.

The order of the SNAT flow may vary depending on whether you:

- select **use default SNAT** in the **CONFIGURATION > Network > Interface > Trunk** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the Zyxel Device takes the corresponding action and does not perform any further flow checking.

Figure 598   Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

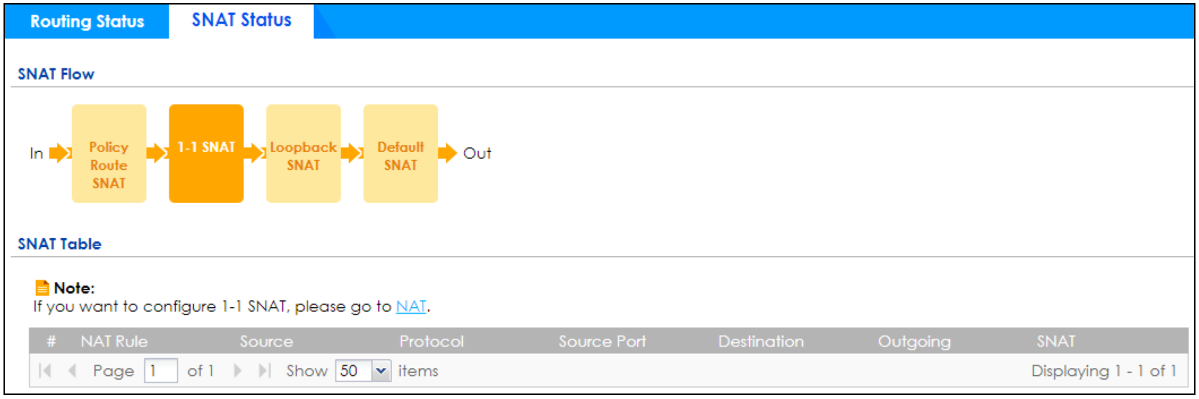


Note:
If you want to configure Policy Route SNAT, please go to Policy Route.

#	Outgoing	SNAT
1	any	N/A

Page 1 of 1   Show 50 items   Displaying 1 - 1 of 1

Figure 599 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)



SNAT Flow

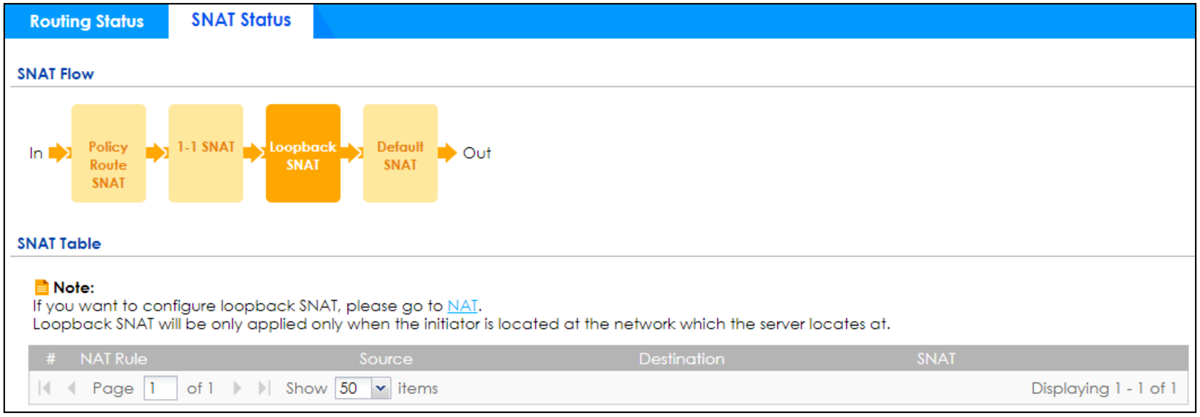
SNAT Table

Note:
If you want to configure 1-1 SNAT, please go to NAT.

#	NAT Rule	Source	Protocol	Source Port	Destination	Outgoing	SNAT

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Figure 600 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)



SNAT Flow

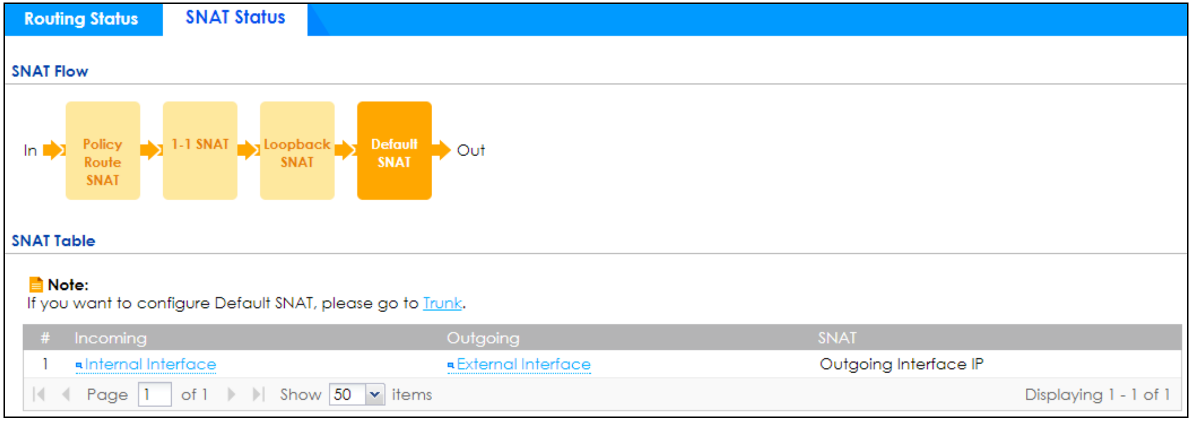
SNAT Table

Note:
If you want to configure loopback SNAT, please go to NAT.
Loopback SNAT will be only applied only when the initiator is located at the network which the server locates at.

#	NAT Rule	Source	Destination	SNAT

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Figure 601 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



SNAT Flow

SNAT Table

Note:
If you want to configure Default SNAT, please go to Trunk.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 371 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the Zyxel Device changes the source IP address for a packet according to the rules you have configured in the Zyxel Device. Click a function box to display the related settings in the **SNAT Table** section.
SNAT Table	The table fields in this section vary depending on the function box you select in the **SNAT Flow** section.
The following fields are available if you click **Policy Route SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.

Table 371 Maintenance > Packet Flow Explore > SNAT Status (continued)

LABEL	DESCRIPTION
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **1-1 SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the external source IP address(es).
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Destination	This is the external destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **Loopback SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the Zyxel Device uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click **Default SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the Zyxel Device uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

CHAPTER 43 Shutdown

43.1 Overview

Use this to shutdown the device in preparation for disconnecting the power.

Always use the Maintenance > Shutdown > Shutdown screen or the “shutdown” command before you turn off the Zyxel Device or remove the power. Not doing so can cause the firmware to become corrupt.

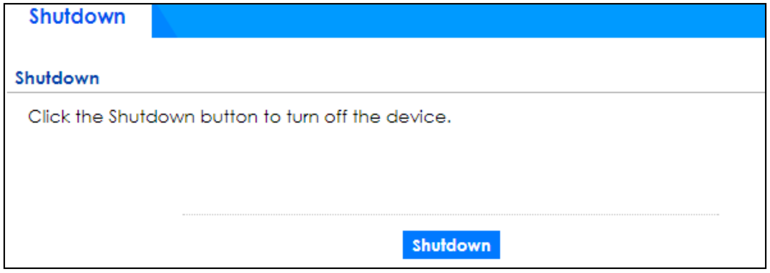
43.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

43.2 The Shutdown Screen

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

Figure 602 Maintenance > Shutdown



Click the Shutdown button to turn off the device.

Click the **Shutdown** button to shut down the Zyxel Device. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shutdown the Zyxel Device.

PART III

Appendices and Troubleshooting

CHAPTER 44
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Section 6.36 on page 181).
- For the order in which the Zyxel Device applies its features and checks, see Chapter 42 on page 842.

None of the LEDs turn on.

Make sure that you have the power cord connected to the Zyxel Device and plugged in to an appropriate power source. Make sure you have the Zyxel Device turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Cannot access the Zyxel Device from the LAN.

- Check the cable connection between the Zyxel Device and your computer or switch.
- Ping the Zyxel Device from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the Zyxel Device's.
- In the computer, click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the Zyxel Device's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The Zyxel Device should reply.
- If you've forgotten the Zyxel Device's password, use the **RESET** button. Press the button in for about 5 seconds (or until the **SYS** LED starts to blink), then release it. It returns the Zyxel Device to the factory defaults (password is 1234, LAN IP address 192.168.1.1, etc).
- If you've forgotten the Zyxel Device's IP address, you can use the commands through the **CONSOLE** port to check it. Connect your computer to the **CONSOLE** port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the Zyxel Device's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- Check the WAN interface's status in the **Dashboard**. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

I cannot update the anti-malware/IDP/application patrol/botnet filter/IP reputation signatures.

- Make sure your Zyxel Device has the anti-malware/IDP/application patrol service registered and that the license is not expired. Purchase a new license if the license is expired.
- Make sure your Zyxel Device is connected to the Internet.

I cannot update the threat intelligence machine learning (TIML) signatures.

- Make sure your Zyxel Device has the anti-malware service registered and that the gold security pack license is not expired. Purchase a new license if the license is expired.
- Make sure your Zyxel Device is connected to the Internet.

I downloaded updated anti-malware/IDP/application patrol/botnet filter/IP reputation signatures. Why has the Zyxel Device not re-booted yet?

The Zyxel Device does not have to reboot when you upload new signatures.

The content filter category service is not working.

- Make sure your Zyxel Device has the content filter category service registered and that the license is not expired. Purchase a new license if the license is expired.
- Make sure your Zyxel Device is connected to the Internet.
- Make sure you select **Enable Content Filter Category Service** when you add a filter profile in the **Configuration > Security Service > Content Filter > Profile > Add or Edit** screen.

I configured security settings but the Zyxel Device is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The Zyxel Device is not applying the custom policy route I configured.

The Zyxel Device checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that the traffic would also match.

The Zyxel Device is not applying the custom security policy I configured.

The Zyxel Device checks the security policies in the order that they are listed. So make sure that your custom security policy comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

The format of interface names other than the Ethernet interface names is very strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, VLAN interfaces are vlan0, vlan1, vlan2,...; and so on.

- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

My rules and settings that apply to a particular interface no longer work.

The interface's IP address may have changed. To avoid this, create an IP address object based on the interface. This way the Zyxel Device automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

You have to set up an ISP account before you create a PPPoE or PPTP interface.

The data rates through my cellular connection are no-where near the rates I expected.

The actual cellular data rate you obtain varies depending on the cellular device you use, the signal strength to the service provider's base station, and so on.

I created a cellular interface but cannot connect through it.

- Make sure you have a compatible mobile broadband device installed or connected. See www.zyxel.com for details.
- Make sure you have the cellular interface enabled.
- Make sure the cellular interface has the correct user name, password, and PIN code configured with the correct casing.
- If the Zyxel Device has multiple WAN interfaces, make sure their IP addresses are on different subnets.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

Each VLAN interface is created on top of only one Ethernet interface.

The Zyxel Device is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the Zyxel Device does not support ingress bandwidth management.

The Zyxel Device is not applying my application patrol bandwidth management settings.

Bandwidth management in policy routes has priority over application patrol bandwidth management.

The Zyxel Device's performance slowed down after I configured many new application patrol entries.

The Zyxel Device checks the ports and conditions configured in application patrol entries in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the Zyxel Device by putting more commonly used ports at the top of the list.

The Zyxel Device's anti-malware scanner cleaned an infected file but now I cannot use the file.

The scanning engine checks the contents of the packets for malware. If a malware pattern is matched, the Zyxel Device removes a portion of the file, while the rest goes through. Since the Zyxel Device erases a portion of the file before sending it, you may not be able to open the file.

The Zyxel Device sent an alert that a malware-infected file has been found, but the file was still forwarded to the user and could still be executed.

Make sure you enable **Destroy Infected File** in the **Configuration > Security Service > Anti-Malware** screen to modify infected files before forwarding the files to the user, preventing them from being executed.

I added a file pattern in the anti-malware white list, but the Zyxel Device still checks and modifies files that match this pattern.

Make sure you select the **Check White List** check box above the white list table. If it is already selected, make sure that the white list entry corresponding to this file pattern is activated.

The Zyxel Device is not scanning some zipped files.

The Zyxel Device cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the Zyxel Device can concurrently unzip.

The Zyxel Device is deleting some zipped files.

The anti-malware policy may be set to delete zipped files that the Zyxel Device cannot unzip. The Zyxel Device cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the Zyxel Device can concurrently unzip.

The threat intelligence machine learning (TIML) feature is not working.

1 Make sure you purchase the gold security pack.

- Make sure you've registered the Zyxel Device and activated the anti-malware service on portal.myZyxel.com.
- Go to the screen, and select the **Enable** check box in the **Configuration** > **Security Service** > **Anti-Malware** to activate the TIML feature.

2 Make sure the gold security pack is not expired. If it is, renew the license.
The Zyxel Device won't scan the TIML signatures that were downloaded when the gold security pack expired.

The Zyxel Device's performance seems slower after configuring IDP.

Depending on your network topology and traffic load, binding every packet direction to an IDP profile may affect the Zyxel Device's performance. You may want to focus IDP scanning on certain traffic directions such as incoming traffic.

IDP is dropping traffic that matches a rule that says no action should be taken.

The Zyxel Device checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the Zyxel Device applies the more restrictive action (**reject-both**, **reject-receiver** or **reject-sender**, **drop**, **none** in this order). If a packet matches a rule for **reject-receiver** and it also matches a rule for **reject-sender**, then the Zyxel Device will reject-both.

I uploaded a custom signature file and now all of my earlier custom signatures are gone.

The name of the complete custom signature file on the Zyxel Device is 'custom.rules'. If you import a file named 'custom.rules', then all custom signatures on the Zyxel Device are overwritten with the new file. If this is not your intention, make sure that the files you import are not named 'custom.rules'.

I cannot configure some items in IDP that I can configure in Snort.

Not all Snort functionality is supported in the Zyxel Device.

The Zyxel Device's performance seems slower after configuring ADP.

Depending on your network topology and traffic load, applying an anomaly profile to each and every packet direction may affect the Zyxel Device's performance.

Some of the files I download don't go through Sandboxing even though it is enabled.

The Sandboxing feature only applies to certain file types. Check the list in **File Submission Options** to see if the file types you use are included. If they are, make sure you select their corresponding check box.

The Zyxel Device detected a malicious file from Sandboxing, but the file still went through the Zyxel Device and is still usable.

Make sure you set your Sandboxing settings to destroy malicious files in the **Configuration > Security Service** > **Sandboxing**: **Action For Malicious File** drop-down list box.

The Zyxel Device destroyed/dropped a file/email without notifying me.

Make sure you enable logs for your security features, such as in the following screens:

- **Configuration > Security Service > IDP**
- **Configuration > Security Service > Anti-Malware**
- **Configuration > Security Service** > **Sandboxing**
- **Configuration > Security Service** > **Email Security**

The Zyxel Device routes and applies SNAT for traffic from some interfaces but not from others.

The Zyxel Device automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **General**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the **Interface Type** set to **Internal** or **External**.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.

- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the Zyxel Device.
- You may need to configure the DDNS entry's IP Address setting to **Auto** if the interface has a dynamic IP address or there are one or more NAT routers between the Zyxel Device and the DDNS server.
- The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

I cannot get the application patrol to manage SIP traffic.

Make sure you have the SIP ALG enabled.

I cannot get the application patrol to manage H.323 traffic.

Make sure you have the H.323 ALG enabled.

I cannot get the application patrol to manage FTP traffic.

Make sure you have the FTP ALG enabled.

The Zyxel Device keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged.

You can set the Zyxel Device's security policy to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the Zyxel Device. A better solution is to use virtual interfaces to put the Zyxel Device and the backup gateway on separate subnets. See Asymmetrical Routes on page 495 and the chapter about interfaces for more information.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both Zyxel IPSec routers and check the settings in each field methodically and slowly. Make sure both the Zyxel Device and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 20 on page 396.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- The Zyxel Device and remote IPSec router must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode.
- Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.
- When using pre-shared keys, the Zyxel Device and the remote IPSec router must use the same pre-shared key.
- The Zyxel Device's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- The Zyxel Device and remote IPSec router must use the same active protocol.
- The Zyxel Device and remote IPSec router must use the same encapsulation.
- The Zyxel Device and remote IPSec router must use the same SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learned by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the Zyxel Device and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following Zyxel Device features.

- The Zyxel Device does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Chapter 10 on page 310.
- Make sure the To-Zyxel Device security policies allow IPSec VPN traffic to the Zyxel Device. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The Zyxel Device supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-Zyxel Device security policies allow UDP port 4500 too.
- Make sure regular security policies allow traffic between the VPN tunnel and the rest of the network. Regular security policies check packets the Zyxel Device sends before the Zyxel Device encrypts them and check packets the Zyxel Device receives after the Zyxel Device decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).

- If you have the Zyxel Device and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the Zyxel Device and remote IPSec router first and make sure they trust each other's certificates. If the Zyxel Device's certificate is self-signed, import it into the remote IPSec router. If it is signed by a CA, make sure the remote IPSec router trusts that CA. The Zyxel Device uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

If you have the **Configuration > VPN > IPSec VPN > VPN Connection** screen's **Use Policy Route to control dynamic IPSec rules option** enabled, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

I uploaded a logo to show in the SSL VPN user screens but it does not display properly.

The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The Zyxel Device automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

I logged into the SSL VPN but cannot see some of the resource links.

Available resource links vary depending on the SSL application object's configuration.

I cannot download the Zyxel Device's firmware package.

The Zyxel Device's firmware package cannot go through the Zyxel Device when you enable the anti-malware **Destroy compressed files that could not be decompressed** option. The Zyxel Device classifies the firmware package as not being able to be decompressed and deletes it.

You can upload the firmware package to the Zyxel Device with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 28.2 on page 548 for more on the anti-malware **Destroy compressed files that could not be decompressed** option.

I changed the LAN IP address and can no longer access the Internet.

The Zyxel Device automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I configured application patrol to allow and manage access to a specific service but access is blocked.

- If you want to use a service, make sure the security policy allows Security Service application patrol to go through the Zyxel Device.

I configured policy routes to manage the bandwidth of TCP and UDP traffic but the bandwidth management is not being applied properly.

It is recommended to use application patrol instead of policy routes to manage the bandwidth of TCP and UDP traffic.

I cannot get the RADIUS server to authenticate the Zyxel Device's default admin account.

The default **admin** account is always authenticated locally, regardless of the authentication method setting.

The Zyxel Device fails to authentication the ext-user user accounts I configured.

An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts. If the Zyxel Device tries to use the local database to authenticate an **ext-user**, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in other chapters in this guide.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default **admin** account into any user group.

The schedule I configured is not being applied at the configured times.

Make sure the Zyxel Device's current date and time are correct.

I cannot get a certificate to import into the Zyxel Device.

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

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

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

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

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

I cannot access the Zyxel Device from a computer connected to the Internet.

Check the service control rules and to-Zyxel Device security policies.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The Zyxel Device's traffic throughput rate decreased after I started collecting traffic statistics.

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

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

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

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the Zyxel Device treat the line as a comment.
- Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the Zyxel Device exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

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

See Chapter 40 on page 806 for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

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

My packet capture captured less than I wanted or failed.

The packet capture screen's **File Size** sets a maximum size limit for the total combined size of all the capture files on the Zyxel Device, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The Zyxel Device stops the capture and generates the capture file when either the capture files reach the **File Size** or the time period specified in the **Duration** field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the **File Suffix** field's setting to avoid this.

IP reputation doesn't work on IPv6 addresses.

At the time of writing, IP reputation is only for IPv4 addresses. See Chapter 29 on page 556 for more information.

The SecuReporter banner keeps showing up.

See SecuReporter Banner on page 729 for more information.

44.1 Resetting the Zyxel Device

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

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

Note: This procedure removes the current configuration.

1 Make sure the **SYS** LED is on and not blinking.

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

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

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

44.2 Getting More Troubleshooting Help

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

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 *http://www.zyxel.com/homepage.shtml* and also *http://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.
- http://www.zyxel.cn

India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- Zyxel Kazakhstan
- http://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
- http://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

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

Europe

Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Belarus

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

Belgium

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

Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

Estonia

- Zyxel Estonia
- http://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- http://www.zyxel.fi

France

- Zyxel France
- http://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

Norway

- Zyxel Communications
- http://www.zyxel.no

Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

Romania

- Zyxel Romania
- http://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- http://www.zyxel.ru

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

Sweden

- Zyxel Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

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

UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

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

Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

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

Oceania

Australia

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

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

APPENDIX B
Product Features

Please refer to the product datasheet for the latest product features.

Version	4.35	4.35	4.35	4.35
Model Name	**ATP100**	**ATP200**	**ATP500**	**ATP800**
# Of MAC	6	7	7	14
Interface				
VLAN	8	16	64	128
Virtual (Alias)	4 per interface	4 per interface	4 per interface	4 per interface
PPP (System Default)	2	3	8	8
PPP (User Created)	2	4	16	32
Bridge	2	8	16	16
Tunnel (GRE/IPv6 Transition)	4	4	4	4
Routing				
Static Route	64	128	256	512
Policy Route	100	500	500	1000
Reserved Sessions For Managed Devices	500	500	500	500
Max OSPF Areas	10	10	10	10
Max. BGP Neighbor	5	5	5	5
BGP Max. Network	16	16	16	16
Sessions				
Max. TCP Concurrent Sessions (Forwarding, NAT/Firewall)	300,000	600,000	1,000,000	2,000,000
Session Rate	4,000	8,000	12,000	15,000
NAT				
Max. Virtual Server Number	128	256	1024	1024
Firewall (Secure Policy)				
Max Firewall ACL Rule Number = Secure Policy Number	500	500	2000	5000
Max Session Limit per Host Rules	1000	1000	1000	1000
ADP				
Max. ADP Profile Number	8	32	32	32
Max. ADP Rule Number	32	32	32	32
Application Patrol				
Max. App Patrol Number	32	32	64	96
Max. Application Object In Each Profile (Object + Object Group)	32	32	64	96
User Profile				
Max. Local User	64	128	128	512
Max. Admin User	5	5	5	10
Max. User Group	16	32	32	128
Max User In One User Group	64	128	128	512
Default Concurrent Device Login	64	100	200	800
Max. Concurrent Device Upgrade (License)	64	128	200	800
HTTPd				
Max HTTPd Number	128	256	512	512
Objects				
Address Object	300	300	1000	2000
Address Group	25	50	200	400
Max. Address Object In One Group	64	128	128	256

Service Object	200	500	1000	1000
Service Group	50	100	200	200
Max. Service Object In One Group	64	128	128	256
Schedule Object	32	32	32	32
Schedule Group	16	16	16	16
Max. Schedule Object In One Group	24	24	24	24
Application Object	500	500	1000	1000
Application Group	100	100	200	200
Max. Application Object In One Group	128	128	128	256
ISP Account	16 (PPP+3G)	16(PPP+3G)	32(PPP+3G)	32
Max. LDAP Server Object #	2	8	16	16
Max. RADIUS Server Object #	2	8	16	16
Max. Ad Server Object #	4	8	16	16
Max. Zone Number (System Default)	8	9	9	8
Max. Zone Number (User Defined)	8	16	16	32
Trunk				
Max. Trunk Number (System Default)	1	1	1	1
Max. Trunk Number (User Defined)	4	8	16	32
Max. Member Number Per Trunk	4+8	4+8	16+8	32+8
VPN				
Max. VPN Tunnels Number	40	40	300	1000
Max. VPN Concentrator Number	2	2	16	32
Max. VPN Configuration Provision Rule Number	40	40	300	1000
Certificate				
Certificate Buffer Size	128k	256k	512k	512k
Built-In Service				
A Record	64	64	128	128
NS Record (DNS Domain Zone Forward)	8	16	16	16
MX Record	8	8	16	16
Max Service Control Entries	16 per service	16 per service	32 per service	32 per service
Max. DHCP Network Pool	vlan+brg+ethernet	vlan+brg+ethernet	vlan+brg+ethernet	vlan+brg+ethernet
Max. DHCP Host Pool (Static DHCP)	96	256	512	1024
Max. DHCP Extended Options	10	15	30	30
Max DDNS Profiles	10	10	10	10
DHCP Relay	2 per interface	2 per interface	2 per interface	2 per interface
USB Storage				
Device Number	1	1	1	1
Centralized Log				
Log Entries	512	1024	1024	2048
Debug Log Entries	1024	1024	1024	1024
Admin E-Mail Address	2	2	2	2
Syslog Server	4	4	4	4
IDP				
Max. IDP Profile Number	1	1	1	16
Max. Custom Signatures	32	32	256	512
SSL Inspection				
Max. SSL Inspection Profile	6	8	16	16
Max. Exclude List	128	256	256	256
Content Filtering				
Max. Number Of Content Filter Policies	16	16	32	64
Forbidden Domain Entry Number	256 per profiles	256 per profiles	512 per profiles	512 per profiles
Trusted Domain Entry Number	256 per profiles	256 per profiles	512 per profiles	512 per profiles
Keyword Blocking Number	128 per profiles	128 per profiles	256 per profiles	256 per profiles

Common Forbidden Domain Entry Number	1024	1024	1024	1024
Common Trusted Domain Entry Number	1024	1024	1024	1024
Email Security				
Maximum AS Rule Number (Profile)	1	1	1	1
Maximum White List Rule Support	128	128	128	256
Maximum Black List Rule Support	128	128	128	256
Maximum DNSBL Domain Support	5	5	5	10
Concurrent Mail Session Scanning	200	200	200	200
Max. Statistics Number	500	500	500	500
Max. Statistics Ranking	10	10	10	10
Anti-Malware				
Max. AV Rule (Profile)	1	1	1	1
Max. Statistics Number	500	500	500	500
Max. Statistics Ranking	10	10	10	10
SandBoxing				
Support protocol	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP
Concurrent File Collect Capability	64	64	64	N/A
upload file size	Up to10MB	Up to10MB	Up to10MB	Up to10MB
SSL VPN				
Default SSL VPN Connections	10	10	50	100
Maximum SSL VPN Connections	10	10	50	100
Max. SSL VPN Network List	8	8	8	8
SSL VPN Max Policy	16	16	16	16
AP Controller				
Default # Of Control AP	2	2	2	2
Max. # Of Control AP	10	18	34	130
Max Radio Profile	32	32	64	128
Max SSID Profile	32	128	128	1024
Max Security Profile	32	128	128	1024
Max MAC Filter Profile	32	32	32	32
MAX MAC Entry Per MAC Filter Profile	512	512	512	512
Zymesh	32	32	32	32
BWM				
Maximum BWM Rule Number	128	256	512	1024
BWM Per Source IP (Max.)	256	1024	1024	2048
SIP				
Maximum SIP Concurrent Call	50	100	100	100
Custom Web Portal Page				
Max Internal Web Portal Customize File	4	4	4	4
Upload Zip File Size	Up to 2MB	Up to 2MB	Up to 2MB	Up to 2MB
Unzip File Size	Up to 5MB	Up to 5MB	Up to 5MB	Up to 5MB

APPENDIX C
Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

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

Disclaimer

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

Regulatory Notice and Statement (Class B)

Model List: ATP100, ATP100W, ATP200

UNITED STATES of AMERICA

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

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

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

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 22 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

CANADA

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

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

EUROPEAN UNION

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

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

Model List: ATP100W

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.

List of national codes

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

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.

- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- CLASS 1 LASER PRODUCT
- APPAREIL À LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Environment Statement

ErP (Energy-related Products)

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

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

European Union - Disposal and Recycling Information

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

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

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

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

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

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

台灣

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。

- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
    - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
    - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

以下訊息僅適用於產品具有無線功能且銷售至台灣地區 (ATP100W)

- 第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
- 前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Notice and Statement (Class A)

Model List: ATP500, ATP700, ATP800

United States of America

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

FCC EMC Statement

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

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

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This device has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

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

Innovation, Science and Economic Development Canada Industry ICES Statement

CAN ICES-3 (A)/NMB-3(A)

European Union

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

CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

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

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Caution: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- This equipment must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- CLASS 1 LASER PRODUCT
- APPAREIL À LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Environment Statement

European Union - Disposal and Recycling Information

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

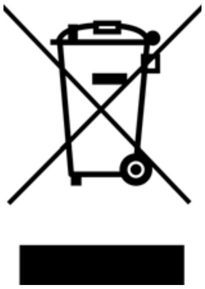
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung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

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

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

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

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



台灣

警告使用者

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。

- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index