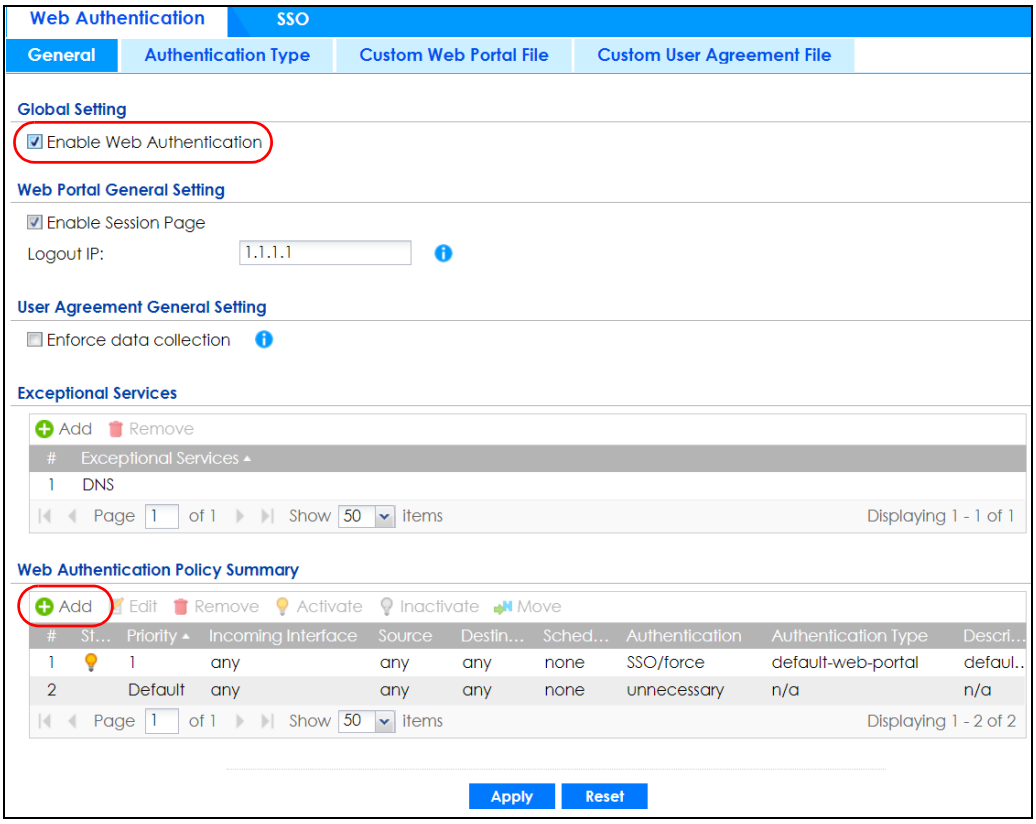
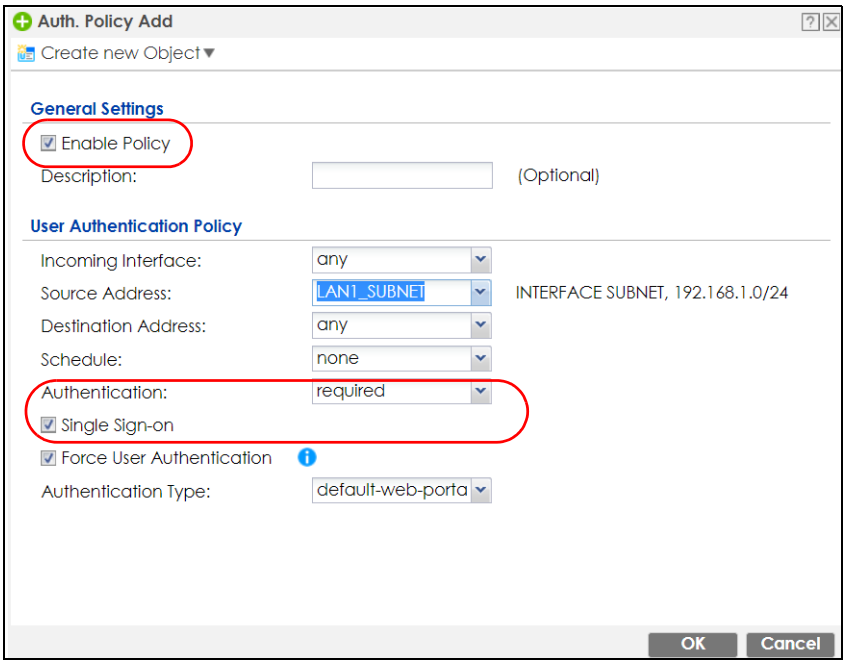


Make sure you select **Enable Policy, Single Sign-On** and choose **required** in **Authentication**.

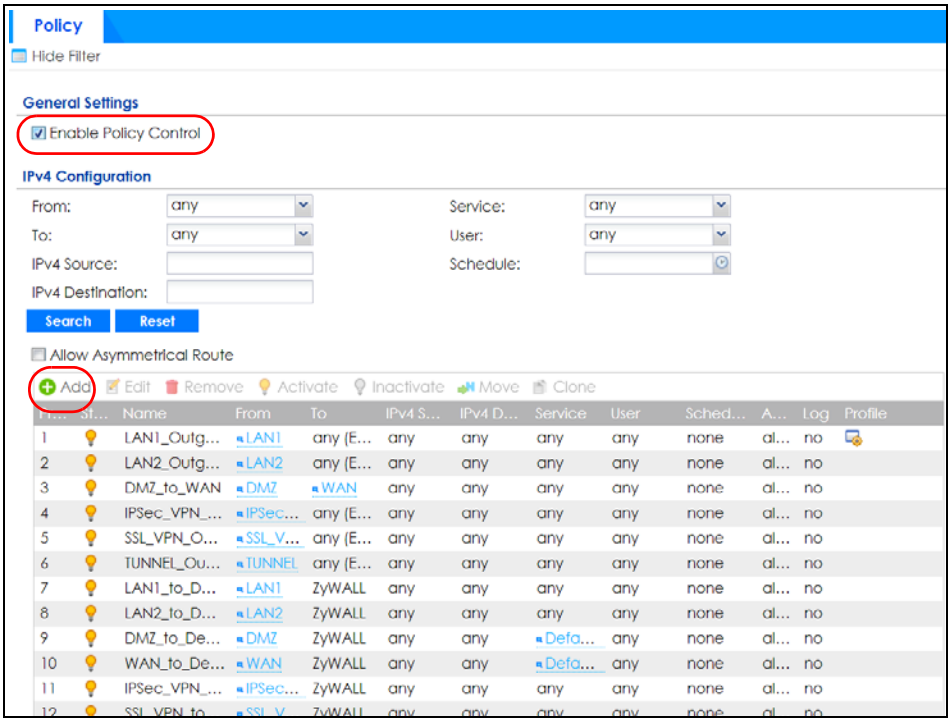
Do NOT select **any** as the **source address** unless you want all incoming connections to be authenticated!



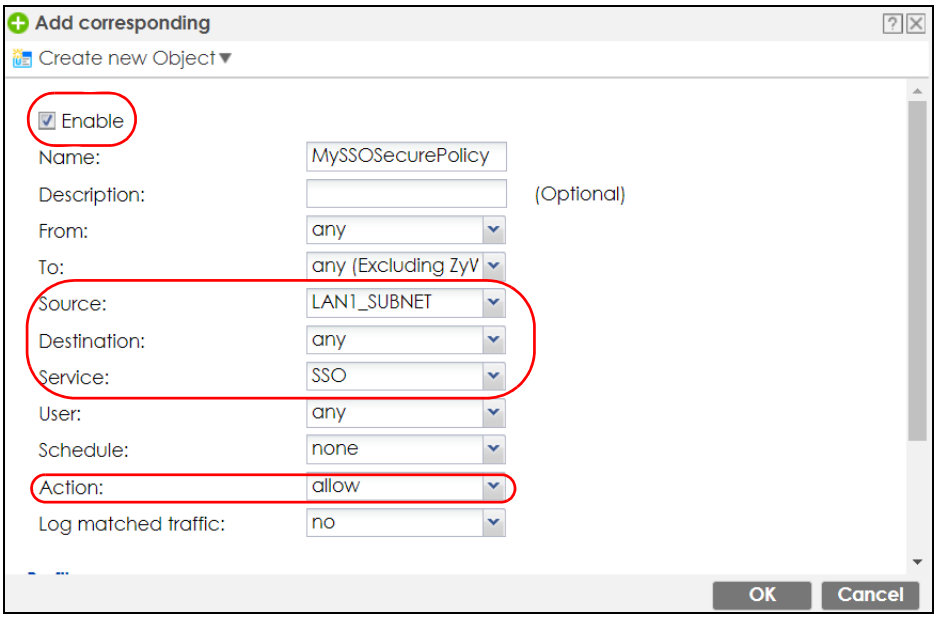
See Table 184 on page 462 and Table 185 on page 465 for more information on configuring these screens.

24.4.4 Create a Security Policy

Configure a Security Policy for SSO traffic source and destination direction in order to prevent the security policy from blocking this traffic. Go to **Configuration > Security Policy > Policy Control** and add a new policy if a default one does not cover the SSO web authentication traffic direction.

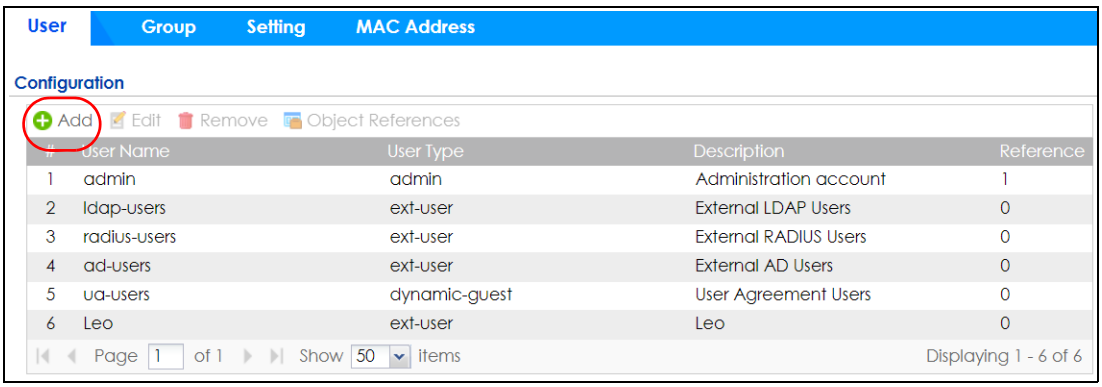


Configure the fields as shown in the following screen. Configure the source and destination addresses according to the SSO web authentication traffic in your network.

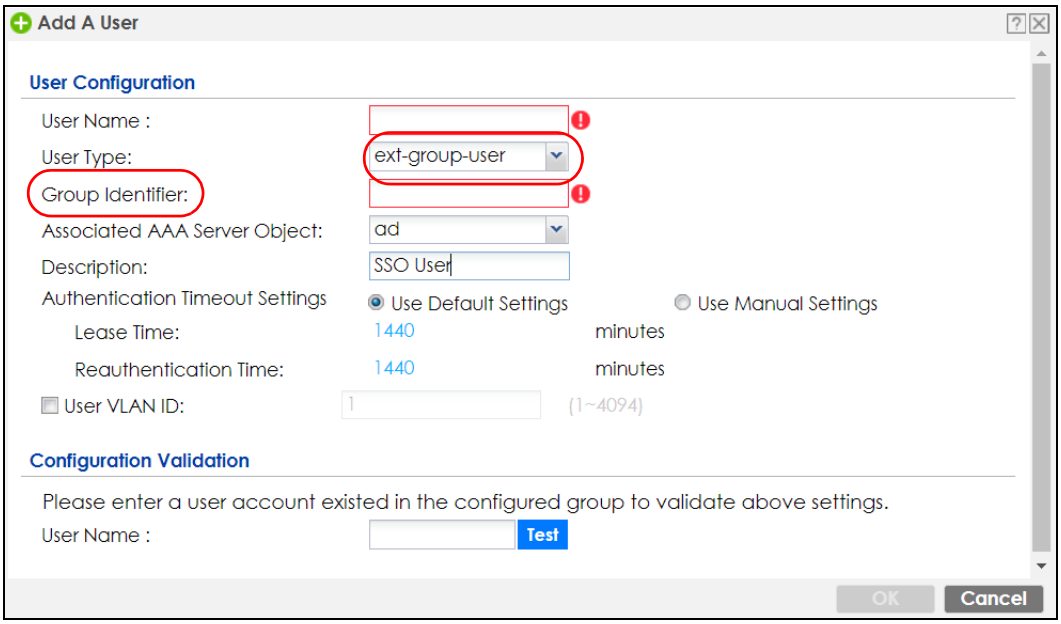


24.4.5 Configure User Information

Configure a **User** account of the **ext-group-user** type.

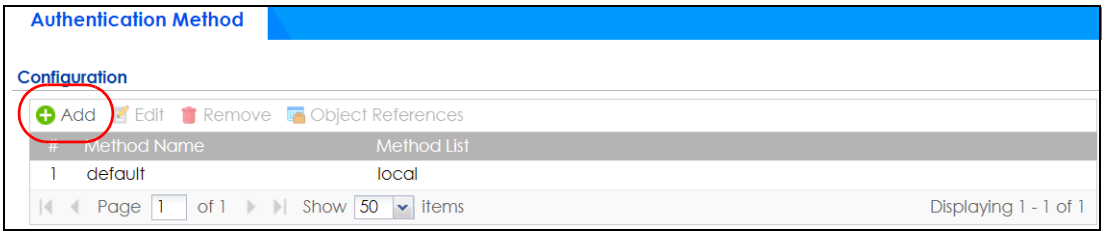


Configure **Group Identifier** to be the same as **Group Membership** on the SSO agent.

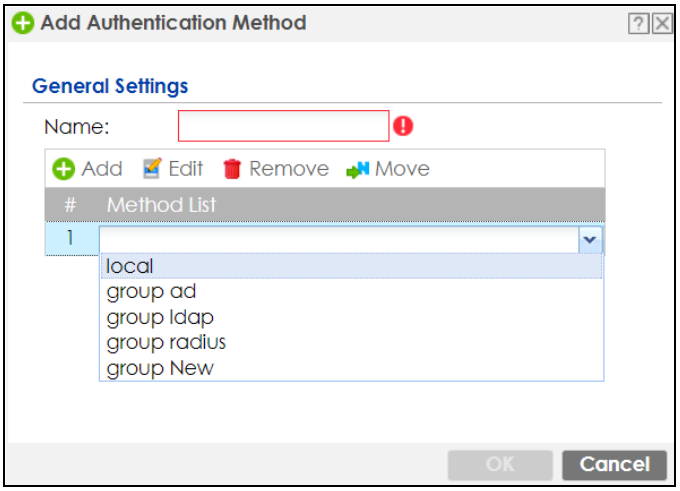


24.4.6 Configure an Authentication Method

Configure Active Directory (AD) for authentication with SSO.

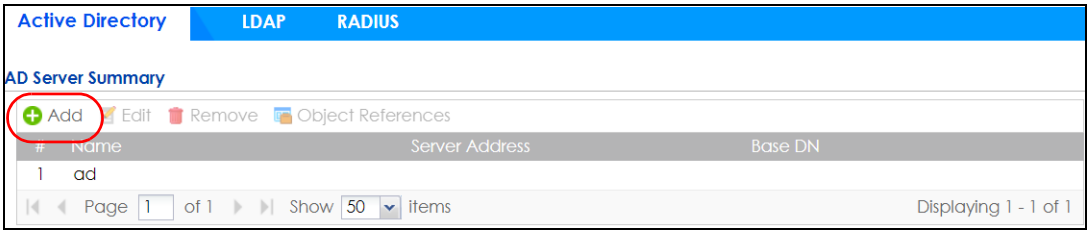


Choose **group ad** as the authentication server for SSO.

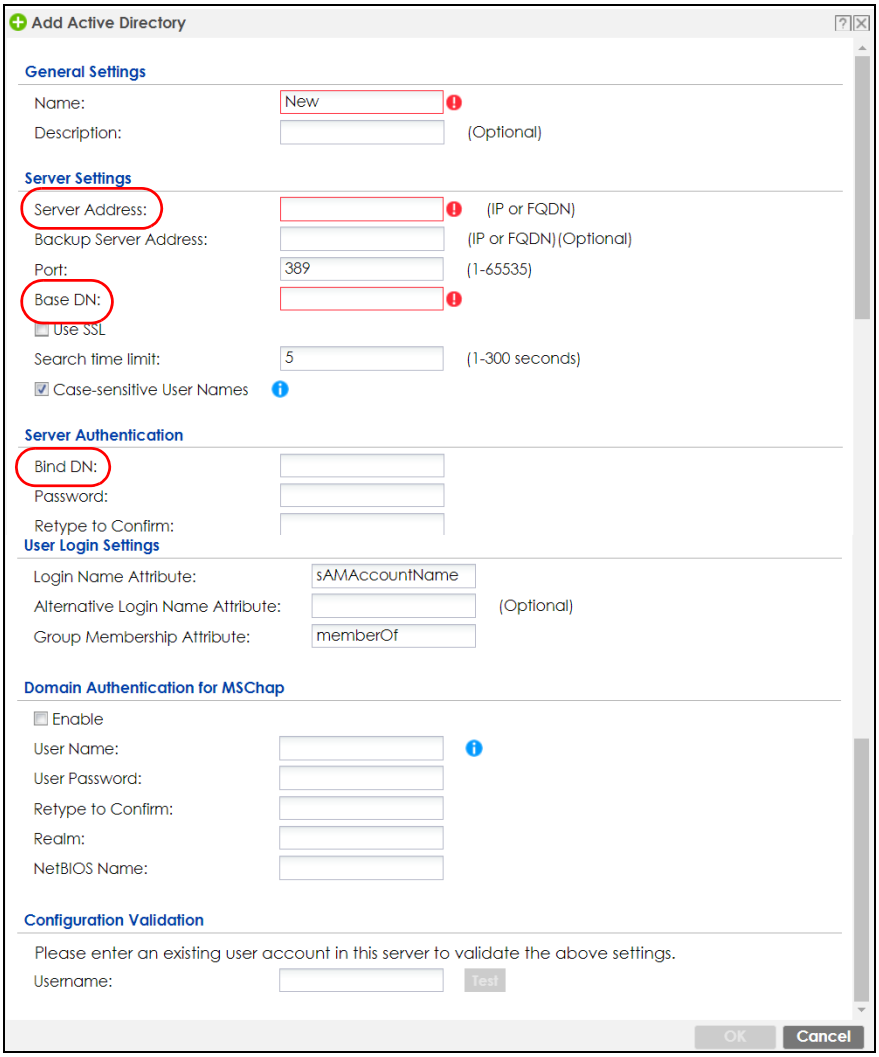


24.4.7 Configure Active Directory

You must configure an Active Directory (AD) server in **AAA Setup** to be the same as AD configured on the SSO agent.



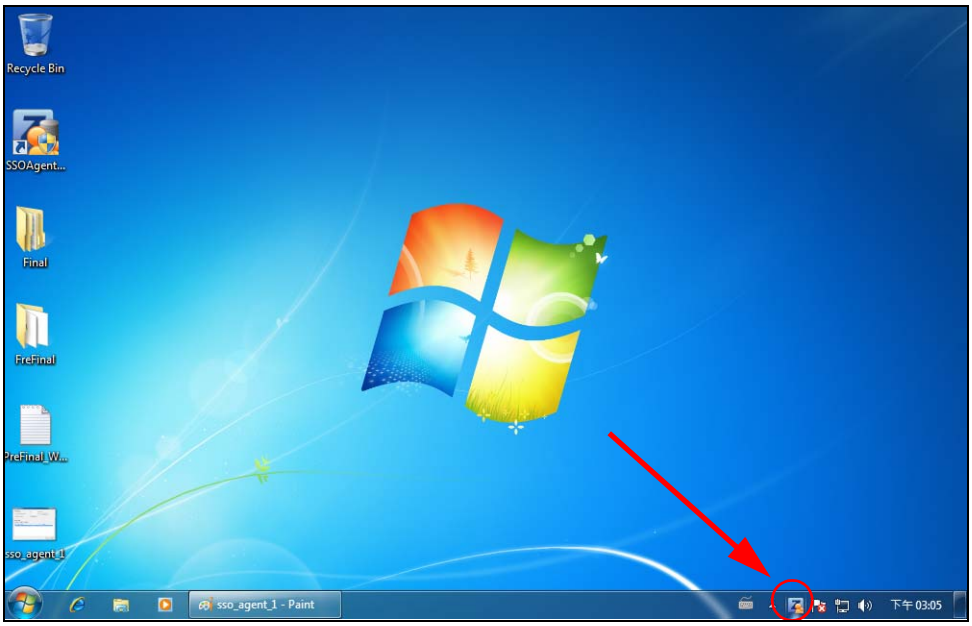
The default AD server port is 389. If you change this, make sure you make the same changes on the SSO. Configure the **Base DN** exactly the same as on the Domain Controller and SSO. **Bind DN** is a user name and password that allows the Zyxel Device to join the domain with administrative privileges. It is a required field.



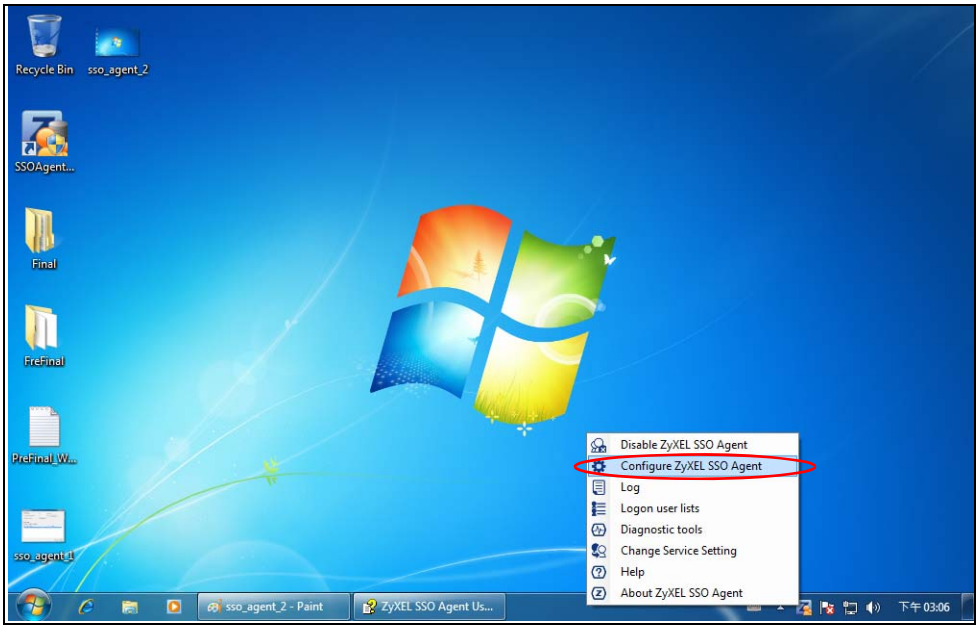
24.5 SSO Agent Configuration

This section shows what you have to do on the SSO agent in order to work with the Zyxel Device.

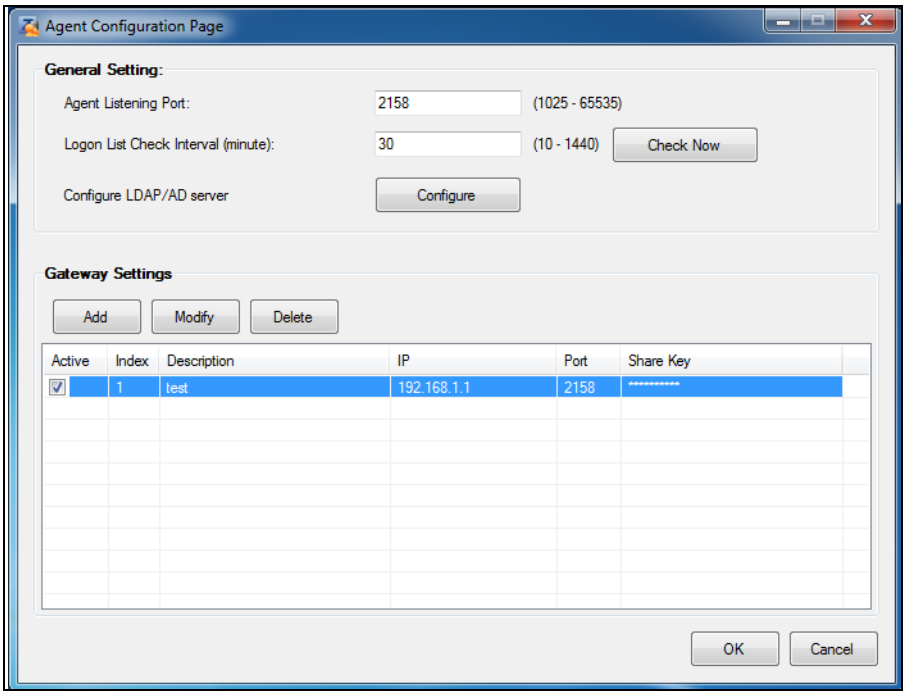
After you install the SSO agent, you will see an icon in the system tray (bottom right of the screen)



Right-click the SSO icon and select **Configure Zyxel SSO Agent**.

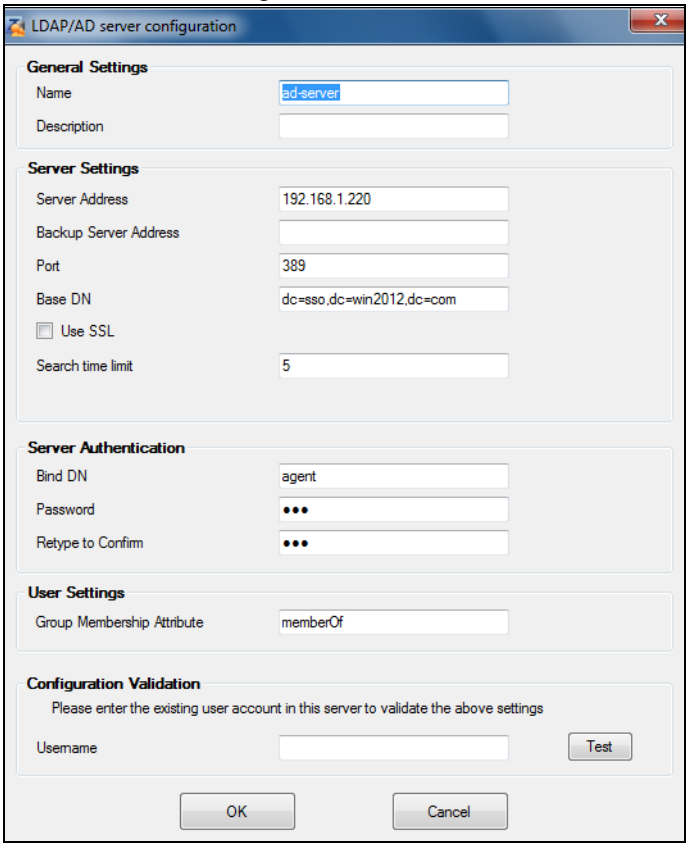


Configure the **Agent Listening Port**, **AD server** exactly as you have done on the Zyxel Device. Add the Zyxel Device IP address as the **Gateway**. Make sure the Zyxel Device and SSO agent are able to communicate with each other.

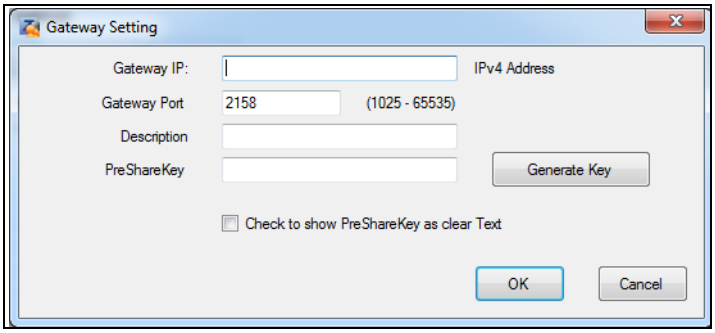


Configure the **Server Address**, **Port**, **Base DN**, **Bind DN**, **Login Name Attribute** and **Group Membership** for the AD server settings exactly as you have done on the Zyxel Device. **Group Membership** is called **Group Identifier** on the Zyxel Device.

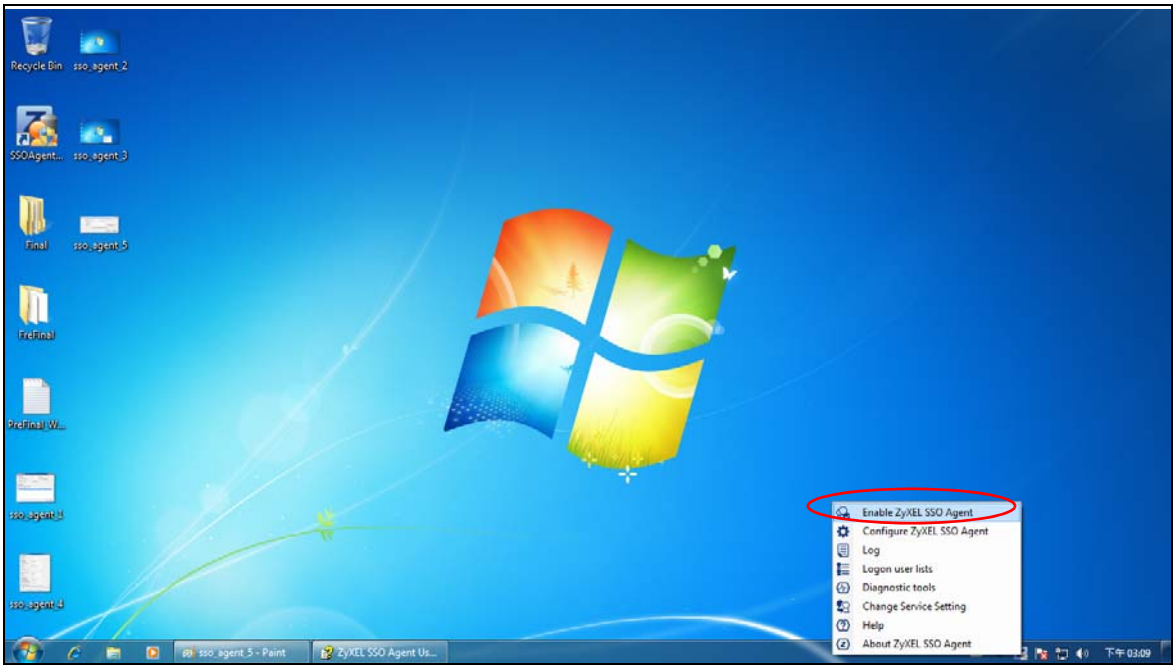
LDAP/AD Server Configuration



Configure the **Gateway IP** address, **Gateway Port** and **PreShareKey** exactly as you have done in the Zyxel Device **Configuration > Web Authentication > SSO** screen. If you want to use **Generate Key** to have the SSO create a random password, select **Check** to show **PreShareKey** as clear Text so as to see the password, then copy and paste it to the Zyxel Device.



After all SSO agent configurations are done, right-click the SSO icon in the system tray and select **Enable Zyxel SSO Agent**.



CHAPTER 25
Security Policy

25.1 Overview

A security policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

The policy can be configured:

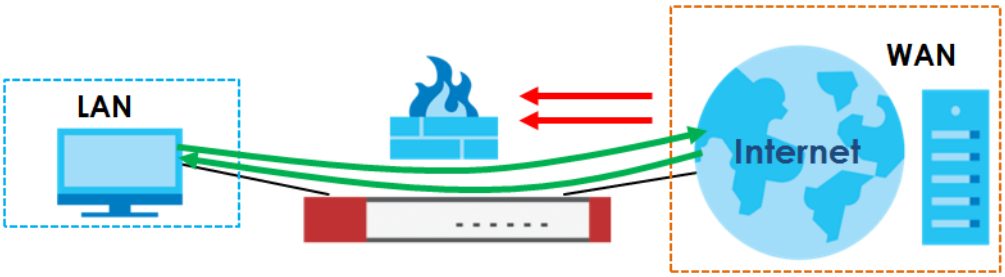
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the profiles (application patrol, content filter, IDP, anti-malware, email security) to traffic that matches the criteria above

Note: Security policies can be applied to both IPv4 and IPv6 traffic.

The security policies can also limit the number of user sessions.

The following example shows the Zyxel Device's default security policies behavior for a specific direction of travel of packets. WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the Zyxel Device allows the response. However, the Zyxel Device blocks incoming Telnet traffic initiated from the WAN zone and destined for the LAN zone.

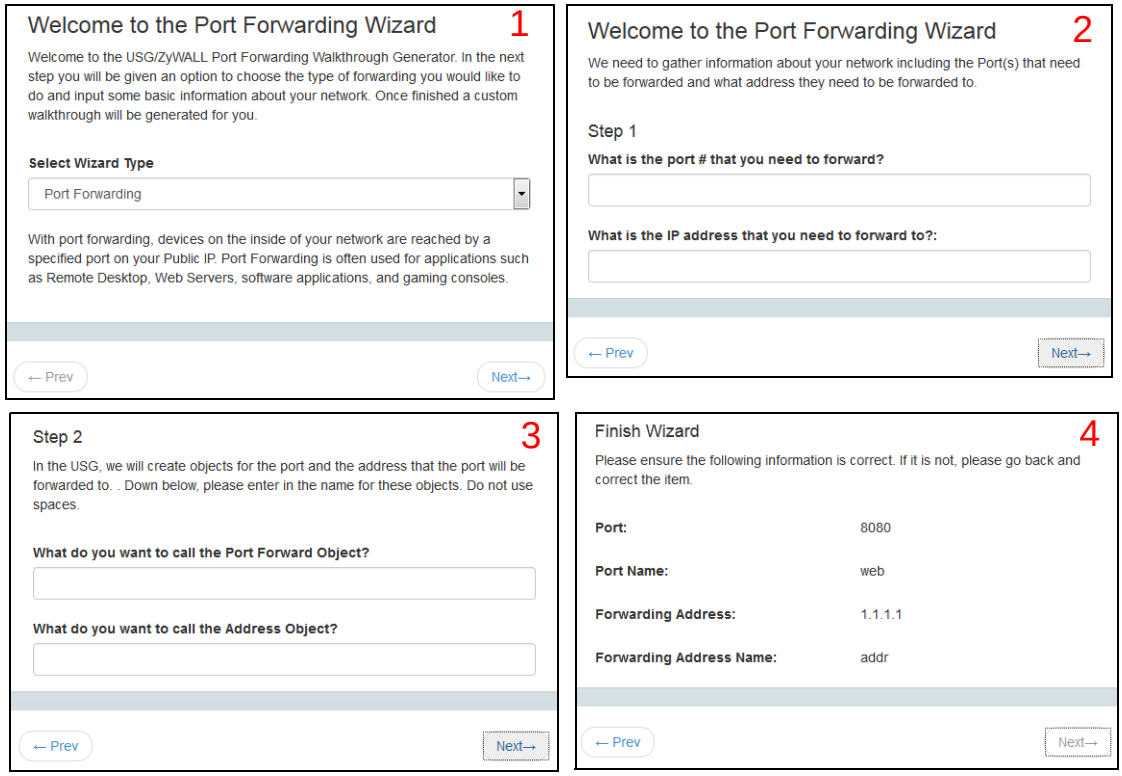
Figure 341 Default Directional Security Policy Example



25.2 One Security

OneSecurity is a website with guidance on configuration walkthroughs, troubleshooting, and other information. This is an example of a port forwarding configuration walkthrough.

Figure 342 Example of a Port Forwarding Configuration Walkthrough.



This is an example of L2TP over IPSec VPN Troubleshooting troubleshooting.

Figure 343 Example of L2TP over IPSec Troubleshooting - 1

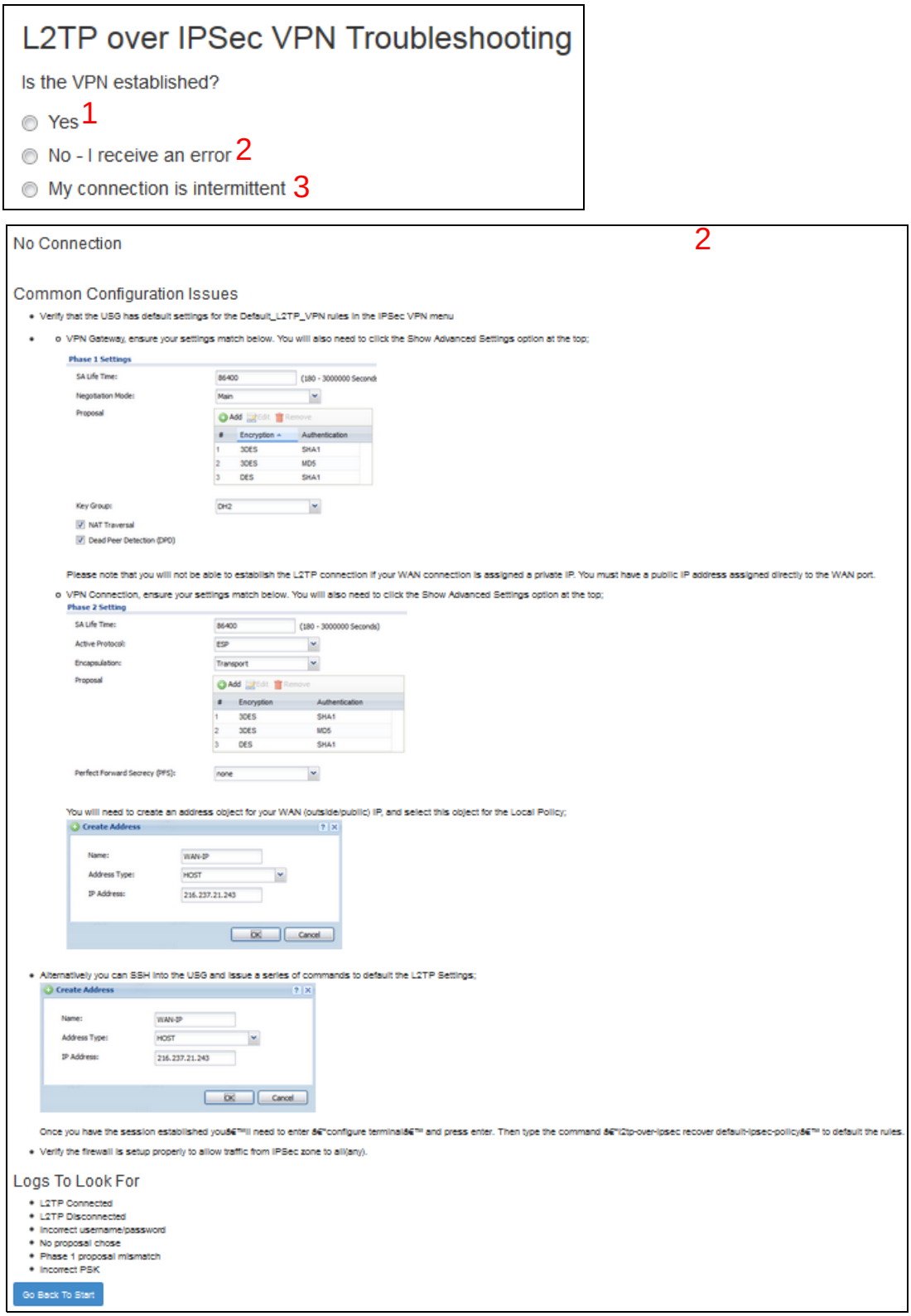
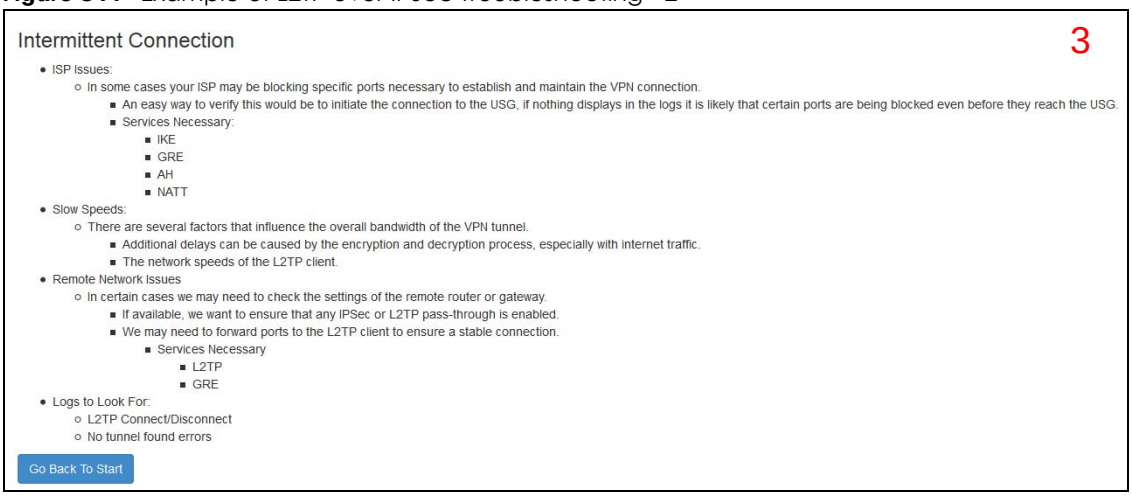


Figure 344 Example of L2TP over IPSec Troubleshooting - 2



In the Zyxel Device, you will see icons that link to OneSecurity walkthroughs, troubleshooting and so on in certain screens.

For example, at the time of writing, these are the OneSecurity icons you can see.

Table 191 OneSecurity Icons

ONESECURITY ICON	SCREEN
Configuration Walkthrough	Click this icon to go to a series of screens that guide you how to configure the feature. Note that the walkthroughs do not perform the actual configuring, but just show you how to do it. • Device HA > General • Licensing > Registration • Network > NAT • Network > Routing > Policy Route • Security Service > App Patrol • Security Service > Content Filter • Security Service > IDP • Security Service > Anti-Malware • Security Service > Email Security • VPN > IPSec VPN • VPN > SSL VPN • VPN > L2TP VPN
Troubleshooting	Click this icon to go to a series of screens that guide you how to fix problems with the feature. • Device HA > General • Network > NAT • Network > Routing > Policy Route • Security Service > App Patrol • Security Service > Content Filter • Security Service > IDP • Security Service > Anti-Malware • Security Service > Email Security • VPN > IPSec VPN • VPN > SSL VPN • VPN > L2TP VPN

Table 191 OneSecurity Icons (continued)

ONESECURITY ICON	SCREEN
Application Patrol	Click this icon for more information on Application Patrol, which identifies traffic that passes through the Zyxel Device, so you can decide what to do with specific types of traffic. Traffic not recognized by application patrol is ignored. • Security Service > Application Patrol
Content Filter	Click this icon for more information on Content Filter, which controls access to specific web sites or web content. • Security Service > Content Filter
VPN	Click this icon for more information on IPSec and SSL VPN. Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. SSL VPN allows users to use a web browser for secure remote user login without need of a VPN router or VPN client software. • VPN > IPSec VPN • VPN > SSL VPN
Download VPN Client	Click this icon to download VPN client software. • VPN > IPSec VPN • VPN > SSL VPN
Wireless AP Controller	Click this icon for more information on the Wireless AP Controller which sets how the Zyxel Device allows APs to connect to the wireless network. • Wireless > AP Management > Mgnt. AP List

25.3 What You Can Do in this Chapter

- Use the **Security Policy Control** screens (Section 25.4 on page 495) to enable or disable policies, asymmetrical routes, and manage and configure policies.
- Use the **Anomaly Detection and Prevention** (ADP) screens (Section 25.5 on page 501) to detect traffic with protocol anomalies and take appropriate action.
- Use the **Session Control** screens (see Section 25.5 on page 501) to limit the number of concurrent NAT/security policies traffic sessions a client can use.

25.3.1 What You Need to Know

Stateful Inspection

The Zyxel Device uses stateful inspection in its security policies. The Zyxel Device restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces. Group the Zyxel Device's interfaces into different zones based on your needs. You can configure security policies for data passing between zones or even between interfaces.

Default Directional Security Policy Behavior

Security Policies can be grouped based on the direction of travel of packets to which they apply. Here is the The Zyxel Device has default Security Policy behavior for traffic going through the Zyxel Device in various directions.

Table 192 Directional Security Policy Behavior

FROM ZONE TO ZONE	BEHAVIOR
From any to Device	DHCP traffic from any interface to the Zyxel Device is allowed.
From LAN1 to any (other than the Zyxel Device)	Traffic from the LAN1 to any of the networks connected to the Zyxel Device is allowed.
From LAN2 to any (other than the Zyxel Device)	Traffic from the LAN2 to any of the networks connected to the Zyxel Device is allowed.
From LAN1 to Device	Traffic from the LAN1 to the Zyxel Device itself is allowed.
From LAN2 to Device	Traffic from the LAN2 to the Zyxel Device itself is allowed.
From WAN to Device	The default services listed in To-Device Policies are allowed from the WAN to the Zyxel Device itself. All other WAN to Zyxel Device traffic is dropped.
From any to any	Traffic that does not match any Security policy is dropped. This includes traffic from the WAN to any of the networks behind the Zyxel Device. This also includes traffic to or from interfaces that are not assigned to a zone (extra-zone traffic).

To-Device Policies

Policies with **Device** as the **To Zone** apply to traffic going to the Zyxel Device itself. By default:

- The Security Policy allows only LAN, or WAN computers to access or manage the Zyxel Device.
- The Zyxel Device allows DHCP traffic from any interface to the Zyxel Device.
- The Zyxel Device drops most packets from the WAN zone to the Zyxel Device itself and generates a log except for AH, ESP, GRE, HTTPS, IKE, NATT.

When you configure a Security Policy rule for packets destined for the Zyxel Device itself, make sure it does not conflict with your service control rule. The Zyxel Device checks the security policy before the service control rules for traffic destined for the Zyxel Device.

A **From Any To Device** direction policy applies to traffic from an interface which is not in a zone.

Global Security Policies

Security Policies with **from any** and/or **to any** as the packet direction are called global Security Policies. The global Security Policies are the only Security Policies that apply to an interface that is not included in a zone. The **from any** policies apply to traffic coming from the interface and the **to any** policies apply to traffic going to the interface.

Security Policy Rule Criteria

The Zyxel Device checks the schedule, user name (user's login name on the Zyxel Device), source IP address and object, destination IP address and object, IP protocol type of network traffic (service) and Security Service profile criteria against the Security Policies (in the order you list them). When the traffic matches a policy, the Zyxel Device takes the action specified in the policy.

User Specific Security Policies

You can specify users or user groups in Security Policies. For example, to allow a specific user from any computer to access a zone by logging in to the Zyxel Device, you can set up a policy based on the user name only. If you also apply a schedule to the Security Policy, the user can only access the network at the scheduled time. A user-aware Security Policy is activated whenever the user logs in to the Zyxel Device and will be disabled after the user logs out of the Zyxel Device.

Session Limits

Accessing the Zyxel Device or network resources through the Zyxel Device requires a NAT session and corresponding Security Policy session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the Zyxel Device. The Zyxel Device lets you limit the number of concurrent NAT/Security Policy sessions a client can use.

25.4 The Security Policy Screen

Asymmetrical Routes

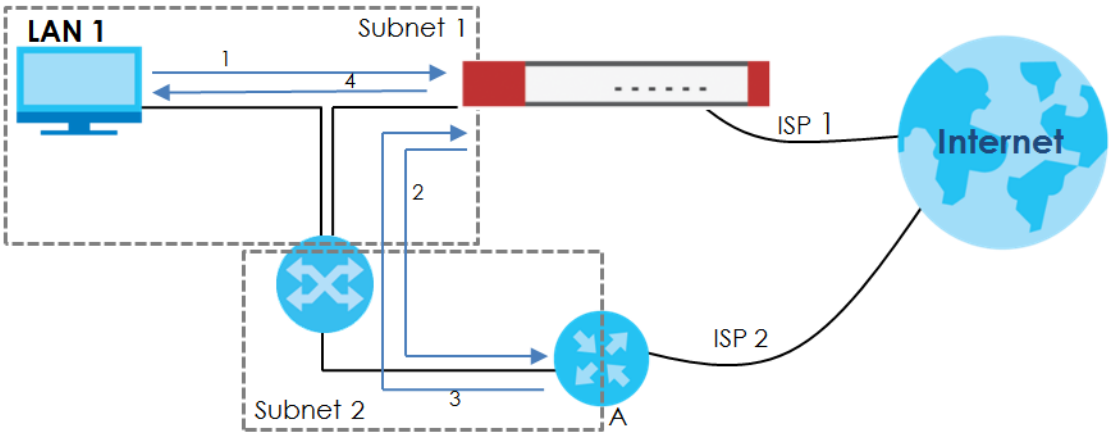
If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged.

You can have the Zyxel Device permit the use of asymmetrical route topology on the network (not reset the connection). However, 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. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the Zyxel Device to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The Zyxel Device reroutes the packet to gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the Zyxel Device.
4. The Zyxel Device then sends it to the computer on the LAN1 in **Subnet 1**.

Figure 345 Using Virtual Interfaces to Avoid Asymmetrical Routes



25.4.1 Configuring the Security Policy Control Screen

Click **Configuration > Security Policy > Policy Control** to open the **Security Policy** screen. Use this screen to enable or disable the Security Policy and asymmetrical routes, set a maximum number of sessions per host, and display the configured Security Policies. Specify from which zone packets come and to which zone packets travel to display only the policies specific to the selected direction. Note the following.

- Besides configuring the Security Policy, you also need to configure NAT rules to allow computers on the WAN to access LAN devices.
- The Zyxel Device applies NAT (Destination NAT) settings before applying the Security Policies. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding Security Policy to allow the traffic, you need to set the LAN IP address as the destination.
- The ordering of your policies is very important as policies are applied in sequence.

The following screen shows the Security Policy summary screen.

Figure 346 Configuration > Security Policy > Policy Control

Policy

Hide Filter

General Settings

Enable Policy Control

IPv4 Configuration

From: any | Service: any
To: any | User: any
IPv4 Source: | Schedule:
IPv4 Destination:

Search Reset

Allow Asymmetrical Route

Add Edit Remove Activate Inactivate Move Clone

Pr...	St...	Name	From	To	IPv4 S...	IPv4 D...	Service	User	Sched...	A...	Log	Profile
1		LAN1_Outg...	LAN1	any (E...	any	any	any	any	none	al...	no	
2		LAN2_Outg...	LAN2	any (E...	any	any	any	any	none	al...	no	
3		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	al...	no	
4		IPSec_VPN_...	IPSec...	any (E...	any	any	any	any	none	al...	no	
5		SSL_VPN_O...	SSL_...	any (E...	any	any	any	any	none	al...	no	
6		TUNNEL_Ou...	TUNNEL	any (E...	any	any	any	any	none	al...	no	
7		LAN1_to_D...	LAN1	ZyWALL	any	any	any	any	none	al...	no	
8		LAN2_to_D...	LAN2	ZyWALL	any	any	any	any	none	al...	no	
9		DMZ_to_De...	DMZ	ZyWALL	any	any	Defa...	any	none	al...	no	
10		WAN_to_D...	WAN	ZyWALL	any	any	Defa...	any	none	al...	no	
11		IPSec_VPN_...	IPSec...	ZyWALL	any	any	any	any	none	al...	no	
12		SSL_VPN_to...	SSL_...	ZyWALL	any	any	any	any	none	al...	no	
13		TUNNEL_to_...	TUNNEL	ZyWALL	any	any	any	any	none	al...	no	
D...			any	any	any	any	any	any	none	d...	log	

Page 1 of 1 Show 50 items Displaying 1 - 14 of 14

IPv6 Configuration

From: any | Service: any
To: any | User: any
Source: | Schedule:
Destination:

Search Reset

Allow Asymmetrical Route

Add Edit Remove Activate Inactivate Move Clone

Pr...	St...	Name	From	To	IPv6 S...	IPv6 D...	Service	User	Sched...	A...	Log	Profile
1		Device_Def...	any	ZyWALL	any	any	Defa...	any	none	al...	no	
2		LAN1_Outg...	LAN1	any (E...	any	any	any	any	none	al...	no	
3		LAN2_Outg...	LAN2	any (E...	any	any	any	any	none	al...	no	
4		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	al...	no	
5		IPSec_VPN_...	IPSec...	any (E...	any	any	any	any	none	al...	no	
6		SSL_VPN_O...	SSL_...	any (E...	any	any	any	any	none	al...	no	
7		TUNNEL_Ou...	TUNNEL	any (E...	any	any	any	any	none	al...	no	
8		LAN1_to_D...	LAN1	ZyWALL	any	any	any	any	none	al...	no	
9		LAN2_to_D...	LAN2	ZyWALL	any	any	any	any	none	al...	no	
10		DMZ_to_De...	DMZ	ZyWALL	any	any	Defa...	any	none	al...	no	
11		WAN_to_D...	WAN	ZyWALL	any	any	Defa...	any	none	al...	no	
12		IPSec_VPN_...	IPSec...	ZyWALL	any	any	any	any	none	al...	no	
13		SSL_VPN_to...	SSL_...	ZyWALL	any	any	any	any	none	al...	no	
14		TUNNEL_to_...	TUNNEL	ZyWALL	any	any	any	any	none	al...	no	
D...			any	any	any	any	any	any	none	d...	log	

Page 1 of 1 Show 50 items Displaying 1 - 15 of 15

Apply Reset

The following table describes the labels in this screen.

Table 193 Configuration > Security Policy > Policy Control

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click **Show Filter** to display IPv4 and IPv6 (if enabled) security policy search filters.
General Settings	Enable or disable the Security Policy feature on the Zyxel Device.
Enable Policy Control	Select this to activate Security Policy on the Zyxel Device to perform access control.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. **any** means all zones.
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
IPv4/IPv6 Policy Management	Use the following items to manage IPv4 and IPv6 policies.
Allow Asymmetrical Route	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. Select this check box to have the Zyxel Device permit the use of asymmetrical route topology on the network (not reset the connection). Note: 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.
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 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.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.

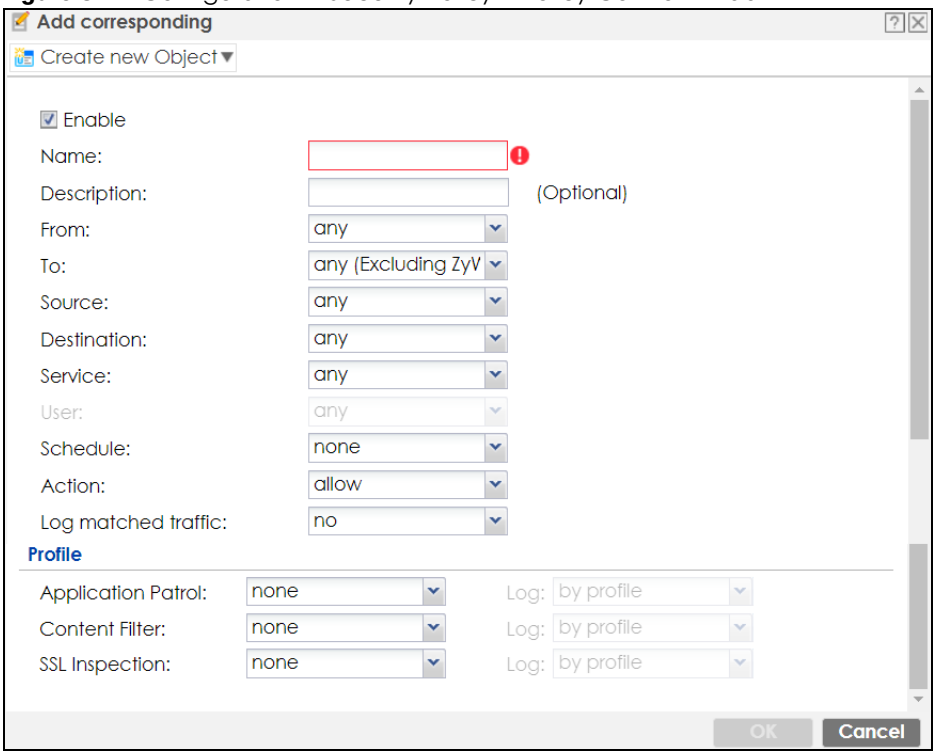
Table 193 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
Move	To change a policy's position in the numbered list, select the policy and click **Move** to display a field to type a number for where you want to put that policy and press [ENTER] to move the policy to the number that you typed. The ordering of your policies is important as they are applied in order of their numbering.
Clone	Use **Clone** to create a new entry by modifying an existing one. • Select an existing entry. • Click **Clone**, type a number where the new entry should go and then press [ENTER]. • A configuration copy of the selected entry pops up. You must at least change the name as duplicate entry names are not allowed.
The following read-only fields summarize the policies you have created that apply to traffic traveling in the selected packet direction.	
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. **Default** displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from **LAN** to **LAN** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From **any** displays all the Security Policies for traffic going to the selected **To Zone**. To **any** displays all the Security Policies for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the Security Policies. To **ZyWALL** policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. **none** means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (**deny**), permits the passage of packets (**allow**) or drops packets with notification (**reject**)
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or not (**no**) when the policy is matched to the criteria listed above.
Profile	This field shows you which Security Service profiles (application patrol, content filter, IDP, anti-malware, email security) apply to this Security policy. Click an applied Security Service profile icon to edit the profile directly.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

25.4.2 The Security Policy Control Add/Edit Screen

In the **Security Policy Control** screen, click the **Edit** or **Add** icon to display the **Security Policy Edit or Add** screen.

Figure 347 Configuration > Security Policy > Policy Control > Add



The following table describes the labels in this screen.

Table 194 Configuration > Security Policy > Policy Control > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to activate the Security policy.
Name	Type a name to identify the policy
Description	Enter a descriptive name of up to 60 printable ASCII characters for the Policy. Spaces are allowed.
From To	For through-Zyxel Device policies, select the direction of travel of packets to which the policy applies. **any** means all interfaces. **Device** means packets destined for the Zyxel Device itself.
Source	Select an IPv4 / IPv6 address or address group object, including geographic address and FQDN (group) objects, to apply the policy to traffic coming from it. Select **any** to apply the policy to all traffic coming from IPv4 / IPv6 addresses.
Destination	Select an IPv4 / IPv6 address or address group, including geographic address and FQDN (group) objects, to apply the policy to traffic going to it. Select **any** to apply the policy to all traffic going to IPv4 / IPv6 addresses.
Service	Select a service or service group from the drop-down list box.

Table 194 Configuration > Security Policy > Policy Control > Add (continued)

LABEL	DESCRIPTION
User	This field is not available when you are configuring a to-Zyxel Device policy. Select a user name or user group to which to apply the policy. The Security Policy is activated only when the specified user logs into the system and the policy will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select **none** and the policy is always effective.
Action	Use the drop-down list box to select what the Security Policy is to do with packets that match this policy. Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **reject** to discard the packets and send a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **allow** to permit the passage of the packets.
Log matched traffic	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or not (**no**) when the policy is matched to the criteria listed above..
Profile	Use this section to apply anti- x profiles (created in the **Configuration > Security Service** screens) to traffic that matches the criteria above. You must have created a profile first; otherwise **none** displays. Use **Log** to generate a log (**log**), log and alert (**log alert**) or not (**no**) for all traffic that matches criteria in the profile.
Application Patrol	Select an Application Patrol profile from the list box; **none** displays if no profiles have been created in the **Configuration > Security Service > App Patrol** screen.
Content Filter	Select a Content Filter profile from the list box; **none** displays if no profiles have been created in the **Configuration > Security Service > Content Filter** screen.
SSL Inspection	Select an SSL Inspection profile from the list box; **none** displays if no profiles have been created in the **Configuration > Security Service > SSL Inspection** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

25.5 Anomaly Detection and Prevention Overview

Anomaly Detection and Prevention (ADP) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces ADP, anomaly profiles and applying an ADP profile to a traffic direction.

Traffic Anomalies

Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-2 and layer-3. Traffic anomaly policies may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder

Protocol anomaly policies may be updated when you upload new firmware.

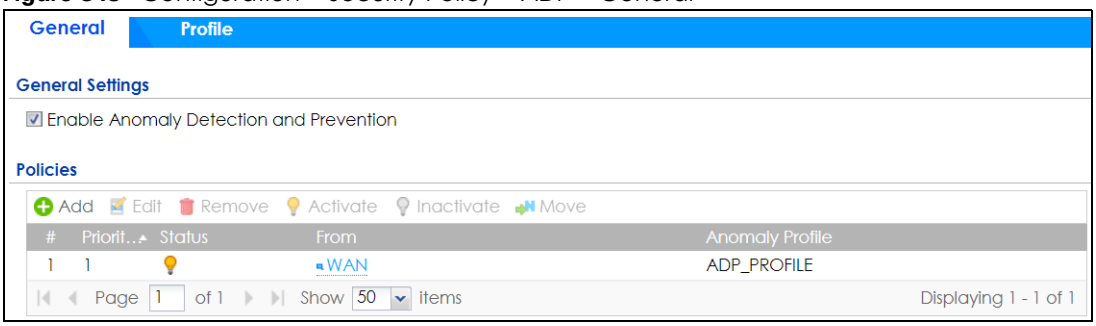
Note: First, create an ADP profile in the In the **Configuration > Security Policy > ADP** > **Profile** screen.

Then, apply the profile to traffic originating from a specific zone in the **Configuration > Security Policy > ADP** > **General** screen.

25.5.1 The Anomaly Detection and Prevention General Screen

Click **Configuration > Security Policy > ADP > General** to display the next screen.

Figure 348 Configuration > Security Policy > ADP > General



The following table describes the labels in this screen.

Table 195 Configuration > Security Policy > ADP > General

LABEL	DESCRIPTION
General Settings	
Enable Anomaly Detection and Prevention	Select this to enable traffic anomaly and protocol anomaly detection and prevention.
Add	Select an entry and click **Add** to append a new row beneath the one selected. ADP policies are applied in order (**Priority**) shown in this screen
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This is the entry's index number in the list.

Table 195 Configuration > Security Policy > ADP > General

LABEL	DESCRIPTION
Priority	This is the rank in the list of anomaly profile policies. The list is applied in order of priority.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
From	This is the direction of travel of packets to which an anomaly profile is bound. Traffic direction is defined by the zone the traffic is coming from. Use the **From** field to specify the zone from which the traffic is coming. Select **ZyWALL** to specify traffic coming from the Zyxel Device itself. **From LAN** means packets traveling from a computer on one LAN subnet to a computer on another subnet via the Zyxel Device's LAN1 zone interfaces. The Zyxel Device does not check packets traveling from a LAN computer to another LAN computer on the same subnet. **From WAN** means packets that come in from the WAN zone and the Zyxel Device routes back out through the WAN zone. Note: Depending on your network topology and traffic load, applying every packet direction to an anomaly profile may affect the Zyxel Device's performance.
Anomaly Profile	An anomaly profile is a set of anomaly policies with configured activation, log and action settings. This field shows which anomaly profile is bound to which traffic direction. Select an ADP profile to apply to the entry's traffic direction. Configure the ADP profiles in the ADP profile screens.

25.5.2 Creating New ADP Profiles

Create new ADP profiles in the **Configuration > Security Policy > ADP > Profile** screens.

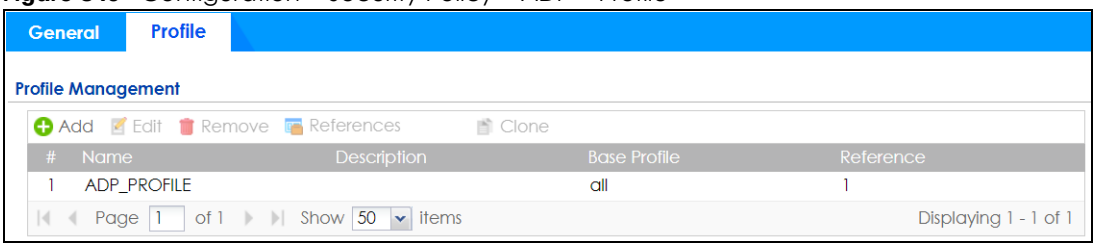
When creating ADP profiles. you may find that certain policies are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the Zyxel Device. As each network is different, false positives and false negatives are common on initial ADP deployment.

To counter this, you could create a 'monitor profile' that creates logs, but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'in-line profile' whereby you configure appropriate actions to be taken when a packet matches a policy.

ADP profiles consist of traffic anomaly profiles and protocol anomaly profiles. To create a new profile, select a base profile and then click **OK** to go to the profile details screen. Type a new profile name, enable or disable individual policies and then edit the default log options and actions.

Click **Configuration > Security Policy > ADP > Profile** to view the following screen.

Figure 349 Configuration > Security Policy > ADP > Profile



The following table describes the labels in this screen.

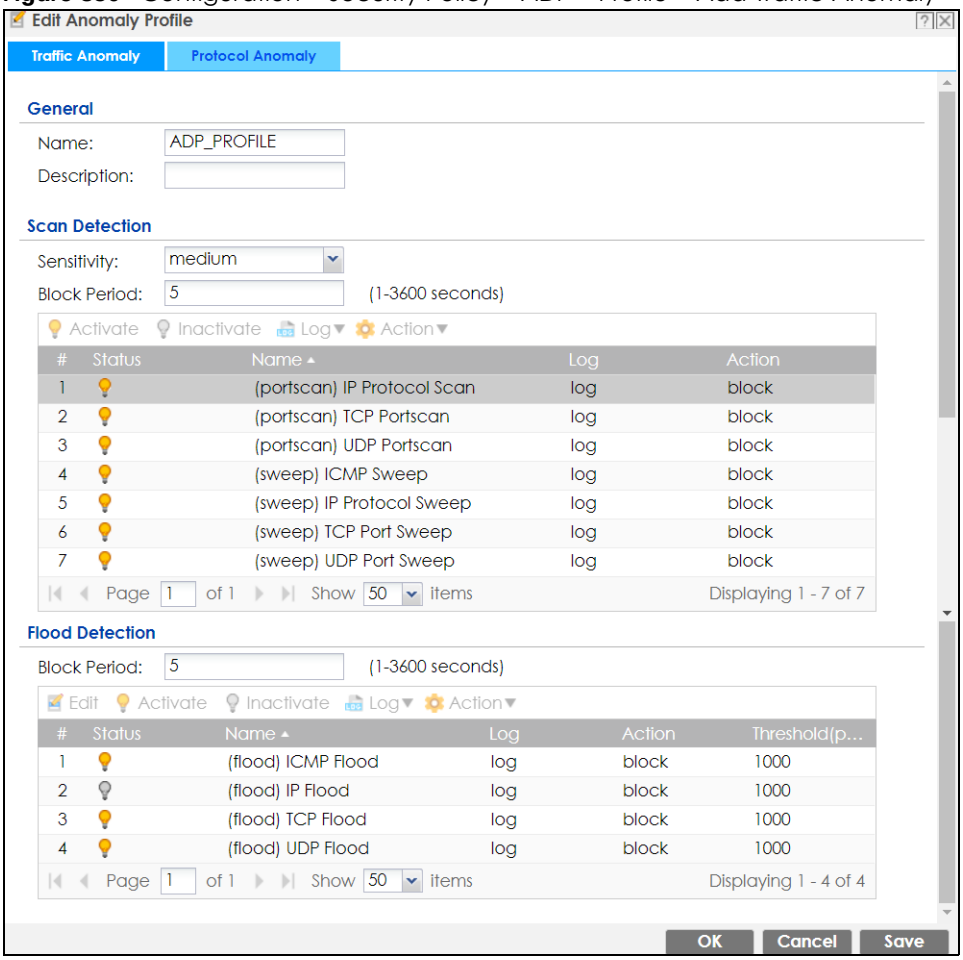
Table 196 Configuration > Security Policy > ADP > Profile

LABEL	DESCRIPTION
Profile Management	Create ADP profiles here and then apply them in the **Configuration > Security Policy > ADP > Profile** screen.
Add	Click **Add** and first choose a **none** or **all Base Profile**. • **none** base profile sets all ADP entries to have **Log** set to **no** and **Action** set to **none** by default. • **all** base profile sets all ADP entries to have **Log** set to **log** and **Action** set to **block** by default.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click **Refresh** to update information on this screen.
Clone	Use **Clone** to create a new entry by modifying an existing one. • Select an existing entry. • Click **Clone**. • A configuration copy of the selected entry pops up. You must at least change the name as duplicate entry names are not allowed.
#	This is the entry's index number in the list.
Name	This is the name of the profile you created.
Description	This is the description of the profile you created.
Base Profile	This is the name of the base profile used to create this profile.
Reference	This is the number of object references used to create this profile.

25.5.3 Traffic Anomaly Profiles

Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. In the **Configuration > Security Policy > ADP > Profile** screen, click the **Edit** or **Add** icon and choose a base profile. **Traffic Anomaly** is the first tab in the profile.

Figure 350 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly



The following table describes the labels in this screen.

Table 197 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly

LABELS	DESCRIPTION
Name	A name is automatically generated that you can edit. The name must be the same in the Traffic Anomaly and Protocol Anomaly screens for the same ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	In addition to the name, type additional information to help you identify this ADP profile.

Table 197 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly (continued)

LABELS	DESCRIPTION
Scan/Flood Detection	Scan detection, such as port scanning, tries to find attacks where an attacker scans device(s) to determine what types of network protocols or services a device supports. Flood detection tries to find attacks that saturate a network with useless data, use up all available bandwidth, and so aim to make communications in the network impossible.
Sensitivity	(Scan detection only.) Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected. If you choose high sensitivity, then scan thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives.
Block Period	Specify for how many seconds the Zyxel Device blocks all packets from being sent to the victim (destination) of a detected anomaly attack. Flood Detection applies blocking to the destination IP address and Scan Detection applies blocking to the source IP address.
Edit (Flood Detection only)	Select an entry and click this to be able to modify it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Log	To edit an item's log option, select it and use the **Log** icon. Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly policy.
Action	To edit what action the Zyxel Device takes when a packet matches a policy, select the policy and use the **Action** icon. **none**: The Zyxel Device takes no action when a packet matches the policy. **block**: The Zyxel Device silently drops packets that matches the policy. Neither sender nor receiver are notified.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the anomaly policy. Click the **Name** column heading to sort in ascending or descending order according to the protocol anomaly policy name.
Log	These are the log options. To edit this, select an item and use the **Log** icon.
Action	This is the action the Zyxel Device should take when a packet matches a policy. To edit this, select an item and use the **Action** icon.
Threshold (pkt/sec)	(Flood detection only.) Select a suitable threshold level (the number of packets per second that match the flood detection criteria) for your network. If you choose a low threshold, most traffic anomaly attacks will be detected, but you may have more logs and false positives. If you choose a high threshold, some traffic anomaly attacks may not be detected, but you will have fewer logs and false positives.
OK	Click **OK** to save your settings to the Zyxel Device, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the Zyxel Device but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

25.5.4 Protocol Anomaly Profiles

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder
- IP Decoder

Teardrop

When an IP packet is larger than the Maximum Transmission Unit (MTU) configured in the Zyxel Device, it is fragmented using the TCP or ICMP protocol.

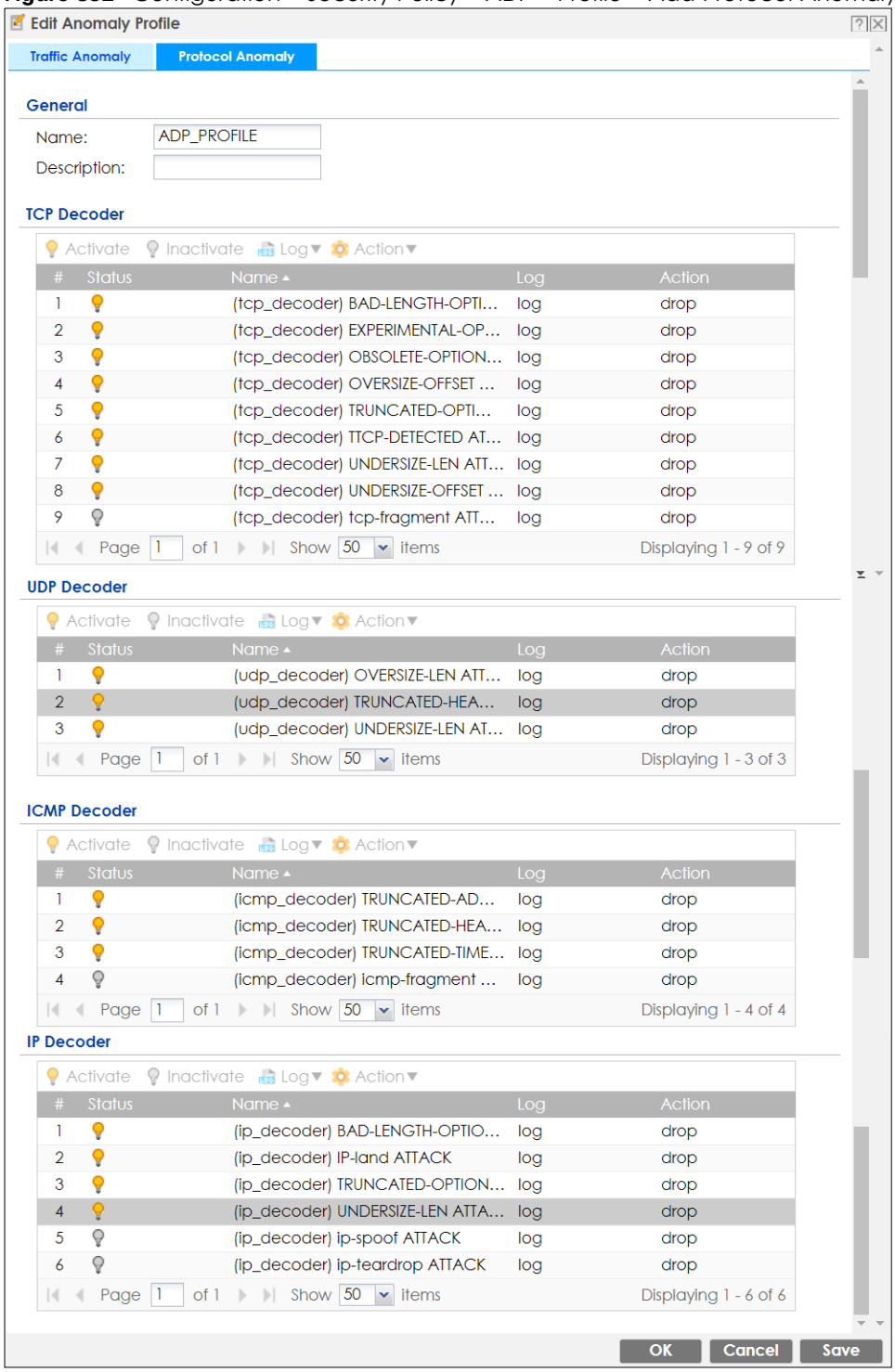
A Teardrop attack falsifies the offset which defines the size of the fragment and the original packet. A series of IP fragments with overlapping offset fields can cause some systems to crash, hang, or reboot when fragment reassembling is attempted at the destination.

IP Spoofing

IP Spoofing is used to gain unauthorized access to network devices by modifying packet headers so that it appears that the packets originate from a host within a trusted network.

- In an IP Spoof from the WAN, the source address appears to be in the same subnet as a Zyxel Device LAN interface.
- In an IP Spoof from a LAN interface, the source address appears to be in a different subnet from that Zyxel Device LAN interface.

Figure 351 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly



The following table describes the labels in this screen.

Table 198 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly

LABEL	DESCRIPTION
Name	A name is automatically generated that you can edit. The name must be the same in the Traffic Anomaly and Protocol Anomaly screens for the same ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 • These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	In addition to the name, type additional information to help you identify this ADP profile.
TCP Decoder/UDP Decoder/ICMP Decoder/IP Decoder	Perform the following actions for each type of encoder.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Log	To edit an item's log option, select it and use the **Log** icon. Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly policy.
Action	To edit what action the Zyxel Device takes when a packet matches a policy, select the policy and use the **Action** icon. **original setting**: Select this action to return each rule in a service group to its previously saved configuration. **none**: Select this action to have the Zyxel Device take no action when a packet matches a policy. **drop**: Select this action to have the Zyxel Device silently drop a packet that matches a policy. Neither sender nor receiver are notified. **reject-sender**: Select this action to have the Zyxel Device send a reset to the sender when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the Zyxel Device will send an ICMP unreachable packet. **reject-receiver**: Select this action to have the Zyxel Device send a reset to the receiver when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with an a 'RST' flag. If it is an ICMP or UDP attack packet, the Zyxel Device will do nothing. **reject-both**: Select this action to have the Zyxel Device send a reset to both the sender and receiver when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the Zyxel Device will send an ICMP unreachable packet.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the anomaly policy. Click the **Name** column heading to sort in ascending or descending order according to the protocol anomaly policy name.

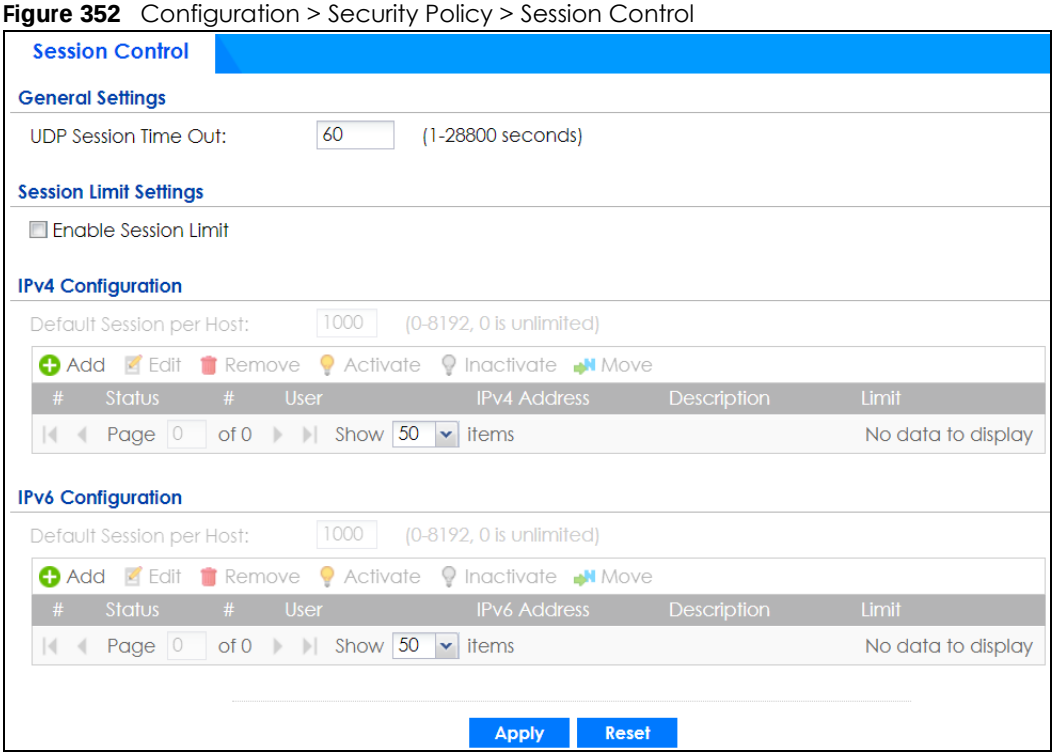
Table 198 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly

LABEL	DESCRIPTION
Log	These are the log options. To edit this, select an item and use the **Log** icon.
Action	This is the action the Zyxel Device should take when a packet matches a policy. To edit this, select an item and use the **Action** icon.
OK	Click **OK** to save your settings to the Zyxel Device, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the Zyxel Device but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

25.6 The Session Control Screen

Click **Configuration > Security Policy > Session Control** to display the **Security Policy Session Control** screen. Use this screen to limit the number of concurrent NAT/Security Policy sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 352 Configuration > Security Policy > Session Control



The following table describes the labels in this screen.

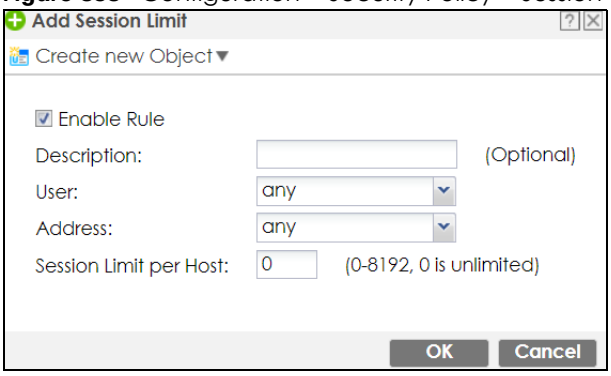
Table 199 Configuration > Security Policy > Session Control

LABEL	DESCRIPTION
General Settings	
UDP Session Time Out	Set how many seconds the Zyxel Device will allow a UDP session to remain idle (without UDP traffic) before closing it.
Session Limit Settings	
Enable Session limit	Select this check box to control the number of concurrent sessions hosts can have.
IPv4 / IPv6 Configuration	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Default Session per Host	This field is configurable only when you enable session limit. Use this field to set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. Create rules below to apply other limits for specific users or addresses.
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 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.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.
User	This is the user name or user group name to which this session limit rule applies.
IPv4 / IPv6 Address	This is the IPv4 / IPv6 address object, including geographic address (group) objects to which this session limit rule applies.
Description	This is the information configured to help you identify the rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

25.6.1 The Session Control Add/Edit Screen

Click **Configuration > Security Policy > Session Control** and the **Add** or **Edit** icon to display the **Add or Edit** screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 353 Configuration > Security Policy > Session Control > Edit



The following table describes the labels in this screen.

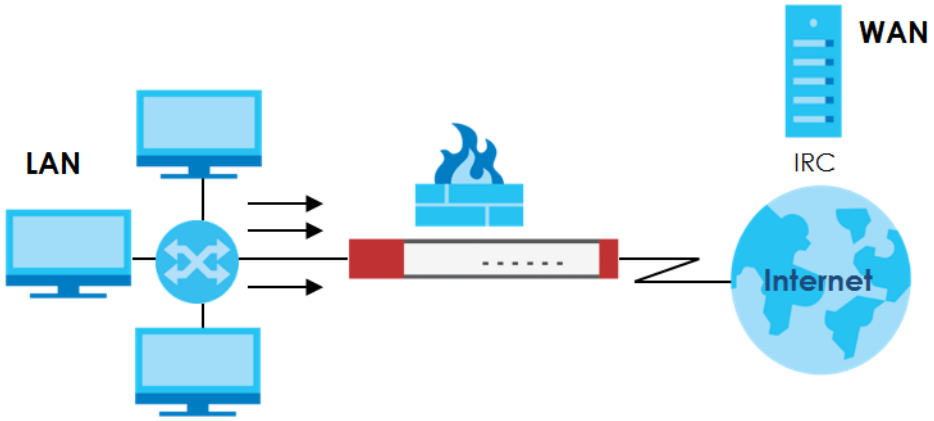
Table 200 Configuration > Security Policy > Session Control > Add / Edit

LABEL	DESCRIPTION
Create new Object	Use to configure new settings for User or Address objects that you need to use in this screen.Click on the down arrow to see the menu.
Enable Rule	Select this check box to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified an IP address (or address group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Address	Select the IPv4 source address or address group, including geographic address (group) object, to which this rule applies. Select **any** to apply the rule to all IPv4 source addresses.
IPv6 Address	Select the IPv6 source address or address group, including geographic address (group) object, to which this rule applies. Select **any** to apply the rule to all IPv6 source addresses.
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/Security Policy sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **Security Policy Session Control** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

25.7 Security Policy Example Applications

Suppose you decide to block LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN Security Policy that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the Security Policy to always be in effect. The following figure shows the results of this policy.

Figure 354 Blocking All LAN to WAN IRC Traffic Example



Your Security Policy would have the following settings.

Table 201 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the Security Policy's default policy that allows all LAN1 to WAN traffic.

The Zyxel Device applies the security policies in order. So for this example, when the Zyxel Device receives traffic from the LAN, it checks it against the first policy. If the traffic matches (if it is IRC traffic) the security policy takes the action in the policy (drop) and stops checking the subsequent security policies. Any traffic that does not match the first security policy will match the second security policy and the Zyxel Device forwards it.

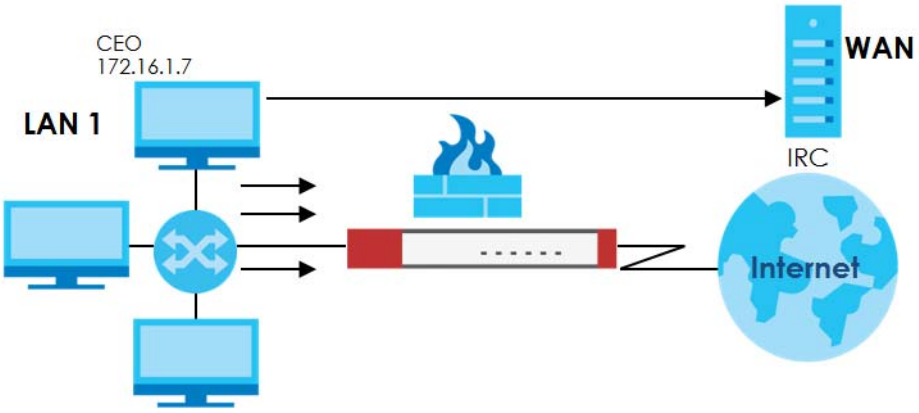
Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN policy that allows IRC traffic from any computer through which the CEO logs into the Zyxel Device with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- Has a static IP address,

  or
- You configure a static DHCP entry for it so the Zyxel Device always assigns it the same IP address.

Now you configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer (172.16.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the security policy to always be in effect. The following figure shows the results of your two custom policies.

Figure 355 Limited LAN to WAN IRC Traffic Example



Your security policy would have the following configuration.

Table 202 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	172.16.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 172.16.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN policy with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your Security Policy would have the following settings.

Table 203 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the Zyxel Device with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing allows all traffic from the LAN1 to go to the WAN.

The policy for the CEO must come before the policy that blocks all LAN1 to WAN IRC traffic. If the policy that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that policy and the Zyxel Device would drop it and not check any other security policies.

CHAPTER 26
Application Patrol

26.1 Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

26.1.1 What You Can Do in this Chapter

- Use the **App Patrol** summary screen (see Section 26.2 on page 516) to manage the application patrol profiles. You can also view license registration and signature information.
- Use the **App Patrol Add/Edit** screens (see Section 26.2.2 on page 520 & Section 26.2.3 on page 521) to set actions for application categories and for specific applications within the category.

26.1.2 What You Need to Know

If you want to use a service, make sure both the Security Policy and application patrol allow the service's packets to go through the Zyxel Device.

Note: The Zyxel Device checks secure policies before it checks application patrol rules for traffic going through the Zyxel Device.

Application patrol examines every TCP and UDP connection passing through the Zyxel Device and identifies what application is using the connection. Then, you can specify whether or not the Zyxel Device continues to route the connection. Traffic not recognized by the application patrol signatures is ignored.

Application Profiles & Policies

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the Zyxel Device takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Use policies to link profiles to traffic flows based on criteria such as source zone, destination zone, source address, destination address, schedule, user.

Classification of Applications

There are two ways the Zyxel Device can identify the application. The first is called auto. The Zyxel Device looks at the IP payload (OSI level-7 inspection) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the Zyxel Device examines several packets to make sure the match

is correct. Before confirmation, packets are forwarded by App Patrol with no action taken. The number of packets inspected before confirmation varies by signature.

Note: The Zyxel Device allows the first eight packets to go through the security policy, regardless of the application patrol policy for the application. The Zyxel Device examines these first eight packets to identify the application.

The second approach is called service ports. The Zyxel Device uses only OSI level-4 information, such as ports, to identify what application is using the connection. This approach is available in case the Zyxel Device identifies a lot of "false positives" for a particular application.

Custom Ports for SIP and the SIP ALG

Configuring application patrol to use custom port numbers for SIP traffic also configures the SIP ALG to use the same port numbers for SIP traffic. Likewise, configuring the SIP ALG to use custom port numbers for SIP traffic also configures application patrol to use the same port numbers for SIP traffic.

26.2 Application Patrol Profile

Use the application patrol screens to customize action and log settings for a group of application patrol signatures. You then link a profile to a policy. Use this screen to create an application patrol profile, and view signature information. It also lists the registration status and details about the signature set the Zyxel Device is using.

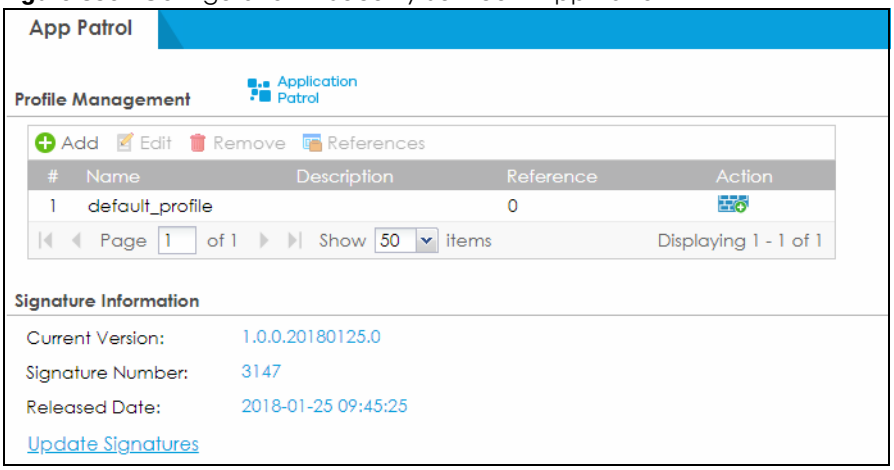
Note: You must register for the AppPatrol signature service (at least the trial) before you can use it.

A profile is an application object(s) or application group(s) that has customized action and log settings.

Click **Configuration > Security Service > App Patrol** to open the following screen.

Click the **Application Patrol** icon for more information on the Zyxel Device's security features.

Figure 356 Configuration > Security Service > App Patrol



The following table describes the labels in this screen.

Table 204 Configuration > Security Service > App Patrol

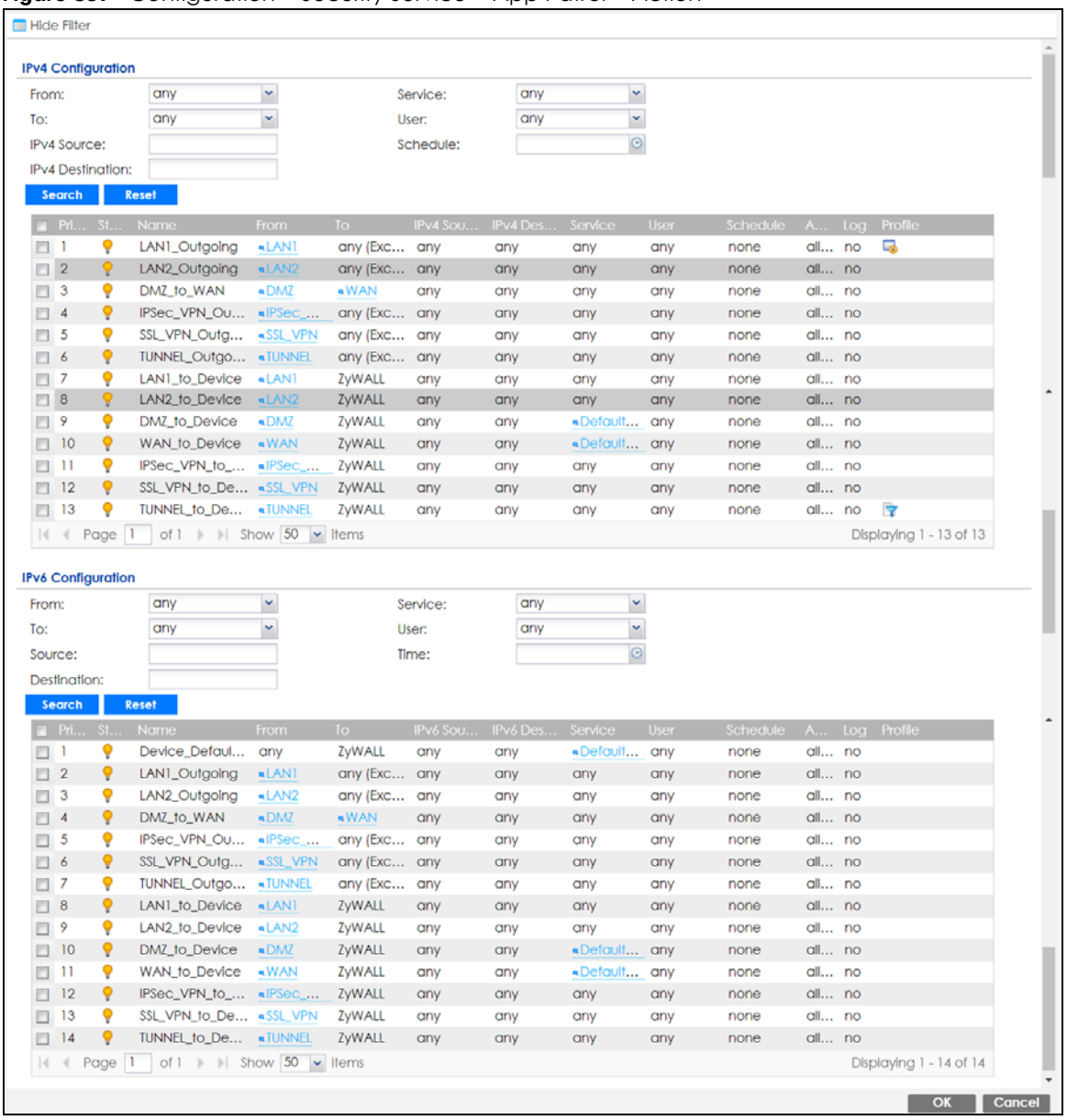
LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	Select an entry and click **Remove** to delete the selected entry.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Name	This displays the name of the profile created.
Description	This displays the description of the App Patrol Profile.
Scan Option	This field displays the scan options from the App Patrol profile.
Reference	This displays the number of times an object reference is used in a profile.
Action	Click this icon to apply the entry to a security policy. Go to the **Configuration > Security Policy > Policy Control** screen to check the result.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the App Patrol signature set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.

26.2.1 Apply to a Security Policy

Click the icon in the **Action** field of an existing application patrol file to apply the profile to a security policy.

Go to the **Configuration > Security Policy > Policy Control** screen to check the result.

Figure 357 Configuration > Security Service > App Patrol > Action



The following table describes the labels in this screen.

Table 205 Configuration > Security Service > App Patrol > Action

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click **Show Filter** to display IPv4 and IPv6 (if enabled) security policy search filters.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. **any** means all zones.

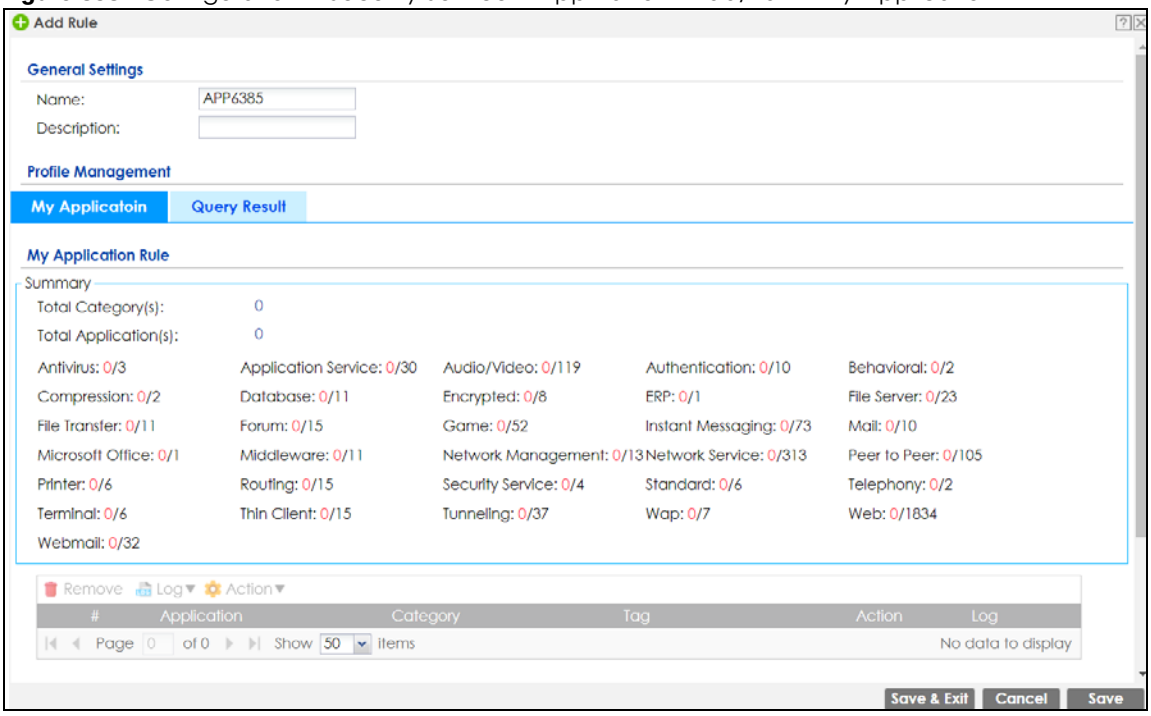
Table 205 Configuration > Security Service > App Patrol > Action

LABEL	DESCRIPTION
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. **Default** displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from **LAN** to **LAN** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From **any** displays all the Security Policies for traffic going to the selected **To Zone**. To **any** displays all the Security Policies for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the Security Policies. To **ZyWALL** policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. **none** means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (**deny**), permits the passage of packets (**allow**) or drops packets with notification (**reject**)
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or not (**no**) when the policy is matched to the criteria listed above.
Profile	This field shows you which Security Service profiles (application patrol, content filter, IDP, anti-malware, email security) apply to this Security policy. Click an applied Security Service profile icon to edit the profile directly.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

26.2.2 The Application Patrol Profile Add/Edit Screen - My Application

Use this screen to configure profile settings. Click **Configuration > Security Service > App Patrol > Add/Edit**, then click **My Application** to open the following screen.

Figure 358 Configuration > Security Service > App Patrol > Add/Edit > My Application



The following table describes the labels in this screen.

Table 206 Configuration > Security Service > App Patrol > Add/Edit > My Application

LABEL	DESCRIPTION
General Settings	
Name	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Type a description for the profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Total Category(s)	This field displays the total number of the selected category(ies) in the **Query Result** screen.
Total Application(s)	This field displays the total number of the selected applications in the **Query Result** screen.
Remove	Select an entry and click **Remove** to delete the selected entry.

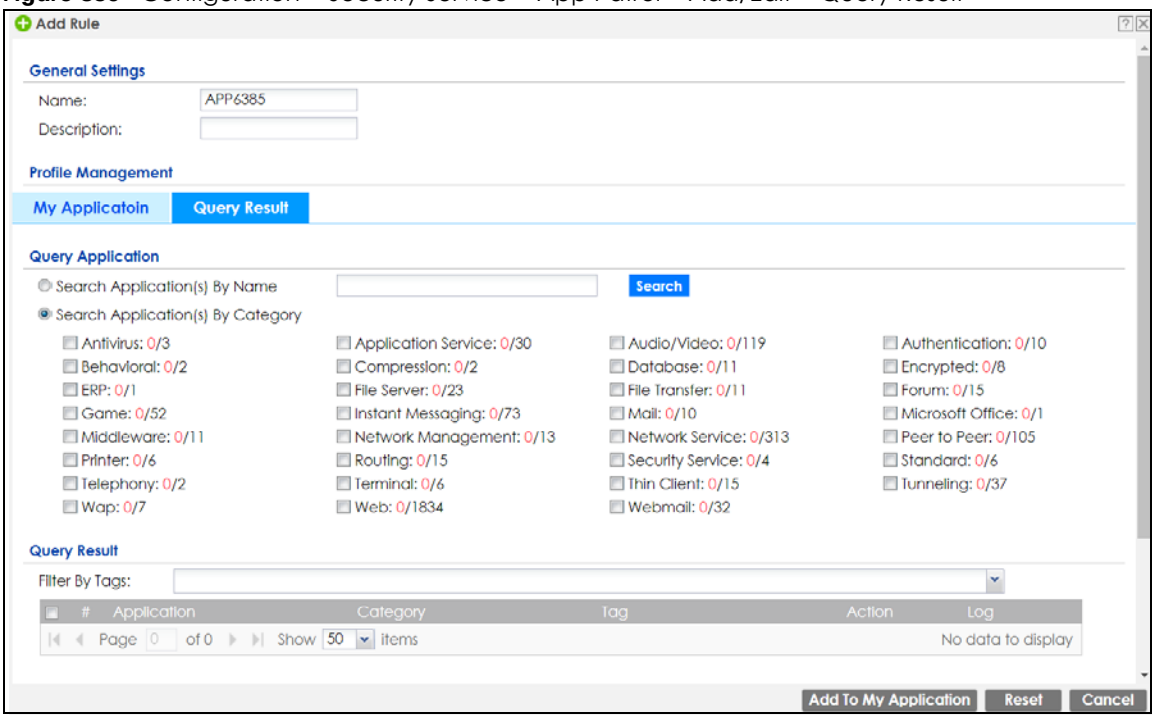
Table 206 Configuration > Security Service > App Patrol > Add/Edit (continued)> My Application

LABEL	DESCRIPTION
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in this category.
Action	Select the default action for all signatures in this category. **forward** - the Zyxel Device routes packets that matches these signatures. **drop** - the Zyxel Device silently drops packets that matches these signatures without notification. **reject** - the Zyxel Device drops packets that matches these signatures and sends notification.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Application	This field displays the application name of the policy.
Category	This field displays the category type of the application.
Tag	This field displays the tag information of the application.
Action	Select the default action for all signatures in this category. **forward** - the Zyxel Device routes packets that matches these signatures. **drop** - the Zyxel Device silently drops packets that matches these signatures without notification. **reject** - the Zyxel Device drops packets that matches these signatures and sends notification.
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in this category.
Save & Exit	A profile consists of separate category editing screens. If you want to configure just one category for a profile, click **OK** to save your settings to the Zyxel Device, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	If you want to configure more than one category for a profile, click **Save** to save your settings to the Zyxel Device without leaving this page.

26.2.3 The Application Patrol Profile Add/Edit Screen - Query Result

Click **Configuration > Security Service > App Patrol > Add**, then click **Query Result** to search for certain applications within a specific category, and the selected applications will be added to **My Application** screen. You can also click an existing profile, click **Edit** (or double-click it), then click **Query Result** to open the following screen.

Figure 359 Configuration > Security Service > App Patrol > Add/Edit > Query Result



The following table describes the labels in this screen.

Table 207 Configuration > Security Service > App Patrol > Add/Edit > Query Result

LABEL	DESCRIPTION
General Settings	
Name	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Type a description for the profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Search Application(s) By Name	Enter a name to search for relevant applications.
Search Application(s) By Category	Select a category(ies) below to search for relevant applications.
Filter by Tags	Add or delete a tag(s) to display or not display an application(s).
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Application	This field displays the application name of the policy.
Category	This field displays the category type of the application.

Table 207 Configuration > Security Service > App Patrol > Add/Edit (continued)> Query Result

LABEL	DESCRIPTION
Tag	This field displays the tag information of the policy.
Action	Select the default action for all signatures in this category. **forward** - the Zyxel Device routes packets that matches these signatures. **drop** - the Zyxel Device silently drops packets that matches these signatures without notification. **reject** - the Zyxel Device drops packets that matches these signatures and sends notification.
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in this category.
Add to My Application	Select an application(s) to show in the **My Application** profile screen.
Reset	Click this button to reset the fields to default settings.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

CHAPTER 27
Content Filter

27.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

27.1.1 What You Can Do in this Chapter

- Use the **Filter Profile** screens (Section 27.2 on page 526) to set up content filtering profiles.
- Use the **Trusted Web Sites** screens (Section 27.3 on page 539) to create a common list of good (allowed) web site addresses.
- Use the **Forbidden Web Sites** screens (Section 27.4 on page 540) to create a common list of bad (blocked) web site addresses.

27.1.2 What You Need to Know

Content Filtering

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

  The Zyxel Device can block access to particular categories of web site content, such as pornography or racial intolerance.

- Restrict Web Features

  The Zyxel Device can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

- Customize Web Site Access

  You can specify URLs to which the Zyxel Device blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the Zyxel Device block access to URLs that contain particular keywords.

Content Filtering Configuration Guidelines

When the Zyxel Device receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The Zyxel Device allows the request if the default policy is not set to block. The Zyxel Device blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your Zyxel Device accesses an external database that has millions of web sites categorized based on content. You can have the Zyxel Device block, block and/or log access to web sites based on these categories.

HTTPS Domain Filter

HTTPS Domain Filter works with the Content Filter category feature to identify HTTPS traffic and take appropriate action. SSL Inspection identifies HTTPS traffic for all Security Service traffic and has higher priority than HTTPS Domain Filter. HTTPS Domain Filter only identifies keywords in the domain name of an URL and matches it to a category. For example, if the keyword is 'picture' and the URL is http://www.google.com/picture/index.htm, then HTTPS Domain Filter cannot identify 'picture' because that keyword in not in the domain name 'www.google.com'. However, SSL Inspection can identify 'picture' in the URL http://www.google.com/picture/index.htm.

Keyword Blocking URL Checking

The Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the Zyxel Device checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the Zyxel Device would find “tw” in the domain name (www.zyxel.com.tw). It would also find “news” in the file path (news/pressroom.php) but it would not find “tw/news”.

Finding Out More

- See Section 27.5 on page 541 for content filtering background/technical information.

27.1.3 Before You Begin

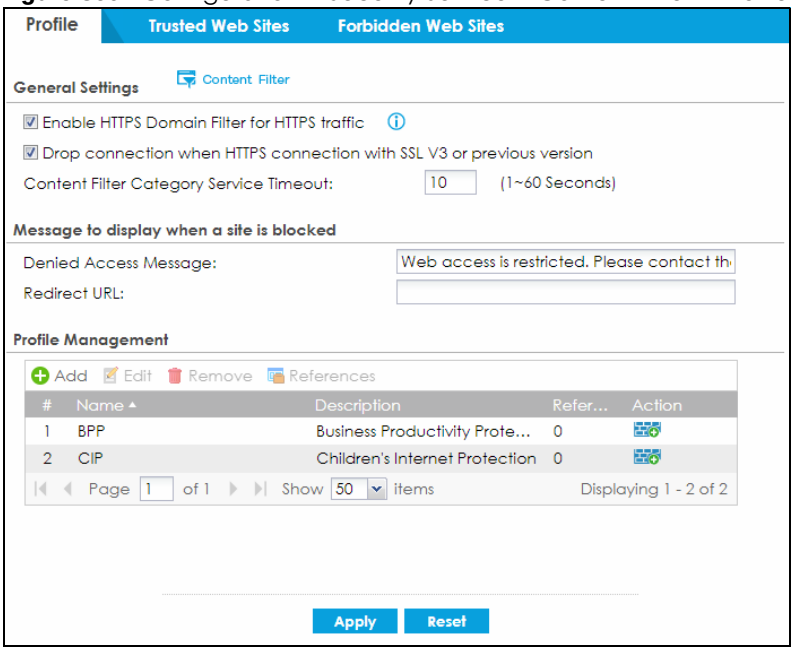
- You must configure an address object, a schedule object and a filtering profile before you can set up a content security policy.
- You must have Content Filtering license in order to use the function.subscribe to use the external database content filtering (see the **Licensing** > **Registration** screens).

27.2 Content Filter Profile Screen

Click **Configuration > Security Service> Content Filter > Profile** to open the **Content Filter Profile** screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Click the **Content Filter** icon for more information on the Zyxel Device's security features.

Figure 360 Configuration > Security Service > Content Filter > Profile



The following table describes the labels in this screen.

Table 208 Configuration > Security Service > Content Filter > Profile

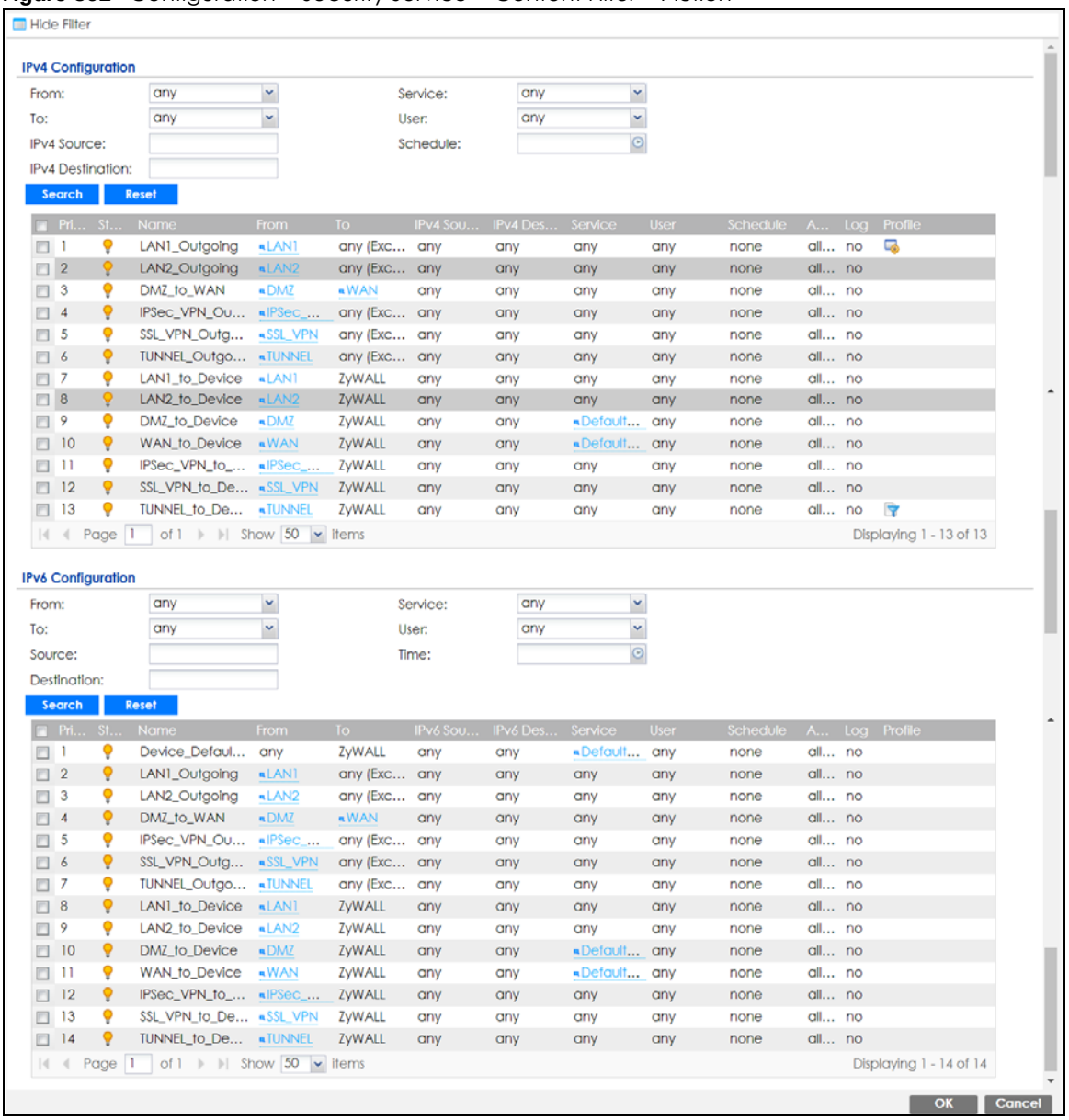
LABEL	DESCRIPTION
General Settings	
Enable HTTPS Domain Filter for HTTPS traffic	Select this check box to have the Zyxel Device block HTTPS web pages using the cloud category service. In an HTTPS connection, the Zyxel Device can extract the Server Name Indication (SNI) from a client request, check if it matches a category in the cloud content filter and then take appropriate action. The keyword match is for the domain name only.
Drop connection when HTTPS connection with SSL V3 or previous version	Select this check box to have the Zyxel Device block HTTPS web pages using SSL V3 or a previous version.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the content filter blocks access to a web page, the Zyxel Device just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Profile Management	
Add	Click Add to create a new content filter rule.
Edit	Click Edit to make changes to a content filter rule.
Remove	Click Remove the delete a content filter rule.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile rule.
Description	This column lists the description of the content filter profile rule.
Reference	This displays the number of times an Object Reference is used in a rule.
Action	Click this icon to apply the content filter profile with a security policy. Go to the **Configuration > Security Policy > Policy Control** screen to check the result.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

27.2.1 Apply to a Security Policy

Click the icon in the **Action** field to apply the entry to a security policy.

Go to the **Configuration > Security Policy > Policy Control** screen to check the result.

Figure 361 Configuration > Security Service > Content Filter > Action



The following table describes the labels in this screen.

Table 209 Configuration > Security Service > Content Filter > Action

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click **Show Filter** to display IPv4 and IPv6 (if enabled) security policy search filters.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. **any** means all zones.

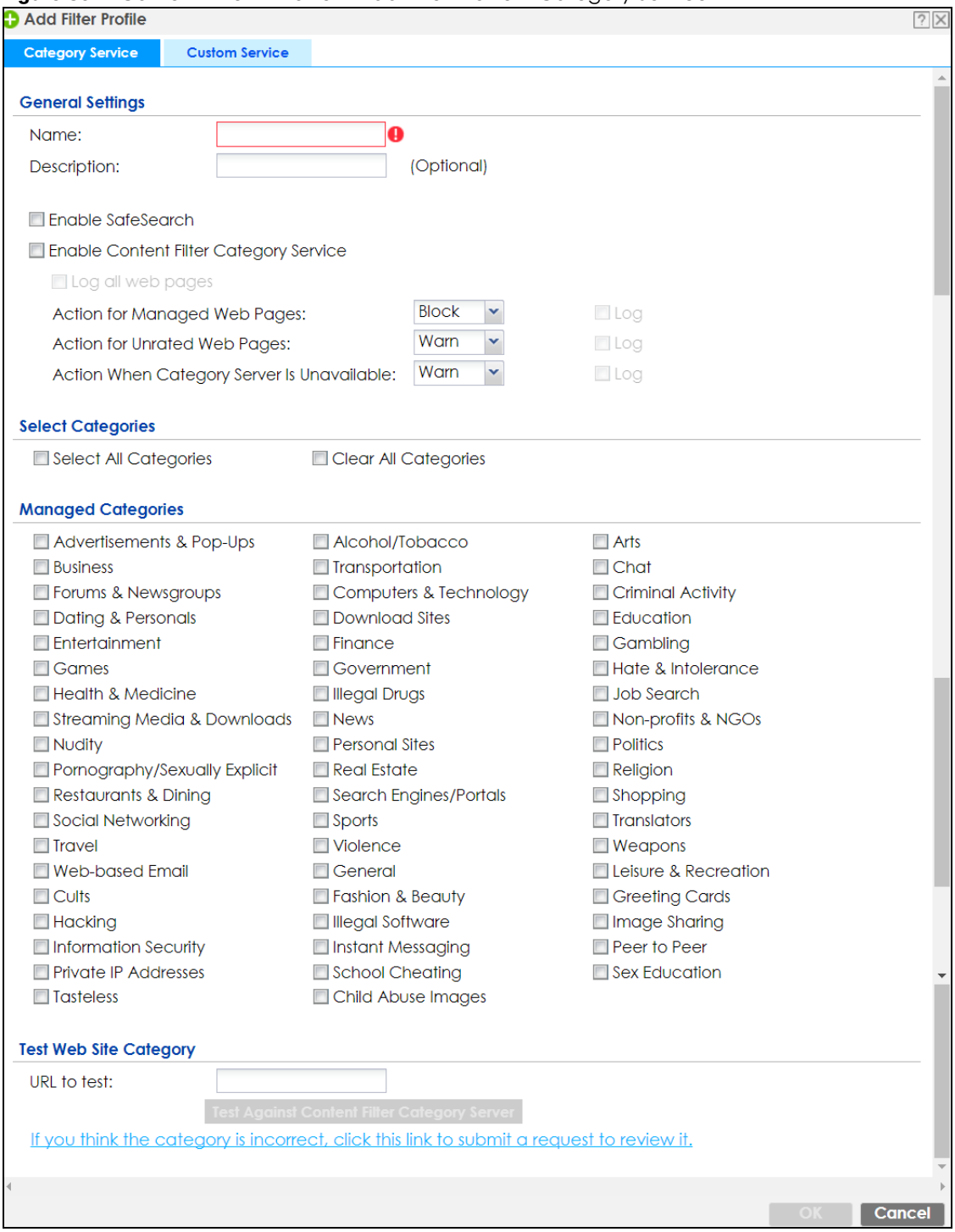
Table 209 Configuration > Security Service > Content Filter > Action

LABEL	DESCRIPTION
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. **Default** displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from **LAN** to **LAN** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From **any** displays all the Security Policies for traffic going to the selected **To Zone**. To **any** displays all the Security Policies for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the Security Policies. To **ZyWALL** policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. **none** means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (**deny**), permits the passage of packets (**allow**) or drops packets with notification (**reject**)
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or not (**no**) when the policy is matched to the criteria listed above.
Profile	This field shows you which Security Service profiles (application patrol, content filter, IDP, anti-malware, email security) apply to this Security policy. Click an applied Security Service profile icon to edit the profile directly.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

27.2.2 Content Filter Add Profile Category Service

Click **Configuration > Security Service > Content Filter > Profile > Add or Edit** to open the **Add Filter Profile** screen.

Figure 362 Content Filter > Profile > Add Filter Profile > Category Service



The following table describes the labels in this screen.

Table 210 Configuration > Security Service > Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable SafeSearch	SafeSearch is a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the Zyxel Device. It does this by adding a parameter in the search URL: *https://www.google.com.tw/?gws_rd=ssl#q=porn&safe=active*. Supported search engines at the time of writing are: Yahoo, Google, MSN Live Bing, Yandex
Enable Content Filter Category Service	Enable external database content filtering to have the Zyxel Device check an external database to find to which category a requested web page belongs. The Zyxel Device then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Log all web pages	Select this to record attempts to access web pages when: • They match the other categories that you select below. • They are not categorized. • The external content filtering database is unavailable.
Action for Managed Web Pages	Select **Pass** to allow users to access web pages that match the other categories that you select below. Select **Block** to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page. Select **Log** to record attempts to access web pages that match the other categories that you select below.
Action for Unrated Web Pages	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page. Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized. Select **Log** to record attempts to access web pages that are not categorized.

Table 210 Configuration > Security Service > Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Action When Category Server Is Unavailable	Select **Pass** to allow users to access any requested web page if the external content filtering database is unavailable. Select **Block** to block access to any requested web page if the external content filtering database is unavailable. Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable. The following are possible causes for the external content filtering server not being available: • There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field. • The Zyxel Device is not able to resolve the domain name of the external content filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable.
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories. See the next table for category details.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filtering can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. **URL to test** displays both results in the test.
If you think the category is incorrect	Click this link to see the category recorded in the Zyxel Device's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

The following table describes the managed categories.

Table 211 Managed Category Descriptions

CATEGORY	DESCRIPTION
Advertisements & Pop-Ups	Sites that provide advertising graphics or other ad content files such as banners and pop-ups. For example, pagead2.googlesyndication.com, ad.yieldmanager.com.

Table 211 Managed Category Descriptions (continued)

Alcohol & Tobacco	Sites that promote or sell alcohol- or tobacco-related products or services. For example, www.drinks.com.tw, www.p9.com.tw, beer.ttl.com.tw.
Arts	Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources. For example, www.npm.gov.tw, www.nmh.gov.tw.
Business	Sites that provide business related information such as corporate Web sites. Information, services, or products that help businesses of all sizes to do their day-to-day commercial activities. For example, www.kinkos.com, www.proctorgamble.com, www.bbb.org.
Transportation	Sites that provide information about motor vehicles such as cars, motorcycles, boats, trucks, RVs and the like. Includes manufacturer sites, dealerships, review sites, pricing,, online purchase sites, enthusiasts clubs, etc. For example, www.toyota.com.tw, www.ford.com.tw, www.sym.com.tw.
Chat	Sites that enable web-based exchange of real time messages through chat services or chat rooms. For example, me.sohu.com, blufiles.storage.live.com.
Forums & Newsgroups	Sites for sharing information in the form of newsgroups, forums, bulletin boards. For example, ck101.com, my.xuite.net, ptt.cc.
Computers & Technology	Sites that contain information about computers, software, hardware, IT, peripheral and computer services, such as product reviews, discussions, and IT news. For example, www.informationsecurity.com.tw, blog.ithome.com.tw.
Criminal Activity	Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Also includes sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software. For example, www.hackbase.com, jia.hackbase.com, ad.adver.com.tw.
Dating & Personals	Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction. For example, www.i-part.com.tw, www.imatchi.com.
Download Sites	Sites that contain downloadable software, whether shareware, freeware, or for a charge. Includes peer-to-peer sites. For example, www.hotdl.com, toget.pchome.com.tw, www.azroo.com.
Education	Sites sponsored by educational institutions and schools of all types including distance education. Includes general educational and reference materials such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides. For example, www.tfam.museum, www.lksf.org, www.1980.org.tw.
Entertainment	Sites related to television, movies, music and video (including video on demand), such as program guides, celebrity sites, and entertainment news. For example, www.ctitv.com.tw, www.hboasia.com, www.startv.com.tw.
Finance	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on. For example, www.concords.com.tw, www.polaris.com.tw, www.bochk.com.
Gambling	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. For example, www.taiwanlottery.com.tw, www.i-win.com.tw, www.hkjc.com.
Games	Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites. For example, www.gamer.com.tw, www.wowtaiwan.com.tw, tw.lineage.gamania.com.
Government	Sites run by governmental organizations, departments, or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counter-terrorism organizations, military and hospitals. For example, www.ey.gov.tw, www.whitehouse.gov, www.npa.gov.tw.

Table 211 Managed Category Descriptions (continued)

Hate & Intolerance	Sites that promote a supremacist political agenda, encouraging oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. For example, www.racist-jokes.com, aryan-nations.org, whitepower.com.
Health & Medicine	Sites containing information pertaining to health, healthcare services, fitness and well-being, including information about medical equipment, hospitals, drugstores, nursing, medicine, procedures, prescription medications, etc. For example, www.lksf.org, www.ohayo.com.tw.
Illegal Drugs	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds For example, www.cannabis.net, www.amphetamines.com.
Job Search	Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters. For example, www.104.com.tw, www.1111.com.tw, www.yes123.com.tw.
Streaming Media & Downloads	Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels. For example, www.youtube.com, pfp.sina.com.cn, my.xunlei.com.
News	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines. For example, www.tvbs.com.tw?Awww.ebc.net.tw?Awww.iset.com.tw.
Non-profits & NGOs	Sites devoted to clubs, communities, unions, and non-profit organizations. Many of these groups exist for educational or charitable purposes. For example, www.tzuchi.org.tw, web.redcross.org.tw, www.lksf.org.
Nudity	Sites that contain full or partial nudity that are not necessarily overtly sexual in intent. Includes sites that advertise or sell lingerie, intimate apparel, or swim wear. For example, www.easyshop.com.tw, www.faster-swim.com.tw, image.baidu.com.
Personal Sites	Sites about or hosted by personal individuals, including those hosted on commercial sites. For example, blog.yam.com, www.wretch.cc, blog.xuite.net.
Politics	Sites that promote political parties or political advocacy, or provide information about political parties, interest groups, elections, legislation or lobbying. Also includes sites that offer legal information and advice. For example, www.kmt.org.tw, www.dpp.org.tw, cpc.people.com.cn.
Pornography/Sexually Explicit	Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts. For example, www.dvd888.com, www.18center.com, blog.sina.com.tw.
Real Estate	Sites relating to commercial or residential real estate services, including renting, purchasing, selling or financing homes, offices, etc. For example, www.sinyi.com.tw, www.yungching.com.tw, house.focus.cn.
Religion	Sites that deal with faith, human spirituality or religious beliefs, including sites of churches, synagogues, mosques and other houses of worship. For example, www.fgs.org.tw, www.twtaoism.net, www.fhl.net.
Restaurants & Dining	Sites that list, review, promote or advertise food, dining or catering services. Includes sites for recipes, cooking instruction and tips, food products, and wine advisors. For example, www.jogoya.com.tw, www.dintaifung.com.tw, www2.pizzahut.com.tw.
Search Engines & Portals	Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. Includes portal and directory sites such as white/yellow pages. For example, tw.yahoo.com, www.pchome.com.tw, www.google.com.tw.
Shopping	Sites for online shopping, catalogs, online ordering, auctions, classified ads. Excludes shopping for products and services exclusively covered by another category such as health & medicine. For example, shopping.pchome.com.tw, buy.yahoo.com.tw, www.tkec.com.tw.

Table 211 Managed Category Descriptions (continued)

Social Networking	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. For example, www.facebook.com, www.flickr.com, www.groups.google.com.
Sports	Sites relating to sports teams, fan clubs, scores and sports news. Relates to all sports, whether professional or recreational. For example, www.yankees.com, www.nba.com, mlb.mlb.com.
Translators	Sites that translate Web pages or phrases from one language to another. These sites may be used to attempt to bypass a filtering system. For example, translate.google.com.tw, www.smartlinkcorp.com, translation.paralink.com.
Travel	Sites that provide travel and tourism information or online booking of travel services such as airlines, accommodations, car rentals. Includes regional or city information sites. For example, www.startravel.com.tw, taipei.grand.hyatt.com.tw, www.car-plus.com.tw.
Violence	Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment. For example, crimescene.com, deathnet.com, michiganmilitia.com.
Weapons	Sites that depict, sell, review or describe guns and weapons, including for sport. For example, www.ak-47.net, warfare.ru.
Web-based Email	Sites that enable users to send and receive email through a web-accessible email account. For example, mail.163.com, mail.google.com, mail.yahoo.com.tw.
General	Sites that do not clearly fall into other categories, for example, blank Web pages. For example, bs.serving-sys.com, simg.sinajs.cn, i0.itc.cn.
Leisure & Recreation	Sites relating to recreational activities and hobbies including zoos, public recreation centers, pools, amusement parks, and hobbies such as gardening, literature, arts & crafts, home improvement, home d?cor, family, etc. For example, tpbg.tfri.gov.tw, tw.fashion.yahoo.com, www.relaxtimes.com.tw.
Cults	Sites relating to non-traditional religious practice typically known as "cults," that is, considered to be false, unorthodox, extremist, or coercive, with members often living under the direction of a charismatic leader. For example, www.churchofsatan.com, www.ccya.org.tw.
Fashion & Beauty	Sites concerning fashion, jewelry, glamour, beauty, modeling, cosmetics or related products or services. Includes product reviews, comparisons, and general consumer information. For example, women.sohu.com, baodian.women.sohu.com.
Greeting cards	Sites that allow people to send and receive greeting cards and postcards. For example, www.e-card.com.tw, card.ivy.net.tw.
Hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information. For example, www.hackbase.com, www.chinahacker.com.
Illegal Software	Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators. For example, www.zhaokey.com.cn, www.tiansha.net.
Image Sharing	Sites that host digital photographs and images, online photo albums and digital photo exchanges. For example, photo.pchome.com.tw, photo.xuite.net, photobucket.com.
Information Security	Sites that provide legitimate information about data protection, including newly discovered vulnerabilities and how to block them. For example, www.informationsecurity.com.tw, www.itis.tw.
Instant Messaging	Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like. For example, www.meebo.com, www.aim.com, www. ebuddy.com.

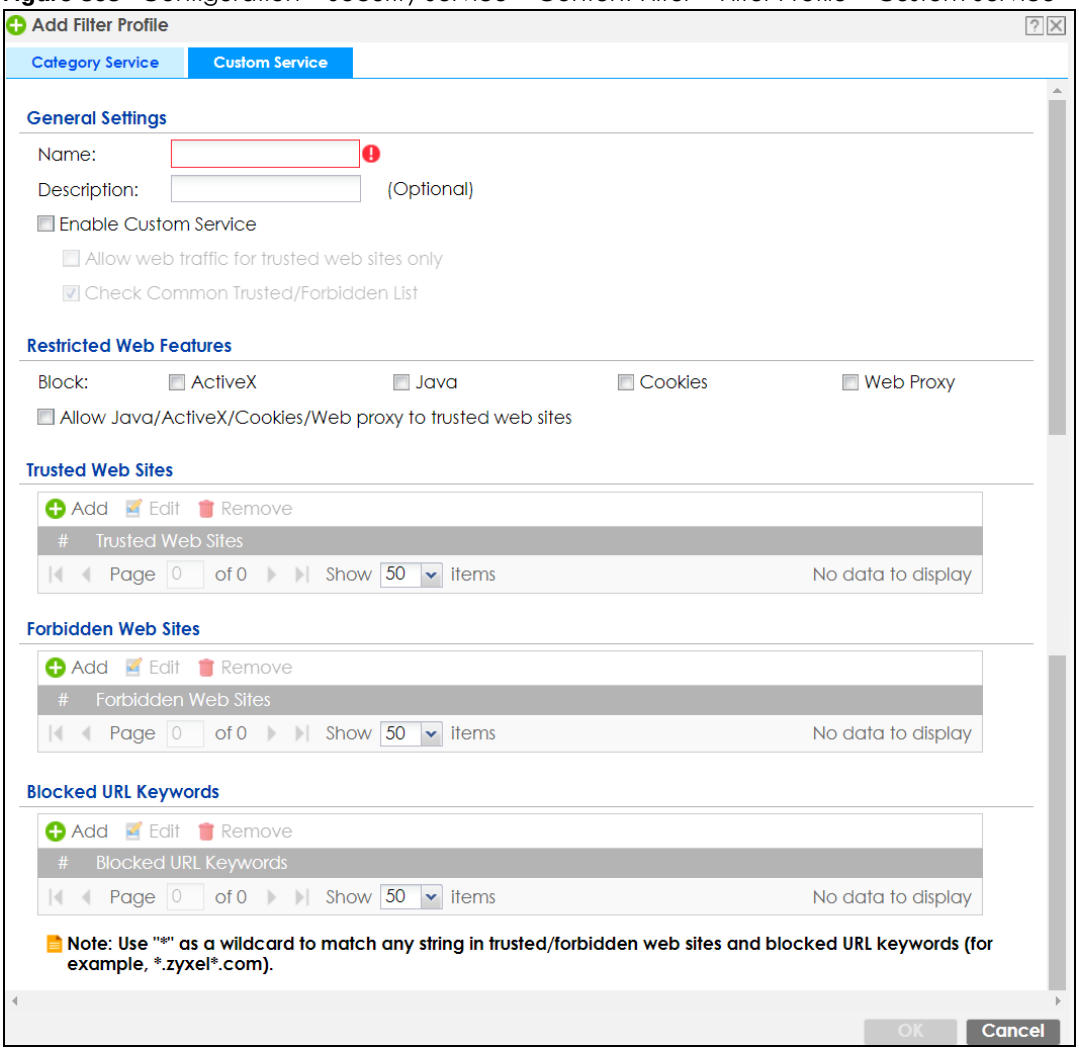
Table 211 Managed Category Descriptions (continued)

Peer-to-Peer	Sites that enable direct exchange of files between users without dependence on a central server. For example, www.eyny.com.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise. For example, 172.21.20.123, 192.168.35.62.
School Cheating	Sites that promote unethical practices such as cheating or plagiarism by providing test answers, written essays, research papers, or term papers. For example, www.zydk788.com, www.huafengksw.com.
Sex Education	Sites relating to sex education, including subjects such as respect for partner, abortion, gay and lesbian lifestyle, contraceptives, sexually transmitted diseases, and pregnancy. For example, apps.rockyou.com, www.howmama.com.tw, www.mombaby.com.tw.
Tasteless	Sites with offensive or tasteless content such as bathroom humor or profanity. For example, comedycentral.com, dilbert.com.
Child Abuse Images	Sites that portray or discuss children in sexual or other abusive acts. For example, a.uuzhijia.info.
Unknown	Unknown For example, www.669.com.tw, www.appleballoon.com.tw, www.uimco.com.tw.

27.2.3 Content Filter Add Filter Profile Custom Service

Click **Configuration > Security Service > Content Filter > Filter Profile > Add or Edit > Custom Service** to open the **Custom Service** screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 363 Configuration > Security Service > Content Filter > Filter Profile > Custom Service



The following table describes the labels in this screen.

Table 212 Configuration > Security Service > Content Filter > Profile > Custom Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Custom Service	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.
Allow Web traffic for trusted web sites only	When this box is selected, the Zyxel Device blocks Web access to sites that are not on the **Trusted Web Sites** list. If they are chosen carefully, this is the most effective way to block objectionable material.

Table 212 Configuration > Security Service > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Check Common Trusted/ Forbidden List	Select this check box to check the common trusted and forbidden web sites lists. See Section 27.3 on page 539 and Section 27.4 on page 540 for information on configuring these lists.
Restricted Web Features	Select the check box(es) to restrict a feature. Select the check box(es) to restrict a feature. • When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X. • When you download a page coming from a Web Proxy, the whole web page will be blocked. • When you download a page containing cookies, the cookies will be removed, but the page will not be blocked.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/ Web proxy to trusted web sites	When this box is selected, the Zyxel Device will permit Java, ActiveX and Cookies from sites on the **Trusted Web Sites** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "*zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter "*.com" to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.

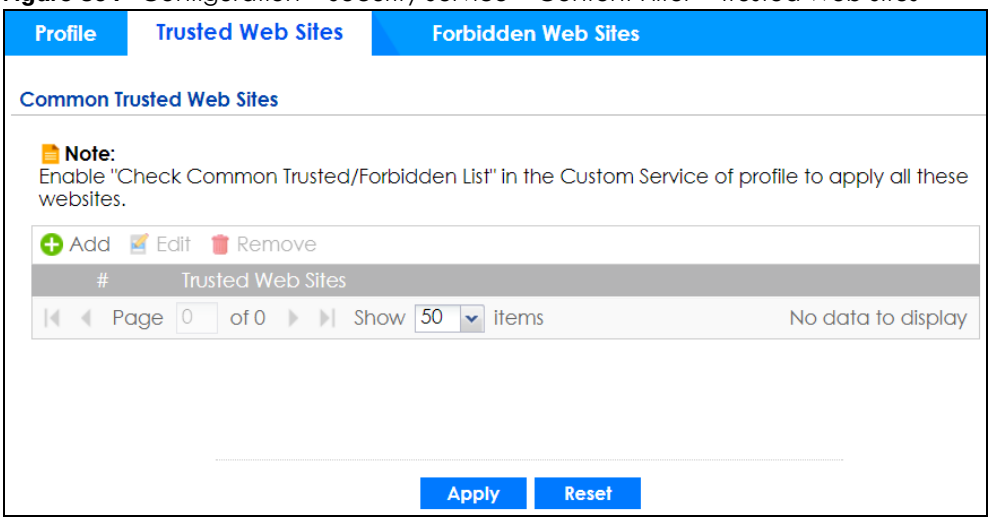
Table 212 Configuration > Security Service > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "*bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter "*.com" to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the blocked URL keywords.
Blocked URL Keywords	This list displays the keywords already added. Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address. Use up to 127 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*()%). "*" can be used as a wildcard to match any string. Use "|*" to indicate a single wildcard character. For example enter *Bad_Site* to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.3 Content Filter Trusted Web Sites Screen

Click **Configuration > Security Service > Content Filter > Trusted Web Sites** to open the **Trusted Web Sites** screen. You can create a common list of good (allowed) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Trusted Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 364 Configuration > Security Service > Content Filter > Trusted Web Sites



The following table describes the labels in this screen.

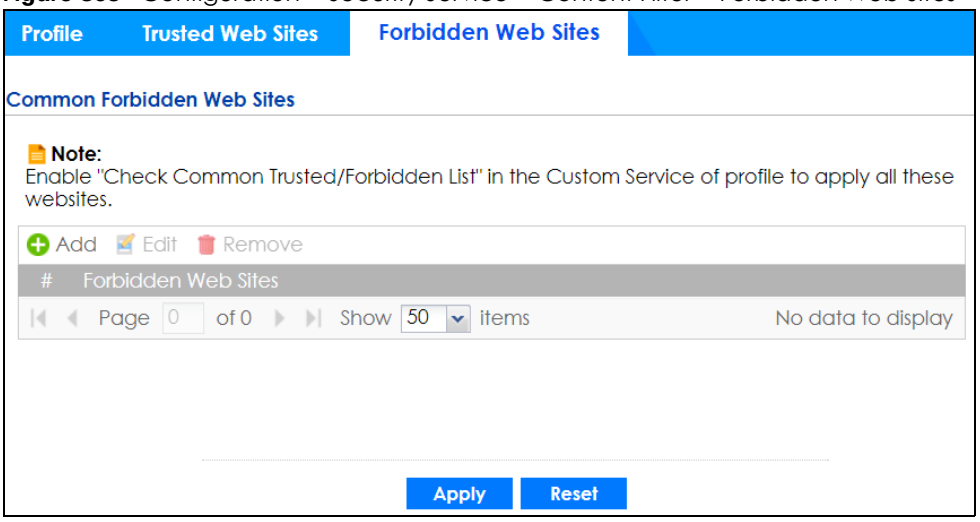
Table 213 Configuration > Security Service > Content Filter > Trusted Web Sites

LABEL	DESCRIPTION
Common Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

27.4 Content Filter Forbidden Web Sites Screen

Click **Configuration > Security Service > Content Filter > Forbidden Web Sites** to open the **Forbidden Web Sites** screen. You can create a common list of bad (blocked) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Forbidden Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 365 Configuration > Security Service > Content Filter > Forbidden Web Sites



The following table describes the labels in this screen.

Table 214 Configuration > Security Service > Content Filter > Forbidden Web Sites

LABEL	DESCRIPTION
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Reset** to return the screen to its last-saved settings.

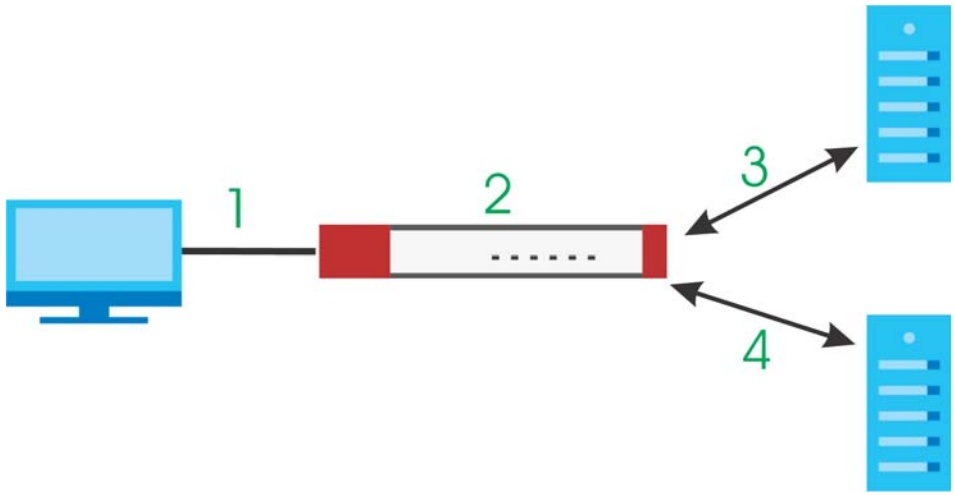
27.5 Content Filter Technical Reference

This section provides content filtering background information.

External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

Figure 366 Content Filter Lookup Procedure



1 A computer behind the Zyxel Device tries to access a web site.

2 The Zyxel Device looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the Zyxel Device's cache. The Zyxel Device blocks, blocks and logs or just logs the request based on your configuration.

3 Use the **Content Filter Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses. All of the web site address records are also cleared from the local cache when the Zyxel Device restarts.

4 If the Zyxel Device has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.

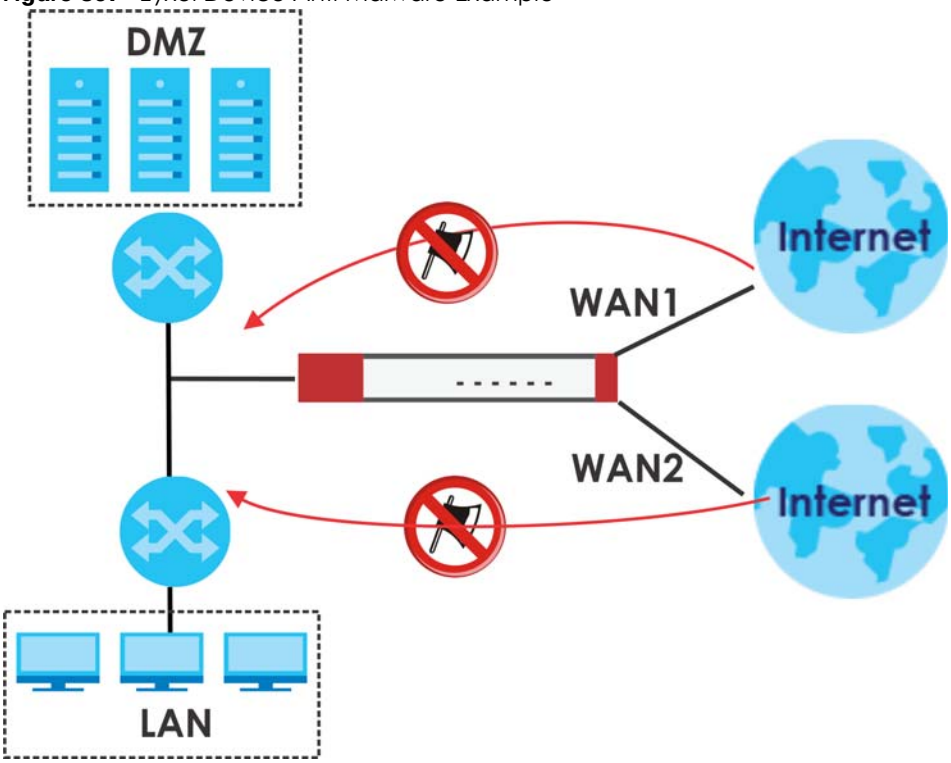
5 The external content filter server sends the category information back to the Zyxel Device, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the Zyxel Device's content filter cache.

CHAPTER 28
Anti-Malware

28.1 Overview

Use the Zyxel Device's anti-malware feature to protect your connected network from malware (malicious software) infection, such as computer virus, worms, and spyware. The Zyxel Device checks traffic going in both directions for signature matches. In the following figure, the Zyxel Device checks traffic coming from the WAN zone (which includes two interfaces) to the LAN zone.

Figure 367 Zyxel Device Anti-Malware Example



The anti-malware matches a file with those in a malware database. This is done as files go through the Zyxel Device.

Virus, Worm, and Spyware

A computer virus is a type of malicious software designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable. Spyware infiltrate your device and secretly gathers information about you, such as your network activity, passwords, bank details, and so on.

Hash Value

A hash function is an algorithm that maps data of arbitrary size to data of fixed size. The value returned by a hash function is a hash value. Hash values can be used to identify the contents of a file. During an anti-malware file scan, the hash value of a file is matched with signatures. At the time of writing, MD5 (Message Digest 5) is supported. MD5 is a hash algorithm used to authenticate packet data.

Local Signature Databases

The Zyxel Device downloads the signature(s) after it is registered and the anti-malware license is activated at myZyxel. A signature is a unique string of bits, or binary pattern, of a malware. A signature acts as a fingerprint that can be used to detect and identify specific malware. The Zyxel Device downloads the following signatures:

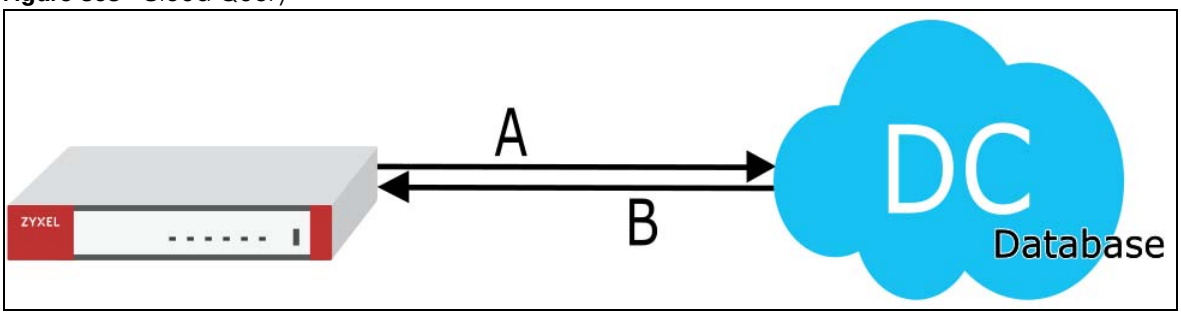
- Anti-malware signature
- Threat Intelligence Machine Learning

These signatures are periodically updated if you have a valid license. See Section 28.2 on page 548 for how the Zyxel Device updates these signatures for the anti-malware license.

Cloud Query

Another method of malware protection is through cloud query. This process is illustrated in the next figure. If **Cloud Query** is enabled, the Zyxel Device queries the **Defend Center** database by sending the file's hash value (**A**) and receiving the scan results (**B**) through the Defend Center (**DC**).

Figure 368 Cloud Query



Anti-Malware Licensing

Having extensive, up-to-date signatures with the most common malware is critical to making the anti-malware service work effectively. Section 7.2 on page 189 shows licensing information for the different signature databases that can be used by the Zyxel Device.

After the anti-malware license expires, you need to purchase an iCard to update your local signature database and use cloud query. Extend your license in the **Registration > Service** screen.

Anti-Malware Scan Process

Before going through the Anti-Malware scan, the Zyxel Device first identifies the packets sent by the following four major protocols with corresponding standard ports:

- FTP (File Transfer Protocol)

- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)

The Zyxel Device records the order of packets in TCP connection-oriented sessions to check for matching malware signatures. The order of non-setup packets such as SYN, ACK and FIN is ignored.

Anti-Malware Scanning Procedure:

1. The Zyxel Device checks every packet of the file for matches with the local signature databases.

   If a malware pattern signature is matched, the actions you specify for identified malware will be applied. If **Destroy infected file** is enabled, the file will be modified. Logs/alerts will be sent according to your settings.

   Note: The receiver is not notified if a file is modified by the Zyxel Device. If the file cannot be used, the receiver should contact the Zyxel Device administrator to confirm if the Zyxel Device modified the file by checking the logs.

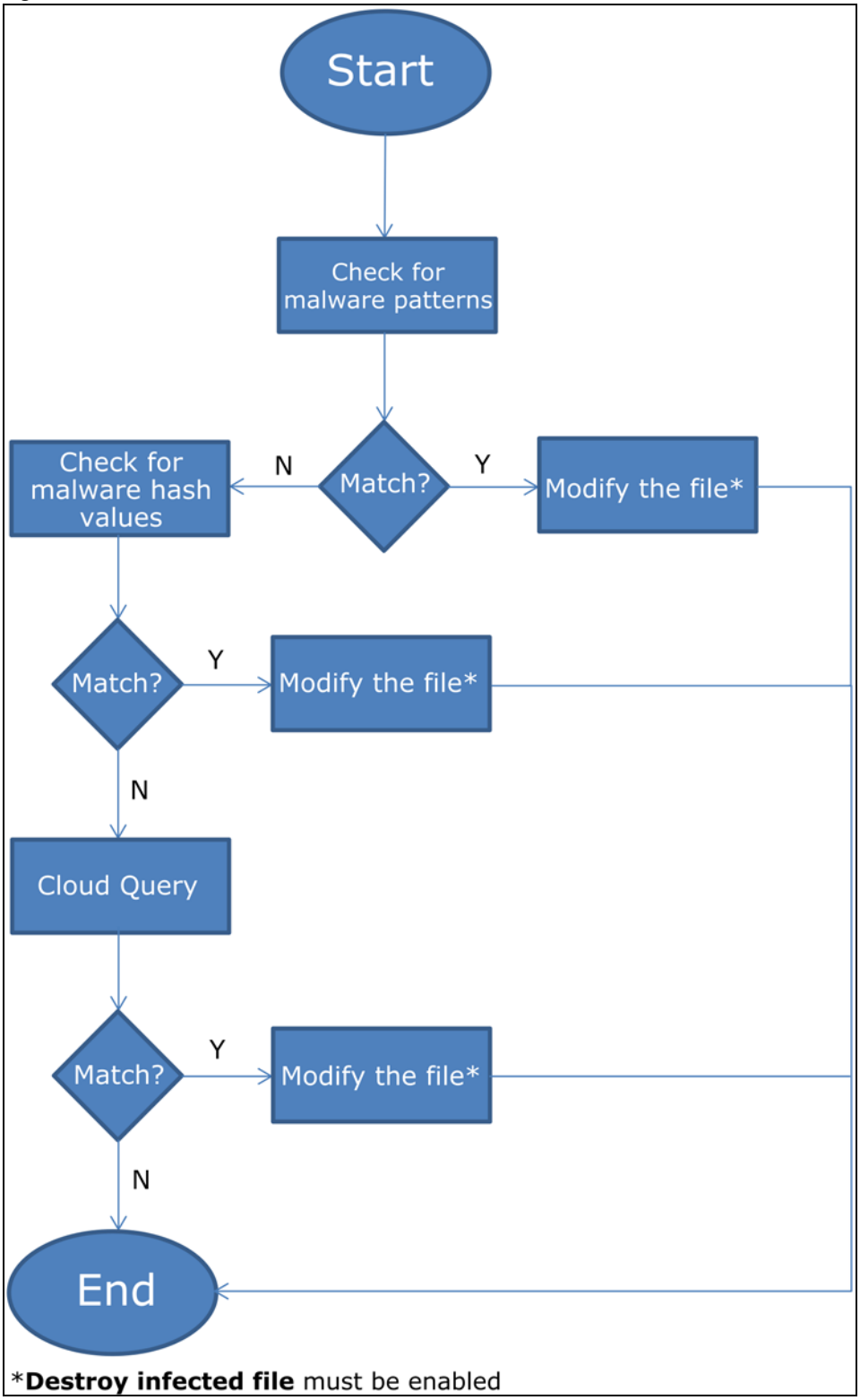
2. If no match is found with the local databases, the Zyxel Device uses **Cloud Query** to forward the file's hash value to Defend Center.

3. Defend Center checks its database for malware signature matches and sends the results back to the Zyxel Device.

   If a malware signature is matched, the actions you specify for identified malware will be applied. If **Destroy infected file** is enabled, the file will be modified. Logs/alerts will be sent according to your settings.

The next figure shows a flow chart detailing the anti-malware scan.

Figure 369 Anti-Malware flowchart



Cloud Query Supported File Types

At the time of writing, the following file types are supported by **Cloud Query**:

- 7z Archive (7z)
- AVI Video (avi)
- BMP Image (bmp)
- BZ2 Archive (bz2)
- Executables (exe)
- Macromedia Flash Data (swf)
- GIF Image (gif)
- GZ Archive (gz)
- JPG Image (jpg)
- MOV Video (mov)
- MP3 Audio (mp3)
- MPG Video (mpg)
- MS Office Document (doc...)
- PDF Document (pdf)
- PNG Image (png)
- RAR Archive (rar)
- RM Video (rm)
- RTF Document (rtf)
- TIFF Image (tif)
- WAV Audio (wav)
- ZIP Archive (zip)

Notes About the Zyxel Device Anti-Malware

The following lists important notes about the Zyxel Device's anti-malware feature:

1. Zyxel's anti-malware feature can detect polymorphic malware (see Section 28.6 on page 554).
2. When malware is detected, a log is created or an alert message is sent to the administrator depending on your log settings.
3. Changes to the Zyxel Device's anti-malware settings only affect new sessions, not sessions that already existed before you applied the changed settings.
4. Enabling **Cloud Query** may affect file transfer speeds.
5. The Zyxel Device does not scan the following file/traffic types:
   - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
   - Encrypted traffic. This could be password-protected files or VPN traffic where the Zyxel Device is not the endpoint (pass-through VPN traffic).
   - Traffic through custom (non-standard) ports. The Zyxel Device scans whatever port number is specified for FTP in the ALG screen.
   - All compressed files within a compressed file. Note that a single file can still be decompressed and scanned if you select **Enable file decompression (ZIP and RAR)**.
   - Traffic compressed or encoded using a method the Zyxel Device does not support.

Finding Out More

- See Section 28.6 on page 554 for anti-malware background information.

28.1.1 What You Can Do in this Chapter

- Use the **Anti-Malware** screen (Section 28.2 on page 548) to turn anti-malware on or off, and check the anti-malware signature status. In addition, you can set up anti-malware black (blocked) and white (allowed) lists of malware patterns.
- Use the **Signature** screen (Section 28.5 on page 553) to search for particular signatures and get more information about them.

28.2 Anti-Malware Screen

Click **Configuration > Security Service** > **Anti-Malware** to display the configuration screen as shown next.

Click the **Anti-Malware** icon for more information on the Zyxel Device's security features.

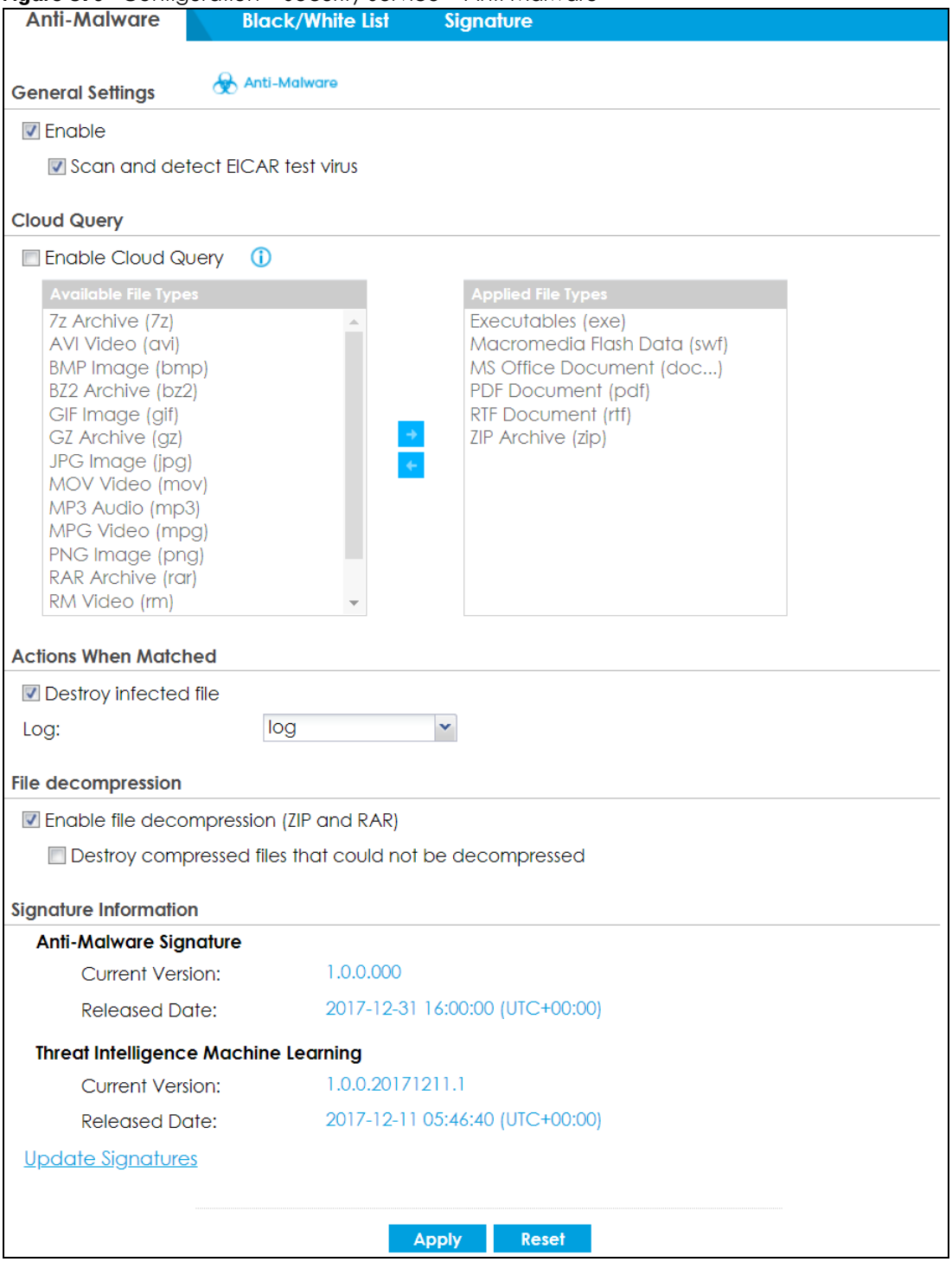
Note: The threat intelligence machine learning (TIML) feature is not available if the gold security pack is expired. Neither will the Zyxel Device update the TIML signatures, nor will it scan the TIML signatures that were downloaded when you used the gold security pack.

See Subscription Services Available on page 186 for more information on the subscription services for the two types of security packs.

Note: If "Destroy infected file" is disabled and "log" is set to "no", the Zyxel Device will still perform the scan but will not do anything else. It is recommended to enable at least one of the two functions.

If "Destroy infected file" is disabled, any malicious file found can still be executed by the end user after it is forwarded. The administrator would have to inform the user if there is an infected file.

Figure 370 Configuration > Security Service > Anti-Malware



The following table describes the labels in this screen.

Table 215 Configuration > Security Service > Anti-Malware

LABEL	DESCRIPTION
General Setting	
Enable	Select this checkbox to activate the anti-malware feature to protect your connected network from infection and the installation of malicious software. Selecting this checkbox also activates the threat intelligence machine learning (TIML) feature. TIML signatures come from the sandboxing inspection results and helps the Zyxel Device block possible malicious or suspicious files.
Scan and detect EICAR test virus	Select this option to have the Zyxel Device check for the EICAR test file and treat it in the same way as a real malware file. The EICAR test file is a standardized test file for signature based anti-malware scanners. When the scanner detects the EICAR file, it responds in the same way as if it found a real malware. Besides straightforward detection, the EICAR file can also be compressed to test whether the anti-malware software can detect it in a compressed file. The test string consists of the following human-readable ASCII characters. X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
Enable Cloud Query	Select this check box to enable the cloud query service. This improves the effectiveness of malware detection, but can affect file transfer speeds as it needs to send information to the cloud.
Available File Types	File types that can be checked by the Zyxel Device through cloud query are listed here. Note that the files on this list are currently bypassed. To use the cloud query feature on a specific file type, click this file type and then click the right arrow button. See available file types in Section 28.1 on page 543.
Applied File Types	File types that go through the cloud query process are listed here. If you don't want a file type to be checked, click this file type and then click the left arrow button.
Destroy infected file	When you select this check box, if a malware signature is matched, the Zyxel Device overwrites the infected portion of the file with zeros before being forwarded to the user. The uninfected portion of the file will pass through unmodified.
Log	These are the log options: • **no**: Do not create a log when a packet matches a signature(s). • **log**: Create a log on the Zyxel Device when a packet matches a signature(s). • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a packet matches a signature(s).
Check White List	Select this check box to have the Zyxel Device not perform the anti-malware check on files with names that match the white list patterns.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
File Pattern	This is the file name pattern. If a file's name matches this pattern, the Zyxel Device does not check the file for malware.
Check Black List	Select this check box to log and delete files with names that match the black list patterns.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.

Table 215 Configuration > Security Service > Anti-Malware (continued)

LABEL	DESCRIPTION
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
File Pattern	This is the file name pattern. If a file's name that matches this pattern, the Zyxel Device logs and then destroys the file.
File decompression	
Enable file decompression (ZIP and RAR)	Select this check box to have the Zyxel Device scan a compressed file (the file does not need to have a "zip" or "rar" file extension). The Zyxel Device first decompresses the file and then scans the contents for malware. Note: The Zyxel Device decompresses a compressed file once. The Zyxel Device does NOT decompress any file(s) within a compressed file.
Destroy compressed files that could not be decompressed	When you select this check box, the Zyxel Device deletes compressed files that use password encryption. Select this check box to have the Zyxel Device delete any compressed files that it cannot decompress. The Zyxel Device cannot decompress password protected files or a file within another compressed file. There are also limits to the number of compressed files that the Zyxel Device can concurrently decompress. Note: The Zyxel Device's firmware package cannot go through the Zyxel Device with this check box enabled. The Zyxel Device classifies the firmware package as a file that cannot be decompressed and then deletes it. Clear this check box when you download a firmware package from the Zyxel website. It's OK to upload a firmware package to the Zyxel Device with the check box selected.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the signature set version number currently used by the Zyxel Device. This number gets larger as the set is enhanced.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

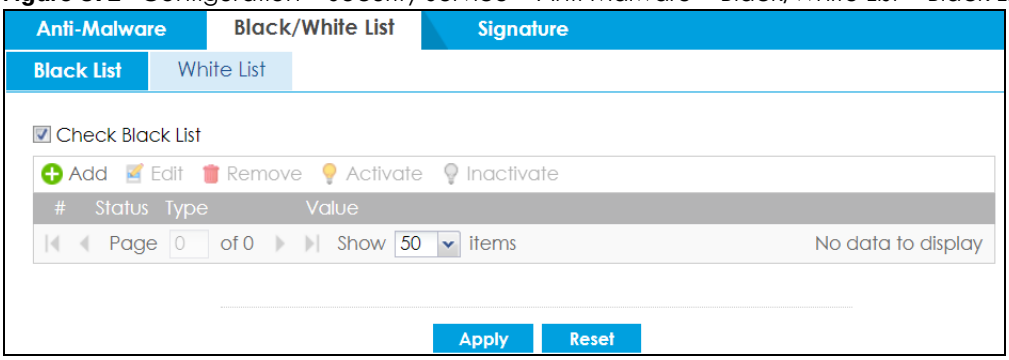
28.3 The Black List Screen

A black list allows you to specify the file or encryption pattern that you want to block. False positives occur when a non-infected file matches a malware signature.

Enter a file or encryption pattern that would cause the Zyxel Device to log and then destroy this file.

Click **Configuration** > **Security Service** > **Anti-Malware** > **Black/White List** > **Black List** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 371 Configuration > Security Service > Anti-Malware > Black/White List > Black List



The following table describes the fields in this screen.

Table 216 Configuration > Security Service > Anti-Malware > Black/White List > Black List

LABEL	DESCRIPTION
Check Black List	Select this check box to log and delete files with names or encryption algorithm (**MD5 Hash**) that match the black list patterns.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
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 entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Type	This field displays the type (**MD5 Hash** or **File Pattern**) used to distinguish whether a file should be blocked. Select the type (**MD5 Hash** or **File Pattern**) that you want to use to distinguish whether a file should be blocked.
Value	This field displays the file or encryption pattern of the entry. Enter the file or encryption pattern for this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

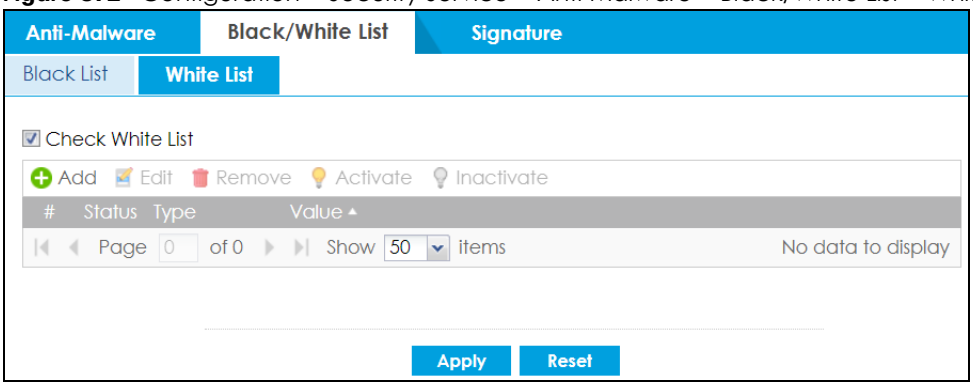
28.4 The White List Screen

A white list allows you to specify the file or encryption pattern to allow in order to avoid false positives. False positives occur when a non-infected file matches a malware signature.

Enter a file or encryption pattern that would cause the Zyxel Device to allow this file.

Click **Configuration** > **Security Service** > **Anti-Malware** > **Black/White List** > **White List** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 372 Configuration > Security Service > Anti-Malware > Black/White List > White List



The following table describes the fields in this screen.

Table 217 Configuration > Security Service > Anti-Malware > Black/White List > White List

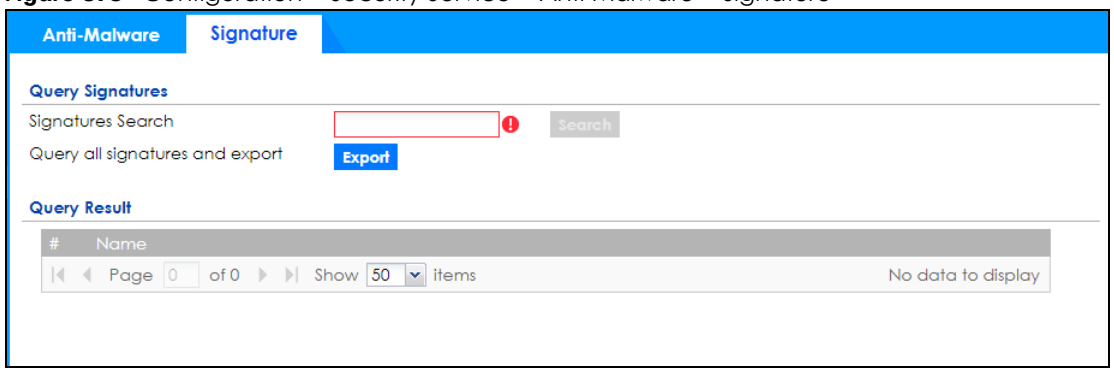
LABEL	DESCRIPTION
Check White List	Select this check box to have the Zyxel Device not perform the anti-malware check on files with names or algorithm (**MD5 Hash**) that match the white list patterns.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
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 entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Type	This field displays the type (**MD5 Hash** or **File Pattern**) used to distinguish whether a file should be allowed. Select the type (**MD5 Hash** or **File Pattern**) that you want to use to distinguish whether a file should be allowed.
Value	This field displays the file or encryption pattern of the entry. Enter the file or encryption pattern for this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

28.5 Anti-Malware Signature Searching

Click **Configuration > Security Service > Anti-Malware > Signature** to display this screen. Use this screen to locate signatures and display details about them.

If your web browser opens a warning screen about a script making the web browser run slowly and the computer unresponsive, just click **No** to continue. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 373 Configuration > Security Service > Anti-Malware > Signature



The following table describes the labels in this screen.

Table 218 Configuration > Security Service > Anti-Malware > Signature

LABEL	DESCRIPTION
Signatures Search	Enter the name, part of the name or keyword of the signature(s) you want to find and click **Search**. This search is not case-sensitive and accepts numerical strings.
Query all signatures and export	Click **Export** to have the Zyxel Device save all of the anti-malware signatures to your computer in a .txt file.
Query Result	
#	This is the entry's index number in the list.
Name	This is the name of the anti-malware signature. Click the **Name** column heading to sort your search results in ascending or descending order according to the signature name. Click a signature's name to see details about the malware.

28.6 Anti-Malware Technical Reference

Types of Malware

The following table describes some of the common malware.

Table 219 Common Malware Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
Email Virus	Email viruses are malicious programs that spread through email.
Polymorphic Virus	A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-malware scanner to detect or intercept it. A polymorphic virus can also belong to any of the virus types discussed above.

Malware Infection and Prevention

The following describes a simple life cycle of malware.

1. A computer gets a copy of malware from a source such as the Internet, email, file sharing or any removable storage media. The malware is harmless until the execution of an infected program.
2. The malware spreads to other files and programs on the computer.
3. The infected files are unintentionally sent to another computer thus starting the spread of the malware.
4. Once the malware is spread through the network, the number of infected networked computers can grow exponentially.

Types of Anti-Malware Scanner

The section describes two types of anti-malware scanner: host-based and network-based.

A host-based anti-malware (HAM) scanner is often software installed on computers and/or servers in the network. It inspects files for malware patterns as they are moved in and out of the hard drive. However, host-based anti-malware scanners cannot eliminate all malware for a number of reasons:

- HAM scanners are slow in stopping malware threats through real-time traffic (such as from the Internet).
- HAM scanners may reduce computing performance as they also share the resources (such as CPU time) on the computer for file inspection.
- You have to update the malware signatures and/or perform malware scans on all computers in the network regularly.

A network-based anti-malware (NAM) scanner is often deployed as a dedicated security device (such as your Zyxel Device) on the network edge. NAM scanners inspect real-time data traffic (such as email messages or web) that tends to bypass HAM scanners. The following lists some of the benefits of NAM scanners.

- NAM scanners stop malware threats at the network edge before they enter or exit a network.
- NAM scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

CHAPTER 29
Reputation Filter

29.1 Overview

Use the **Reputation Filter** screens to configure settings for IP reputation and botnet filtering.

29.1.1 What You Need to Know

IP Reputation

IP reputation checks the reputation of an IP address from a database. An IP address with bad reputation associates with suspicious activities, such as spam, virus, and/or phishing. The Zyxel Device will respond when there are packets coming from an IPv4 address with bad reputation.

Botnet Filtering

A botnet is a network consisting of computers that are infected with malware and remotely controlled. The infected computers will contact and wait for instructions from a command and control (C&C) server(s). An attacker can control the botnet by setting up a C&C server and sending commands to the infected computers. Alternatively, a peer-to-peer network approach is used. The infected computer scans and communicates with the peer devices in the same botnet to share commands or malware sent by the C&C server.

29.1.2 What You Can Do in this Chapter

- Use the **IP Reputation** screen (Section 29.2 on page 556) to enable IP reputation and specify what action the Zyxel Device takes when any IP address with bad reputation is detected.
- Use the **Botnet Filter** screen (Section 29.3 on page 561) to enable botnet filtering and specify what action the Zyxel Device takes when any suspicious activity is detected.

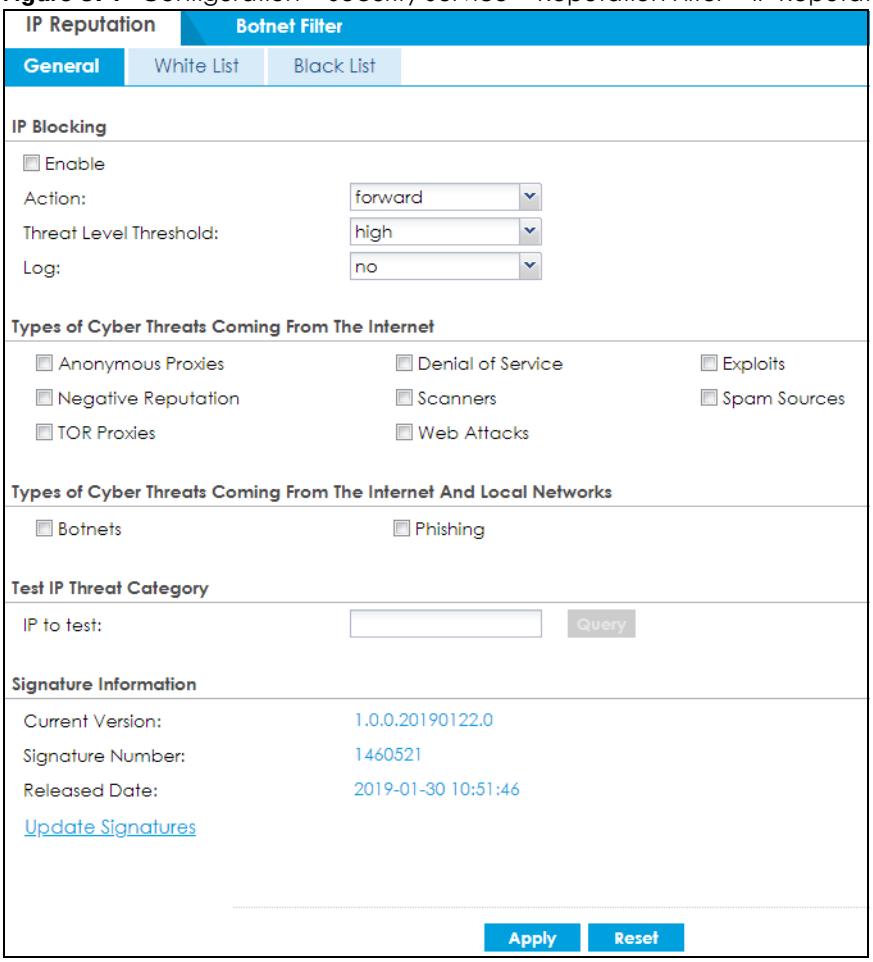
29.2 IP Reputation Screen

When you register for and enable the IP reputation service, your Zyxel Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Zyxel Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.

Use this screen to enable IP reputation and specify the action the Zyxel Device takes when it detects a suspicious activity or a connection attempt to or from an IPv4 address with bad reputation.

Click **Configuration > Security Service > Reputation Filter > IP Reputation > General** to display the configuration screen as shown next.

Figure 374 Configuration > Security Service > Reputation Filter > IP Reputation > General



The following table describes the labels in this screen.

Table 220 Configuration > Security Service > Reputation Filter > IP Reputation > General

LABEL	DESCRIPTION
IP Blocking	
Enable	Select this option to turn on IP blocking on the Zyxel Device. Otherwise, deselect it.
Action	Set what action the Zyxel Device takes when packets come from an IPv4 address with bad reputation. **forward**: Select this action to have the Zyxel Device allow the packet to go through. **block**: Select this action to have the Zyxel Device deny the packets and send a TCP RST to both the sender and receiver when a packet comes from an IPv4 address with bad reputation.
Threat Level Threshold	Select the threshold threat level to which the Zyxel Device will take action (**high**, **medium and above**, **Low and above**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. • **high**: An IPv4 address that scores 0 to 20 points. • **medium and above**: An IPv4 address that scores 0-60 points. • **Low and above**: An IPv4 address that scores 0-80 pointgs.

Table 220 Configuration > Security Service > Reputation Filter > IP Reputation > General (continued)

LABEL	DESCRIPTION
Log	These are the log options: **no**: Do not create a log when the packet comes from an IPv4 address with bad reputation. **log**: Create a log on the Zyxel Device when the packet comes from an IPv4 address with bad reputation. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when the packet comes from an IPv4 address with bad reputation.
Types of Cyber Threats Coming From The Internet	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers. Otherwise, deselect it.
Anonymous Proxies	Sites and proxies that act as an intermediary for surfing to other websites in an anonymous fashion, whether to circumvent Web filtering or for other reasons. For example, blog.go2.tw, anonymizer.com, www.qu365.com.
Denial of Service	Sites that issue Denial of Service (DoS) attacks, such as DoS, DDoS, SYN flood, and anomalous traffic detection. DoS attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The goal of DoS attacks is not to steal information, but to disable a device or network on the Internet. A Distributed Denial of Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. SYN flood is an attack that attackers flood SYN packets to a server in TCP handshakes, and not respond with ACK packets on purpose. This keeps the server waiting for attackers' responses to establish TCP connections, and make the server unavailable. Anomalous traffic detection could be malicious activities, such as malware outbreaks or hacking attempts.
Exploits	Sites that distribute exploits or exploit kits to infect website visitors' devices. Exploits include shellcode, root kits, worms, or viruses that download additional malware to infect devices. An exploit kit consists of different exploits.
Negative Reputation	Sites that have bad reputation and associate with suspicious activities, such as spam, virus, and/or phishing.
Scanners	Sites that run unauthorized system vulnerabilities scan to look for vulnerabilities in website visitors' devices.
Spam Sources	Sites that have been promoted through spam techniques. For example, img.tongji.linezing.com, banner.chinesegamer.net.
TOR Proxies	Sites that act as the exit nodes in a Tor (The Onion Router) network. Tor is a service that keep users anonymous in the Internet and make users' Internet activities untraceable. Tor hides user's real IP addresses by encrypting data and transmitting the encrypted data in a chain of selected nodes acting as intermediaries. Each node can only decrypt the data sent from the node before it. The first node that receives the encrypted data is called the entry node. The last node is the last intermediary that the encrypted data will go through before it arrives at the destination.

Table 220 Configuration > Security Service > Reputation Filter > IP Reputation > General (continued)

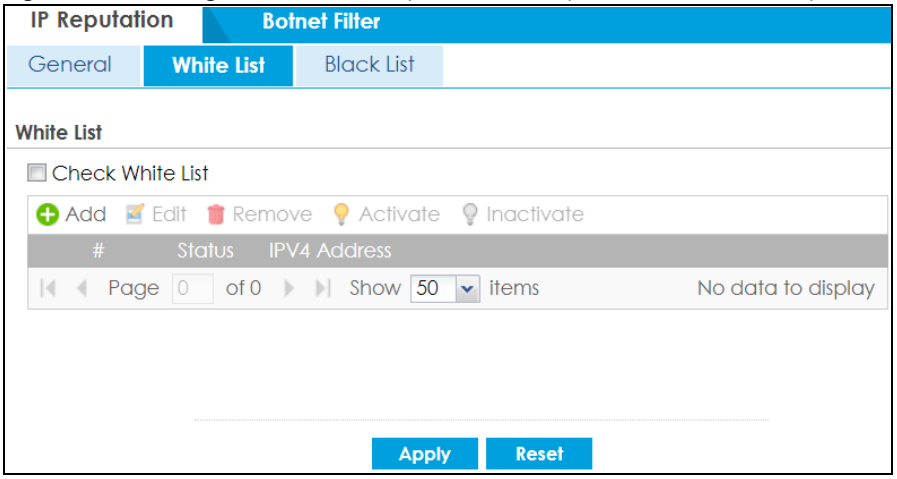
LABEL	DESCRIPTION
Web Attacks	Sites that launch web attacks, such as SQL injection, cross site scripting, iframe injection, and brute force attack. SQL injection (SQLI) is an attack that attackers insert malicious SQL (Structured Query Language) code into a web application database query. Attackers can then access, add, modify, or delete data in users' databases. Cross site scripting (XSS) is an attack that attackers injects malicious scripts to websites or web applications in the form of HTML or JavaScript code. The scripts execute when users visit the infected web page or perform the infected web applications. XSS will cause failures to encrypt traffic, cookie stealing, identity impersonation, and phishing. Iframe injection is an attack that attackers injects malicious iframe (inline frame) tags to websites. The malicious iframe tag downloads malware to the devices of the infected websites' visitors, and steal users' sensitive information. An iframe tag is an HTML tag that is used to embed contents from another source in a website, but attackers misuse this feature. Brute force attack is an attack that attackers attempt to gain access to websites or device via a succession of different passwords.
Types of Cyber Threats Coming From The Internet And Local Networks	Select the categories of packets that come from the Internet and local network. The categories of packets are known to pose a security threat to users or their computers. Otherwise, deselect it.
Botnets	Sites that use bots (zombies) including command-and-control (C&C) servers.
Phishing	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials. For example, optimizedby.rmxads.com, 218.1.71.226/.../e3b.
Test IP Threat Category	
IP to test	Enter an IPv4 address of a website, and click the **Query** button to check if the website associates with suspicious activities that could pose a security threat to users or their computers.
Signature Information	The Zyxel Device comes with signatures for IP reputation. These signatures are continually updated as new malware evolves. New signatures can be downloaded to the Zyxel Device periodically if you have subscribed for the IP reputation signatures service. You need to create an account at myZyxel, register your Zyxel Device and then subscribe for IP reputation service in order to be able to download new signatures from myZyxel (see the **Registration** screens). The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the signature set version number currently used by the Zyxel Device. This number gets larger as new signatures are added.
Signature Number	This field displays the number of signatures in this set.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this to go to the **Configuration > Licensing > Signature Update** screen to check for new signatures at myZyxel. You can schedule or immediately download signatures.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.2.1 IP Reputation White List Screen

Use this screen to create white list entries. The Zyxel Device will allow the incoming and outgoing packets from the listed IPv4 addresses.

You can add up to 256 entries in the IP reputation white list.

Figure 375 Configuration > Security Service > Reputation Filter > IP Reputation > White List



The following table describes the labels in this screen.

Table 221 Configuration > Security Service > Reputation Filter > IP Reputation > White List

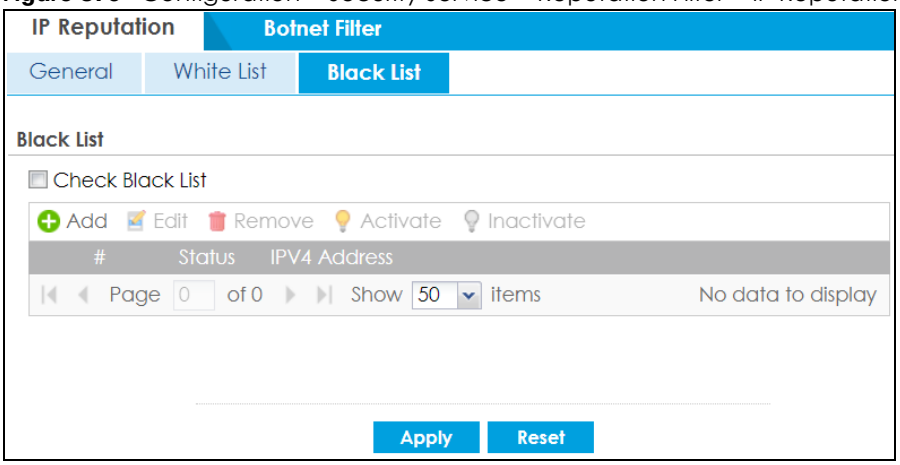
LABEL	DESCRIPTION
White List	
Check White List	Select this check box and the Zyxel Device will allow the incoming packets that come from the listed IPv4 addresses. Note: Enable IP blocking in the **Configuration** > **Security Service** > **Reputation Filter** > **IP Reputation** > **General** screen for the white list to take effect.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
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 entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
IPv4 Address	This field displays the IPv4 address of this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.2.2 IP Reputation Black List Screen

Use this screen to create black list entries. The Zyxel Device will block the incoming and outgoing packets from the listed IPv4 addresses.

You can add up to 256 entries in the IP reputation black list.

Figure 376 Configuration > Security Service > Reputation Filter > IP Reputation > Black List



The following table describes the labels in this screen.

Table 222 Configuration > Security Service > Reputation Filter > IP Reputation > Black List

LABEL	DESCRIPTION
Black List	
Check Black List	Select this check box and the Zyxel Device will block the incoming packets that come from the listed IPv4 addresses. Note: Enable IP blocking in the **Configuration** > **Security Service** > **Reputation Filter** > **IP Reputation** > **General** screen for the black list to take effect.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
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 entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
IPv4 Address	This field displays the IPv4 address of this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.3 Botnet Filter Screen

The Zyxel Device's botnet filtering service allows you to detect and block connection attempts to or from the C&C server or known botnet IP addresses.

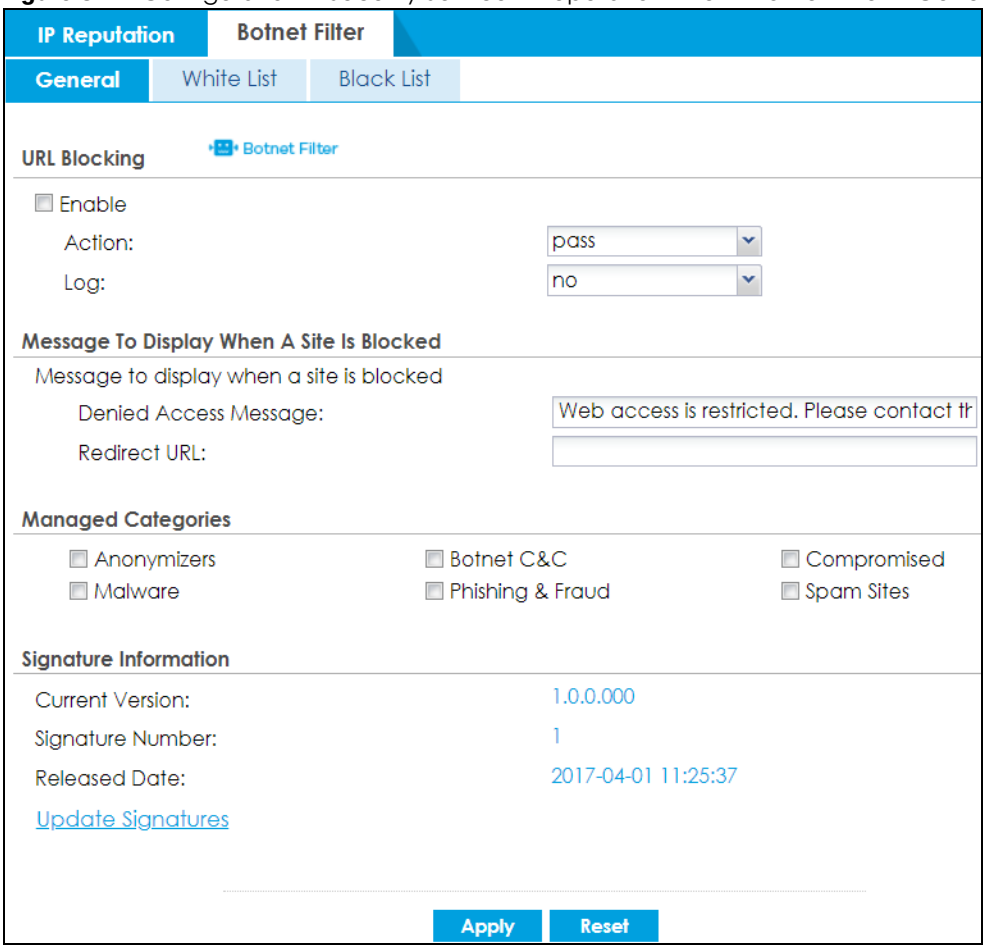
When you register for and enable the botnet filtering service, your Zyxel Device downloads signature files that contain known botnet domain names and IP addresses. The Zyxel Device will also access an external database that has millions of web sites categorized based on content. You can have the Zyxel Device allow, block, block and/or log access to web sites or hosts based on these signatures and categories.

Use this screen to enable botnet filtering and specify the action the Zyxel Device takes when it detects a suspicious activity or a connection attempt to or from a botnet C&C server.

Click the **Botnet Filter** icon for more information on the Zyxel Device's security features.

Click **Configuration > Security Service > Reputation Filter > Botnet Filter** to display the configuration screen as shown next.

Figure 377 Configuration > Security Service > Reputation Filter > Botnet Filter > General



The following table describes the labels in this screen.

Table 223 Configuration > Security Service > Reputation Filter > Botnet Filter > General

LABEL	DESCRIPTION
URL Blocking	
Enable	Select this option to turn on URL blocking on the Zyxel Device.

Table 223 Configuration > Security Service > Reputation Filter > Botnet Filter > General (continued)

LABEL	DESCRIPTION
Action	Set what action the Zyxel Device takes when it detects a connection attempt to or from the web pages of the specified categories. **block**: Select this action to have the Zyxel Device block access to the web pages that match the categories that you select above. **warn**: Select this action to have the Zyxel Device display a warning message to the access requesters for the web pages before allowing users to access web pages that match the categories that you select above. **pass**: Select this action to have the Zyxel Device allow access to the web pages that match the categories that you select above.
Log	These are the log options: **no**: Do not create a log when it detects a connection attempt to or from the web pages of the specified categories. **log**: Create a log on the Zyxel Device when it detects a connection attempt to or from the web pages of the specified categories.
Message to display when a site is blocked	
Denied Access Message	Enter a message to be displayed when the botnet filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the botnet filter blocks access to a web page, the Zyxel Device just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by the botnet filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Managed Categories	Select the categories of web pages that are known to pose a security threat to users or their computers. Otherwise, deselect it.
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent Web filtering or for other reasons. For example, blog.go2.tw, anonymizer.com, www.qu365.com.
Botnet C&C	Sites that use bots (zombies) including command-and-control (C&C) servers.
Compromised	Sites that have been compromised by someone other than the site owner in order to install malicious programs without the user's knowledge. Includes sites that may be vulnerable to a particular high-risk attack. For example, www.wokoo.net, movie.sx.zj.cn.
Malware	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent. For example, www.tqlkg.com, aladel.net.
Phishing & Fraud	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials. For example, optimizedby.rmxads.com, 218.1.71.226/.../e3b.
Spam Sites	Sites that have been promoted through spam techniques. For example, img.tongji.linezing.com, banner.chinesegamer.net.

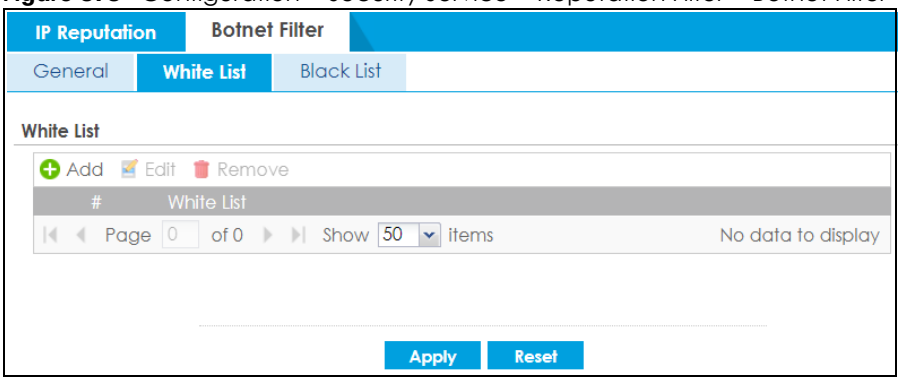
Table 223 Configuration > Security Service > Reputation Filter > Botnet Filter > General (continued)

LABEL	DESCRIPTION
Signature Information	The Zyxel Device comes with signatures for the botnet filter. These signatures are continually updated as new malware evolves. New signatures can be downloaded to the Zyxel Device periodically if you have subscribed for the botnet filter signatures service. You need to create an account at myZyxel, register your Zyxel Device and then subscribe for botnet filter service in order to be able to download new signatures from myZyxel (see the **Registration** screens). The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the signature set version number currently used by the Zyxel Device. This number gets larger as new signatures are added.
Signature Number	This field displays the number of signatures in this set.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this to go to the **Configuration > Licensing > Signature Update** screen to check for new signatures at myZyxel. You can schedule or immediately download signatures.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.3.1 Botnet Filter White List Screen

Use this screen to create white list entries. The Zyxel Device will allow the incoming packets from the listed IPv4 addresses and URLs.

Figure 378 Configuration > Security Service > Reputation Filter > Botnet Filter > White List



The following table describes the labels in this screen.

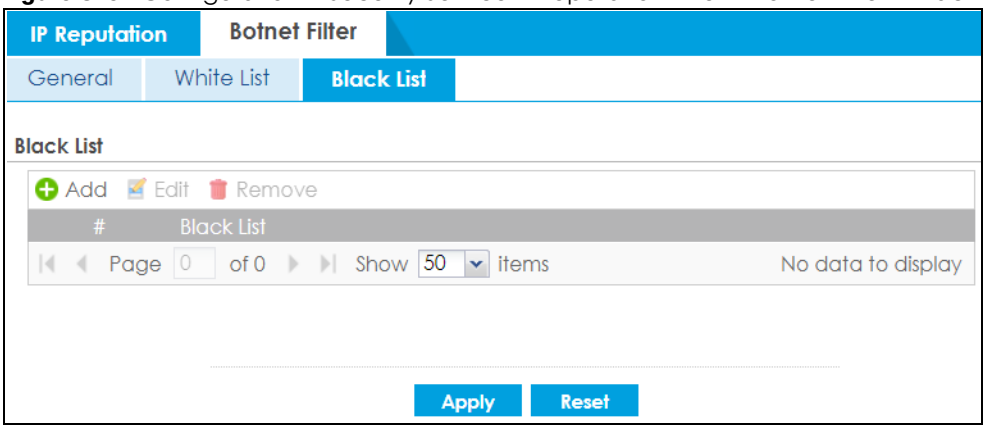
Table 224 Configuration > Security Service > Reputation Filter > Botnet Filter > White List

LABEL	DESCRIPTION
White List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
White List	This field displays the URL of this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.3.2 Botnet Filter Black List Screen

Use this screen to create black list entries. The Zyxel Device will block the incoming packets from the listed IPv4 addresses and URLs.

Figure 379 Configuration > Security Service > Reputation Filter > Botnet Filter > Black List



The following table describes the labels in this screen.

Table 225 Configuration > Security Service > Reputation Filter > Botnet Filter > Black List

LABEL	DESCRIPTION
Black List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Black List	This field displays the URL of this entry.
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 30
IDP

30.1 Overview

This chapter introduces packet inspection IDP (Intrusion, Detection and Prevention), custom signatures, and updating signatures. An IDP system can detect malicious or suspicious packets and respond instantaneously. IDP on the Zyxel Device protects against network-based intrusions.

30.1.1 What You Can Do in this Chapter

- Use the **Security Service > IDP** screen (Section 30.2 on page 566) to view registration and signature information.
- Use the **Security Service > IDP > Custom Signature > Add** screens (Section 30.3 on page 572) to create a new custom signature, edit an existing signature, delete existing signatures or save signatures to your computer.

30.1.2 What You Need To Know

Packet Inspection Signatures

A signature is a pattern of malicious or suspicious packet activity. You can specify an action to be taken if the system matches a stream of data to a malicious signature. You can change the action in the profile screens. Packet inspection examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior.

Applying Your IDP Configuration

Changes to the Zyxel Device's IDP settings affect new sessions, but not the sessions that already existed before you applied the new settings.

30.1.3 Before You Begin

- Register for a trial IDP subscription in the **Registration** screen. This gives you access to free signature updates. This is important as new signatures are created as new attacks evolve. When the trial subscription expires, purchase and enter a license key using the same screens to continue the subscription.

30.2 The IDP Screen

An IDP profile is a set of packet inspection signatures.

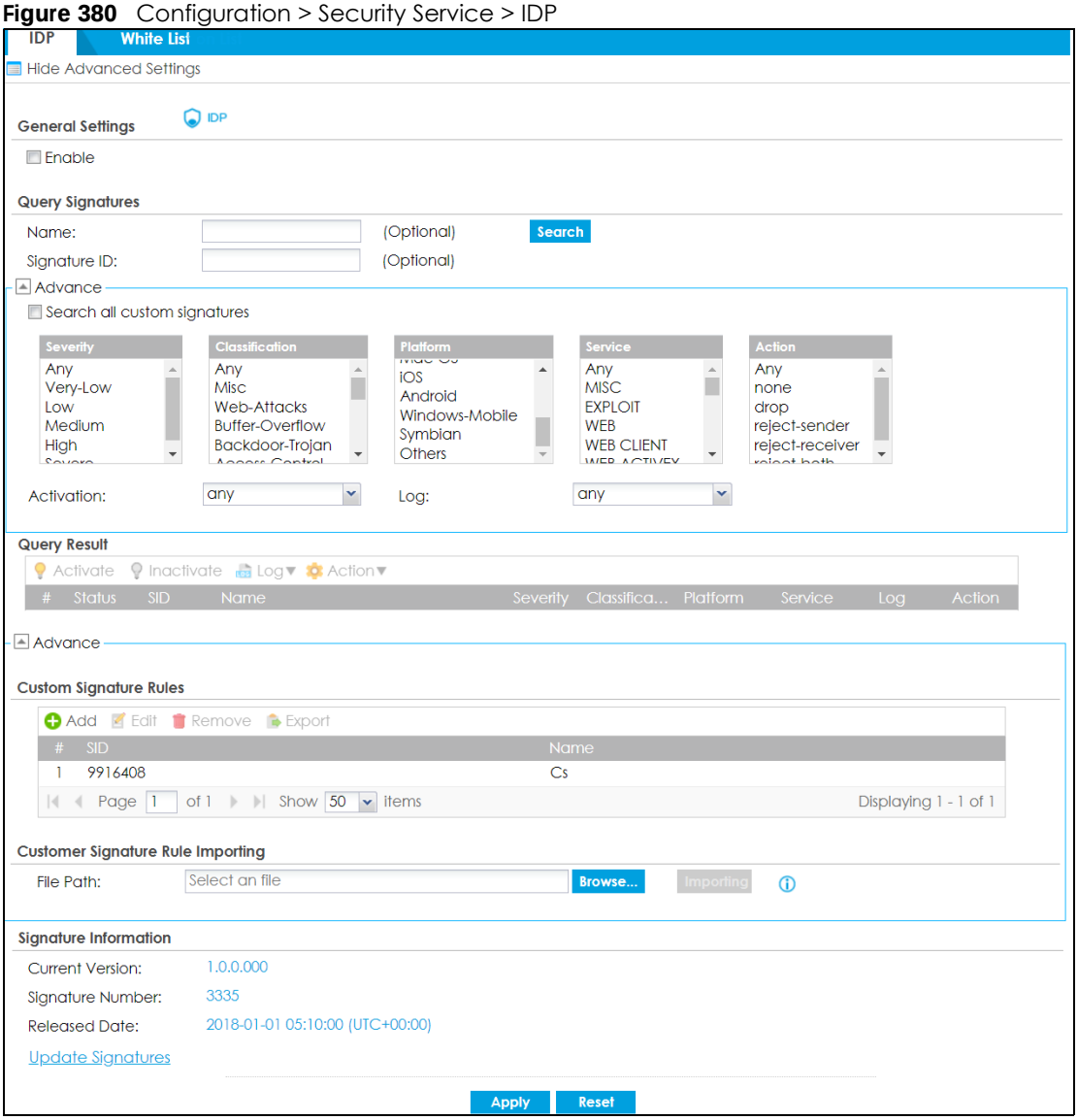
Click **Configuration > Security Service > IDP** to open this screen. Use this screen to view registration and signature information.

Note: You must register in order to update packet inspection signatures. See the **Registration** screens.

If you try to enable IDP when the IDP service has not yet been registered, a warning screen displays and IDP is not enabled.

Click the **IDP** icon for more information on the Zyxel Device's security features.

Figure 380 Configuration > Security Service > IDP



The following table describes the fields in this screen.

Table 226 Configuration > Security Service > IDP

LABEL	DESCRIPTION
General Settings	
Enable	Select this check box to activate the IDP feature which detects and prevents malicious or suspicious packets and responds instantaneously.
Query Signatures	
Name	Type the name or part of the name of the signature(s) you want to find.
Signature ID	Type the ID or part of the ID of the signature(s) you want to find.
Search all custom signatures	Select this check box to include signatures you created or imported in the **Custom Signatures** screen in the search. You can search for specific signatures by name or ID. If the name and ID fields are left blank, then all signatures are searched according to the criteria you select.
Severity	Search for signatures by severity level(s). Hold down the [Ctrl] key if you want to make multiple selections. These are the severities as defined in the Zyxel Device. The number in brackets is the number you use if using commands. **Severe** (5): These denote attacks that try to run arbitrary code or gain system privileges. **High** (4): These denote known serious vulnerabilities or attacks that are probably not false alarms. **Medium** (3): These denote medium threats, access control attacks or attacks that could be false alarms. **Low** (2): These denote mild threats or attacks that could be false alarms. **Very-Low** (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc.
Classification Type	Search for signatures by attack type(s) (see Table 227 on page 569). Attack types are known as policy types in the group view screen. Hold down the [Ctrl] key if you want to make multiple selections.
Platform	Search for signatures created to prevent intrusions targeting specific operating system(s). Hold down the [Ctrl] key if you want to make multiple selections.
Service	Search for signatures by IDP service group(s). See Table 227 on page 569 for group details. Hold down the [Ctrl] key if you want to make multiple selections.
Action	Search for signatures by the response the Zyxel Device takes when a packet matches a signature.Hold down the [Ctrl] key if you want to make multiple selections.
Activation	Search for activated and/or inactivated signatures here.
Log	Search for signatures by log option here.
Query Result	The results are displayed in a table showing the **SID, Name, Severity, Classification Type, Platform, Service, Log**, and **Action** criteria as selected in the search. Click the **SID** column header to sort search results by signature ID.
Custom Signature Rules	Use this part of the screen to create, edit, delete or export (save to your computer) custom signatures.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Export	To save an entry or entries as a file on your computer, select them and click **Export**. Click **Save** in the file download dialog box and then select a location and name for the file. Custom signatures must end with the 'rules' file name extension, for example, MySig.rules.

Table 226 Configuration > Security Service > IDP (continued)

LABEL	DESCRIPTION
#	This is the entry's index number in the list.
SID	SID is the signature ID that uniquely identifies a signature. Click the SID header to sort signatures in ascending or descending order. It is automatically created when you click the **Add** icon to create a new signature. You can edit the ID, but it cannot already exist and it must be in the 9000000 to 9999999 range.
Name	This is the name of your custom signature. Duplicate names can exist, but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent.
Customer Signature Rule Importing	Use this part of the screen to import custom signatures (previously saved to your computer) to the Zyxel Device. Note: 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'.
File Path	Type the file path and name of the custom signature file you want to import in the text box (or click **Browse** to find it on your computer) and then click **Import**ing to transfer the file to the Zyxel Device. New signatures then display in the Zyxel Device **IDP > Custom Signatures** screen.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the IDP signature set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.

Policy Types

This table describes **Policy Types** as categorized in the Zyxel Device.

Table 227 Policy Types

POLICY TYPE	DESCRIPTION
Access Control	Access control refers to procedures and controls that limit or detect access. Access control attacks try to bypass validation checks in order to access network resources such as servers, directories, and files.
Any	Any attack includes all other kinds of attacks that are not specified in the policy such as password, spoof, hijack, phishing, and close-in.
Backdoor/Trojan Horse	A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data. Although a virus, a worm and a Trojan are different types of attacks, they can be blended into one attack. For example, W32/Blaster and W32/Sasser are blended attacks that feature a combination of a worm and a Trojan.

Table 227 Policy Types (continued)

POLICY TYPE	DESCRIPTION
BotNet	A Botnet is a number of Internet computers that have been set up to forward transmissions including spam or viruses to other computers on the Internet though their owners are unaware of it. It is also a collection of Internet-connected programs communicating with other similar programs in order to perform tasks and participate in distributed Denial-Of-Service attacks.
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.
DoS/DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A Distributed Denial of Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Instant Messenger	IM (Instant Messenger) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants.
Mail	A Mail or email bombing attack involves sending several thousand identical messages to an electronic mailbox in order to overflow it, making it unusable.
Misc	Miscellaneous attacks takes advantage of vulnerable computer networks and web servers by forcing cache servers or web browsers into disclosing user-specific information that might be sensitive and confidential. The most common type of Misc. attacks are HTTP Response Smuggling, HTTP Response Splitting and JSON Hijacking.
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the Zyxel Device, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh, etc.
Scan	A scan describes the action of searching a network for an exposed service. An attack may then occur once a vulnerability has been found. Scans occur on several network levels. A network scan occurs at layer-3. For example, an attacker looks for network devices such as a router or server running in an IP network. A scan on a protocol is commonly referred to as a layer-4 scan. For example, once an attacker has found a live end system, he looks for open ports. A scan on a service is commonly referred to a layer-7 scan. For example, once an attacker has found an open port, say port 80 on a server, he determines that it is a HTTP service run by some web server application. He then uses a web vulnerability scanner (for example, Nikto) to look for documented vulnerabilities.
SPAM	Spam is unsolicited “junk” email sent to large numbers of people to promote products or services.
Stream Media	A Stream Media attack occurs when a malicious network node downloads an overwhelming amount of media stream data that could potentially exhaust the entire system. This method allows users to send small requests messages that result in the streaming of large media objects, providing an opportunity for malicious users to exhaust resources in the system with little effort expended on their part.
Tunnel	A Tunneling attack involves sending IPv6 traffic over IPv4, slipping viruses, worms and spyware through the network using secret tunnels. This method infiltrates standard security measures through IPv6 tunnels, passing through IPv4 undetected. An external signal then triggers the malware to spring to life and wreak havoc from inside the network.

Table 227 Policy Types (continued)

POLICY TYPE	DESCRIPTION
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources, thus slowing or stopping other tasks.
Web Attack	Web attacks refer to attacks on web servers such as IIS (Internet Information Services).

IDP Service Groups

An IDP service group is a set of related packet inspection signatures.

Table 228 IDP Service Groups

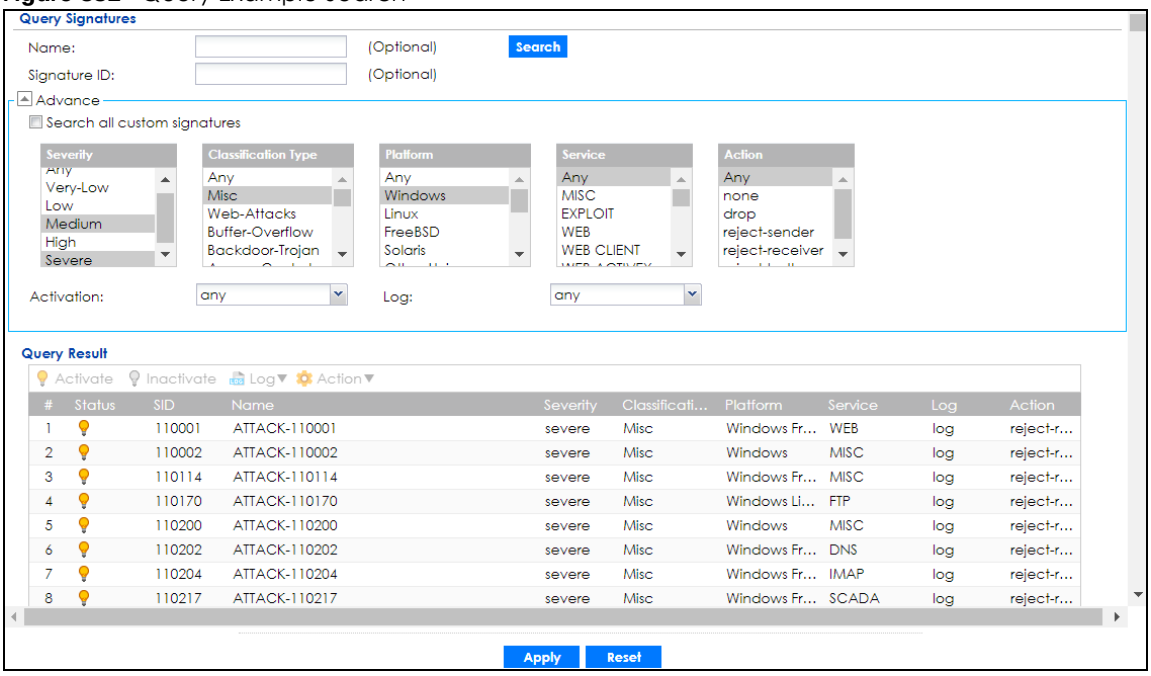
WEB_PHP	WEB_MISC	WEB_IIS	WEB_FRONTPAGE
WEB_CGI	WEB_ATTACKS	TFTP	TELNET
SQL	SNMP	SMTP	RSERVICES
RPC	POP3	POP2	P2P
ORACLE	NNTP	NETBIOS	MYSQL
MISC_EXPLOIT	MISC_DDOS	MISC_BACKDOOR	MISC
IMAP	IM	ICMP	FTP
FINGER	DNS	n/a	

30.2.1 Query Example

This example shows a search with these criteria:

- Severity: Severe
- Classification Type: Misc
- Platform: Windows
- Service: Any
- Actions: Any

Figure 381 Query Example Search



30.3 IDP Custom Signatures

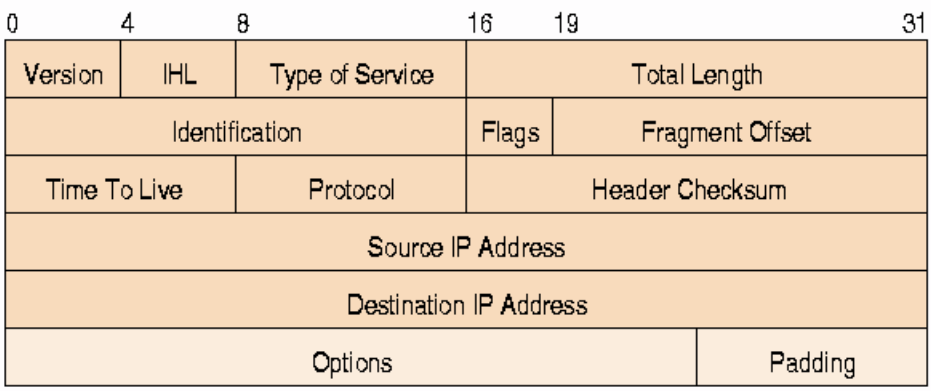
Create custom signatures for new attacks or attacks peculiar to your network. Custom signatures can also be saved to/from your computer so as to share with others.

You need some knowledge of packet headers and attack types to create your own custom signatures.

IP Packet Header

These are the fields in an Internet Protocol (IP) version 4 packet header.

Figure 382 IP v4 Packet Headers



The header fields are discussed in the following table.

Table 229 IP v4 Packet Headers

HEADER	DESCRIPTION
Version	The value 4 indicates IP version 4.
IHL	IP Header Length is the number of 32 bit words forming the total length of the header (usually five).
Type of Service	The Type of Service, (also known as Differentiated Services Code Point (DSCP)) is usually set to 0, but may indicate particular quality of service needs from the network.
Total Length	This is the size of the datagram in bytes. It is the combined length of the header and the data.
Identification	This is a 16-bit number, which together with the source address, uniquely identifies this packet. It is used during reassembly of fragmented datagrams.
Flags	Flags are used to control whether routers are allowed to fragment a packet and to indicate the parts of a packet to the receiver.
Fragment Offset	This is a byte count from the start of the original sent packet.
Time To Live	This is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. It is used to prevent accidental routing loops.
Protocol	The protocol indicates the type of transport packet being carried, for example, 1 = ICMP; 2= IGMP; 6 = TCP; 17= UDP.
Header Checksum	This is used to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check. Packets with an invalid checksum are discarded by all nodes in an IP network.
Source IP Address	This is the IP address of the original sender of the packet.
Destination IP Address	This is the IP address of the final destination of the packet.
Options	IP options is a variable-length list of IP options for a datagram that define IP **Security Option, IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**.
Padding	Padding is used as a filler to ensure that the IP packet is a multiple of 32 bits.

Select **Configuration > Security Service**. The **Custom Signature Rules** section shows a summary of all custom signatures created. Click the **SID** or **Name** heading to sort. Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature. You can also delete custom signatures here or save them to your computer.

Note: 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**.

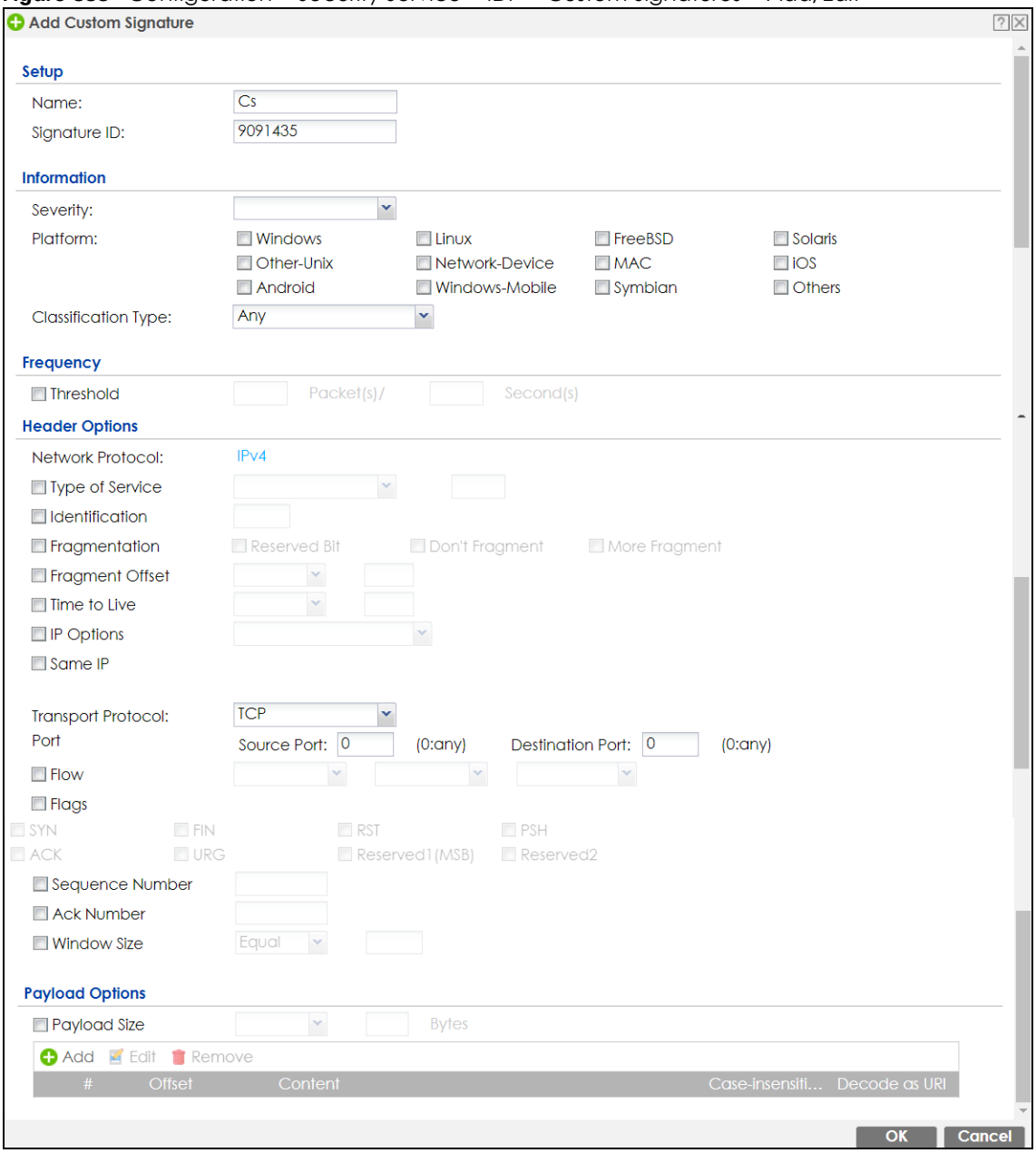
30.3.1 Add / Edit Custom Signatures

Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature in the screen as shown in Figure 380 on page 567.

A packet must match all items you configure in this screen before it matches the signature. The more specific your signature (including packet contents), then the fewer false positives the signature will trigger.

Try to write signatures that target a vulnerability, for example a certain type of traffic on certain operating systems, instead of a specific exploit.

Figure 383 Configuration > Security Service > IDP > Custom Signatures > Add/Edit



The following table describes the fields in this screen.

Table 230 Configuration > Security Service > IDP > Custom Signatures > Add/Edit

LABEL	DESCRIPTION
Name	Type the name of this custom signature. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Duplicate names can exist but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent. Refer to (but do not copy) the packet inspection signature names for hints on creating a naming convention.
Signature ID	A signature ID is automatically created when you click the **Add** icon to create a new signature. You can edit the ID to create a new one (in the 9000000 to 9999999 range), but you cannot use one that already exists. You may want to do that if you want to order custom signatures by SID.
Information	Use the following fields to set general information about the signature as denoted below.
Severity	The severity level denotes how serious the intrusion is. Categorize the seriousness of the intrusion here.
Platform	Some intrusions target specific operating systems only. Select the operating systems that the intrusion targets, that is, the operating systems you want to protect from this intrusion. SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX). A router is an example of a network device.
Classification Type	Categorize the attack type here. See Table 227 on page 569 as a reference.
Frequency	Recurring packets of the same type may indicate an attack. Use the following field to indicate how many packets per how many seconds constitute an intrusion
Threshold	Select **Threshold** and then type how many packets (that meet the criteria in this signature) per how many seconds constitute an intrusion.
Header Options	
Network Protocol	Configure signatures for IP version 4.
Type Of Service	Type of service in an IP header is used to specify levels of speed and/or reliability. Some intrusions use an invalid **Type Of Service** number. Select the check box, then select **Equal** or **Not-Equal** and then type in a number.
Identification	The identification field in a datagram uniquely identifies the datagram. If a datagram is fragmented, it contains a value that identifies the datagram to which the fragment belongs. Some intrusions use an invalid **Identification** number. Select the check box and then type in the invalid number that the intrusion uses.
Fragmentation	A fragmentation flag identifies whether the IP datagram should be fragmented, not fragmented or is a reserved bit. Some intrusions can be identified by this flag. Select the check box and then select the flag that the intrusion uses.
Fragment Offset	When an IP datagram is fragmented, it is reassembled at the final destination. The fragmentation offset identifies where the fragment belongs in a set of fragments. Some intrusions use an invalid **Fragment Offset** number. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number
Time to Live	Time to Live is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. Usually it's used to set an upper limit on the number of routers a datagram can pass through. Some intrusions can be identified by the number in this field. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number.

Table 230 Configuration > Security Service > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
IP Options	IP options is a variable-length list of IP options for a datagram that define IP **Security Option, IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**. **IP Options** can help identify some intrusions. Select the check box, then select an item from the list box that the intrusion uses
Same IP	Select the check box for the signature to check for packets that have the same source and destination IP addresses.
Transport Protocol	The following fields vary depending on whether you choose **TCP**, **UDP** or **ICMP**.
Transport Protocol: TCP	
Port	Select the check box and then enter the source and destination TCP port numbers that will trigger this signature.
Flow	The selected keyword sets the criteria as to which traffic is matched. You can match traffic based on direction or whether the connection is established or not. You can also specify whether you want to match signatures per packet or in a stream of packets. **Established**: Match established connections. **Stateless**: Match packets that are not part of an established connection. **To Client**: Match packets that flow from server to client.. **To Server**: Match packets that flow from client to server. **From Client**: Match packets that flow from client to server. **From Servers**: Match packets that flow from server to client. **No Stream**: Match packets that have not been reassembled by the stream engine. It will not match packets that have been reassembled. **Only Stream**: Match packets that have been reassembled.
Flags	Select what TCP flag bits the signature should check.
Sequence Number	Use this field to check for a specific TCP sequence number.
Ack Number	Use this field to check for a specific TCP acknowledgment number.
Window Size	Use this field to check for a specific TCP window size.
Transport Protocol: UDP	
Port	Select the check box and then enter the source and destination UDP port numbers that will trigger this signature.
Transport Protocol: ICMP	
Type	Use this field to check for a specific ICMP type value.
Code	Use this field to check for a specific ICMP code value.
ID	Use this field to check for a specific ICMP ID value. This is useful for covert channel programs that use static ICMP fields when they communicate.
Sequence Number	Use this field to check for a specific ICMP sequence number. This is useful for covert channel programs that use static ICMP fields when they communicate.
Payload Options	The longer a payload option is, the more exact the match, the faster the signature processing. Therefore, if possible, it is recommended to have at least one payload option in your signature.

Table 230 Configuration > Security Service > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
Payload Size	This field may be used to check for abnormally sized packets or for detecting buffer overflows. Select the check box, then select **Equal**, **Smaller** or **Greater** and then type the payload size. Stream rebuilt packets are not checked regardless of the size of the payload.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Offset	This field specifies where to start searching for a pattern within a packet. For example, an offset of 5 would start looking for the specified pattern after the first five bytes of the payload.
Content	Type the content that the signature should search for in the packet payload. Hexadecimal code entered between pipes is converted to ASCII. For example, you could represent the ampersand as either & or |26| (26 is the hexadecimal code for the ampersand).
Case-insensitive	Select **Yes** if content casing does NOT matter.
Decode as URI	A Uniform Resource Identifier (URI) is a string of characters for identifying an abstract or physical resource (RFC 2396). A resource can be anything that has identity, for example, an electronic document, an image, a service ("today's weather report for Taiwan"), a collection of other resources. An identifier is an object that can act as a reference to something that has identity. Example URIs are: ftp://ftp.is.co.za/rfc/rfc1808.txt; ftp scheme for File Transfer Protocol services http://www.math.uio.no/faq/compression-faq/part1.html; http scheme for Hypertext Transfer Protocol services mailto:mduerst@ifi.unizh.ch; mailto scheme for electronic mail addresses telnet://melvyl.ucop.edu/; telnet scheme for interactive services via the TELNET Protocol Select **Yes** for the signature to search for normalized URI fields. This means that if you are writing signatures that includes normalized content, such as %2 for directory traversals, these signatures will not be triggered because the content is normalized out of the URI buffer. For example, the URI: /scripts/..%c0%af../winnt/system32/cmd.exe?/c+ver will get normalized into: /winnt/system32/cmd.exe?/c+ver
OK	Click this button to save your changes to the Zyxel Device and return to the summary screen.
Cancel	Click this button to return to the summary screen without saving any changes.

30.3.2 Custom Signature Example

Before creating a custom signature, you must first clearly understand the vulnerability.

30.3.2.1 Understand the Vulnerability

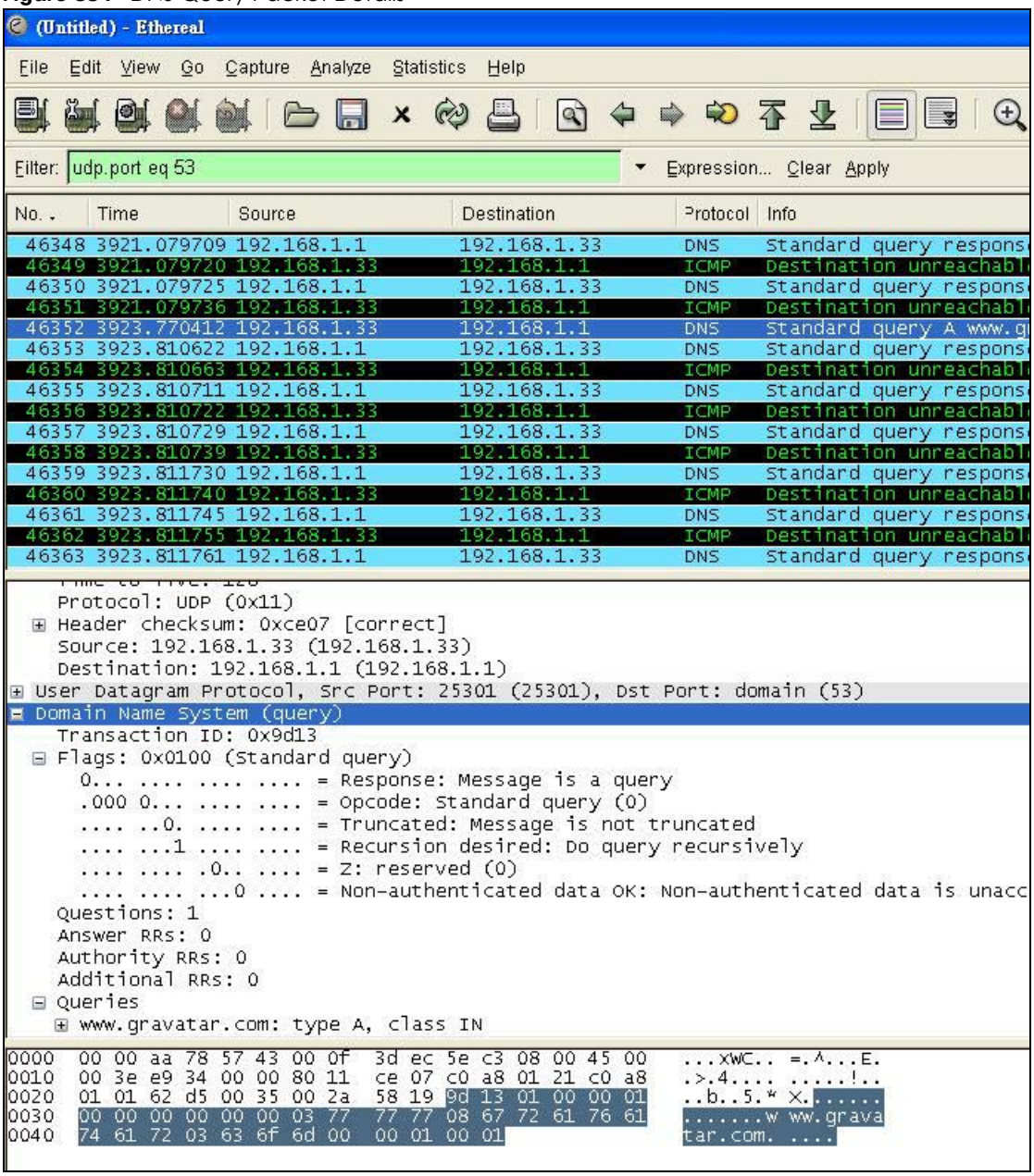
Check the Zyxel Device logs when the attack occurs. Use web sites such as Google or Security Focus to get as much information about the attack as you can. The more specific your signature, the less chance it will cause false positives.

As an example, say you want to check if your router is being overloaded with DNS queries so you create a signature to detect DNS query traffic.

30.3.2.2 Analyze Packets

Use the packet capture screen and a packet analyzer (also known as a network or protocol analyzer) such as Wireshark or Ethereal to investigate some more.

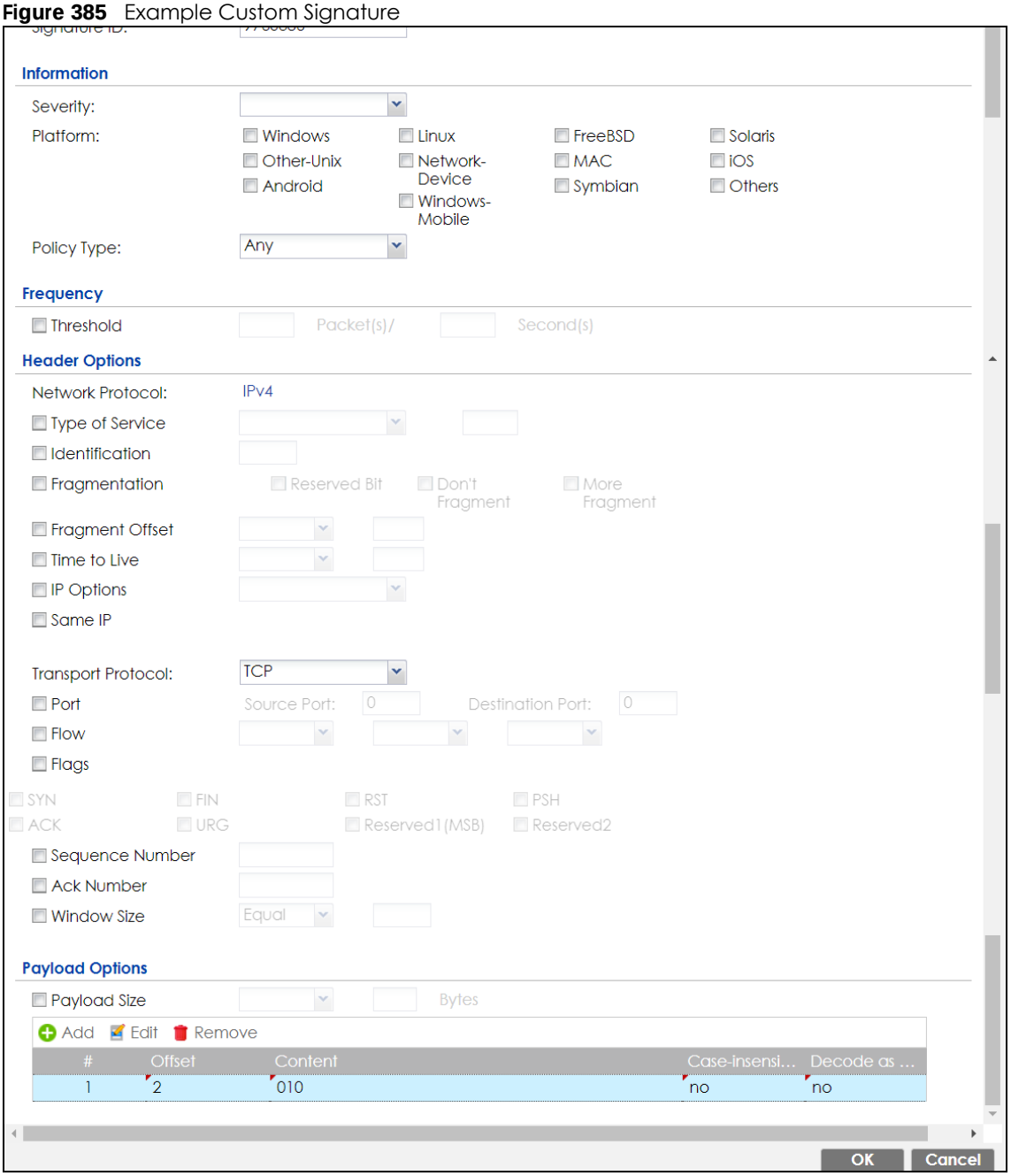
Figure 384 DNS Query Packet Details



From the details about DNS query you see that the protocol is UDP and the port is 53. The type of DNS packet is standard query and the Flag is 0x0100 with an offset of 2. Therefore enter |010| as the first pattern.

The final custom signature should look like as shown in the following figure.

Figure 385 Example Custom Signature



30.3.3 Applying Custom Signatures

After you create your custom signature, it becomes available in an IDP profile (**Configuration > Security Service > IDP > Profile > Edit** screen). Custom signatures have an SID from 9000000 to 9999999.

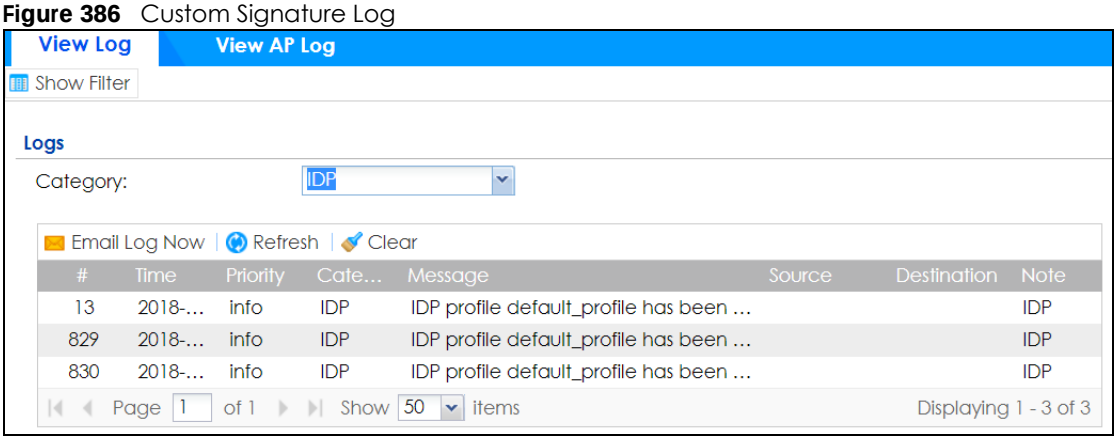
Search for, then activate the signature, configure what action to take when a packet matches it and if it should generate a log or alert in a profile. Then bind the profile to a zone.

30.3.4 Verifying Custom Signatures

Configure the signature to create a log when traffic matches the signature. (You may also want to configure an alert if it is for a serious attack and needs immediate attention.) After you apply the signature to a zone, you can see if it works by checking the logs (**Monitor > Log**).

The **Priority** column shows **warn** for signatures that are configured to generate a log only. It shows **critical** for signatures that are configured to generate a log and alert. All IDP signatures come under the **IDP** category. The **Note** column displays **ACCESS FORWARD** when no action is configured for the signature. It displays **ACCESS DENIED** if you configure the signature action to drop the packet. The destination port is the service port (53 for DNS in this case) that the attack tries to exploit.

Figure 386 Custom Signature Log

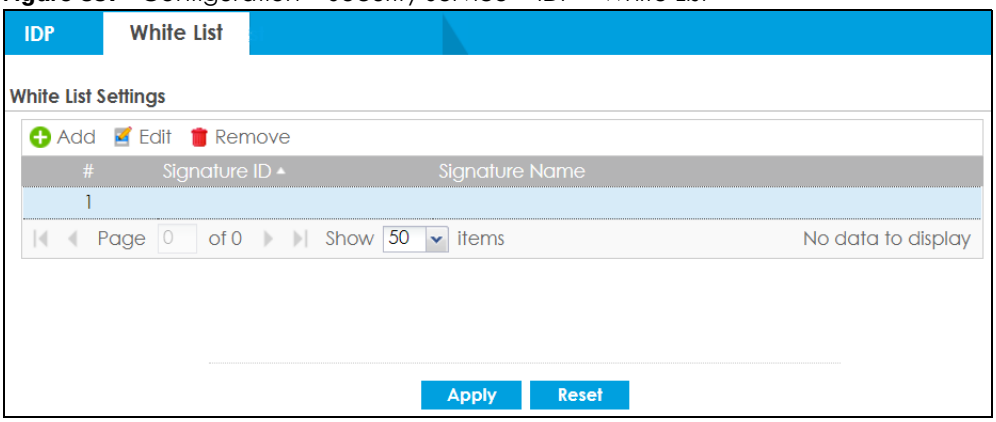


30.4 The White List Screen

Use this screen to view the IDP white list. The Zyxel Device will exclude the incoming packets of the listed signature(s), and these packets won't be intercepted and will be passed through uninspected.

Click **Configuration > Security Service > IDP > White List** to display the following screen. Use **Add** to put a new item in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 387 Configuration > Security Service > IDP > White List



The following table describes the fields in this screen.

Table 231 Configuration > Security Service > IDP > White List

LABEL	DESCRIPTION
White List Settings	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Signature ID	This field displays the signature ID of this entry.
Signature Name	This field displays the signature name of this entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

30.5 IDP Technical Reference

This section contains some background information on IDP.

Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical "network-based intrusions" are SQL slammer, Blaster, Nimda MyDoom etc.

Snort Signatures

You may want to refer to open source Snort signatures when creating custom Zyxel Device ones. Most Snort rules are written in a single line. Snort rules are divided into two logical sections, the rule header and the rule options as shown in the following example:

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 a5|"; msg:"mountd access";)
```

The text up to the first parenthesis is the rule header and the section enclosed in parenthesis contains the rule options. The words before the colons in the rule options section are the option keywords.

The rule header contains the rule's:

- Action
- Protocol
- Source and destination IP addresses and netmasks
- Source and destination ports information.

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

These are some equivalent Snort terms in the Zyxel Device.

Table 232 Zyxel Device - Snort Equivalent Terms

ZYXEL DEVICE TERM	SNORT EQUIVALENT TERM
Type Of Service	tos
Identification	id
Fragmentation	fragbits
Fragmentation Offset	fragoffset
Time to Live	ttl
IP Options	ipopts
Same IP	sameip
Transport Protocol	
Transport Protocol: TCP	
Port	(In Snort rule header)
Flow	flow
Flags	flags
Sequence Number	seq
Ack Number	ack
Window Size	window

Table 232 Zyxel Device - Snort Equivalent Terms (continued)

ZYXEL DEVICE TERM	SNORT EQUIVALENT TERM
Transport Protocol: UDP	(In Snort rule header)
Port	(In Snort rule header)
Transport Protocol: ICMP	
Type	itype
Code	icode
ID	icmp_id
Sequence Number	icmp_seq
Payload Options	(Snort rule options)
Payload Size	dsize
Offset (relative to start of payload)	offset
Relative to end of last match	distance
Content	content
Case-insensitive	nocase
Decode as URI	uricontent

Note: Not all Snort functionality is supported in the Zyxel Device.

CHAPTER 31
Sandboxing

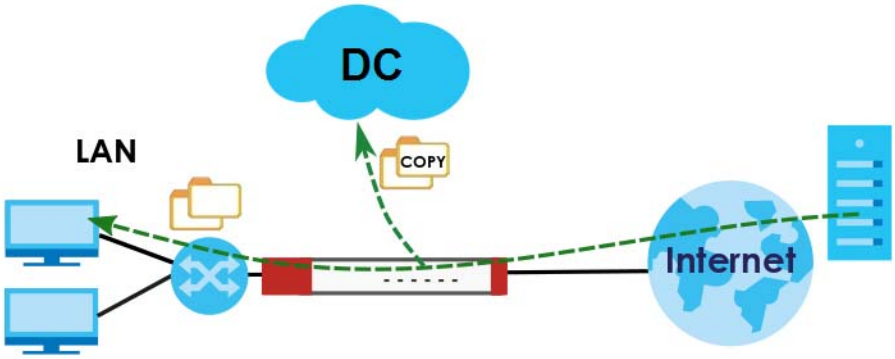
31.1 Overview

Zyxel cloud sandboxing is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs/codes are uploaded to the Defend Center and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Zyxel Device's detection, such as anti-malware. Results of cloud sandboxing are sent from the server to the Zyxel Device.

By default, the Zyxel Device sandbox forwards all unknown files and uploads a copy of the files for inspection after checking the received files against its local cache. The scan result from the Defend Center (**DC**) is added to the Zyxel Device cache and used for future inspection. When a file with malicious or suspicious codes is detected, the Zyxel Device can take specific actions on the threats.

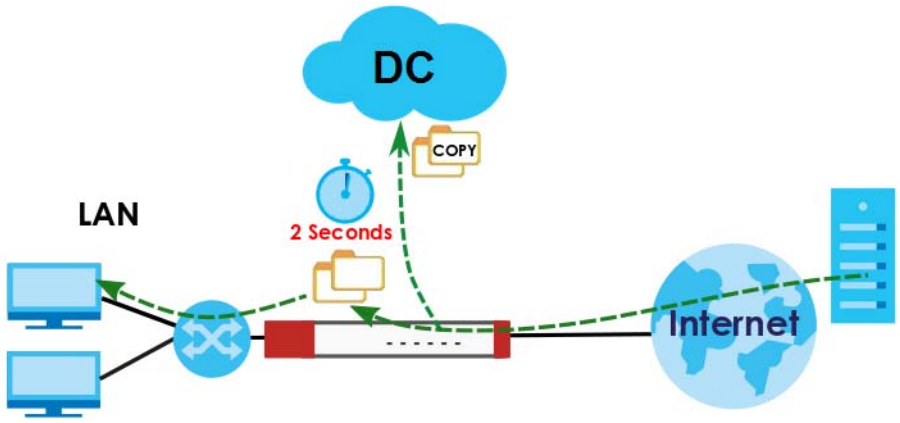
Note: The scan result will be removed from the Zyxel Device cache after the Zyxel Device restarts.

Figure 388 General Zyxel Sandbox Inspection



Alternatively, you can select to hold and inspect the downloaded files for up to two seconds if the downloaded files have never been inspected before.

Figure 389 Advanced Zyxel Sandbox Inspection



31.1.1 What You Need to Know

The Zyxel Device may forward files with attachments before Sandbox has completed checking. If Sandbox discovers a suspect file, please contact the receiver of the suspect file and advise him/her not to open it. If he/she already opened it, then please urge him/her to run an up-to-date anti-malware scanner.

If the receiver of a suspect file cannot open a file, Sandbox may have already modified the file by deleting the infected portion. Please check the logs and let the receiver know if this is so.

Sandbox can only check the types of files listed under **File Submission Options** in the **Sandboxing** screen. If you disabled **Scan and detect EICAR test virus** in the **Anti-Malware** screen, then EICAR test files will be sent to Sandbox.

To use the sandbox, you need to register your Zyxel Device and activate the service license at myZyxel, and then turn on the sandboxing function on the Zyxel Device. See Chapter 7 on page 186 for more information about registration and service licenses.

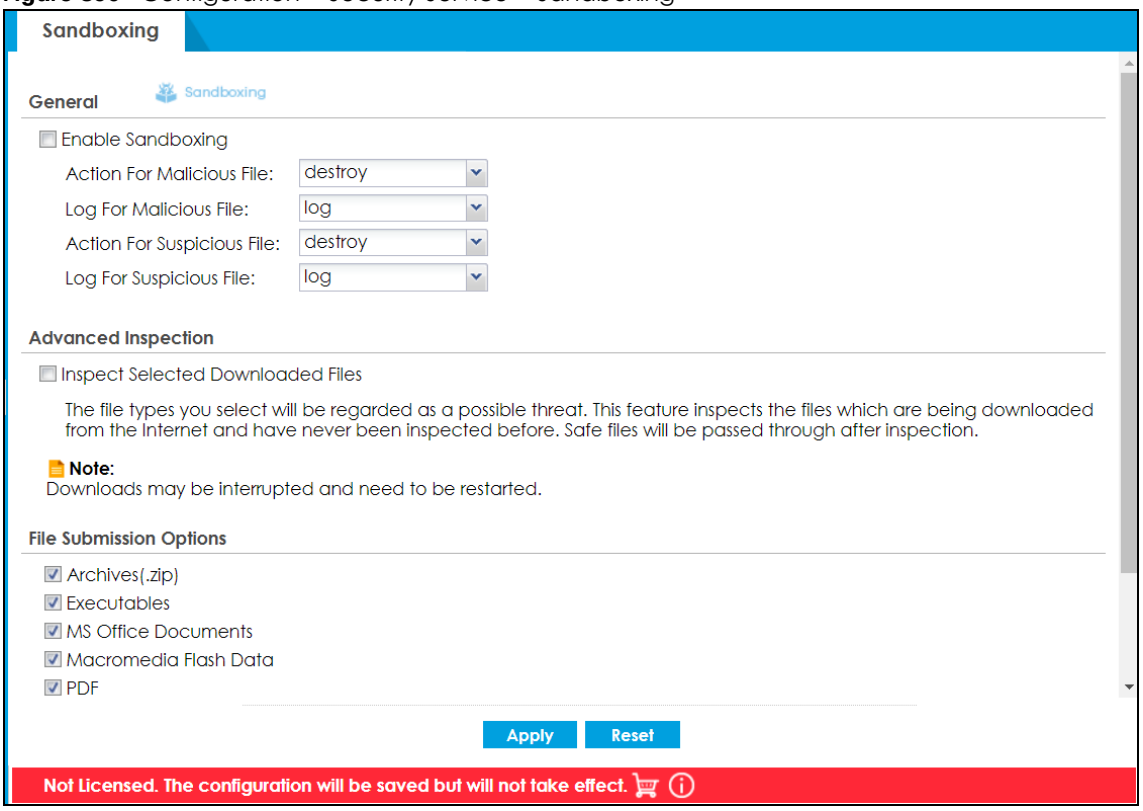
31.2 Sandboxing Screen

Click **Configuration > Security Service** > **Sandboxing** to display the configuration screen as shown next.

Use this screen to enable sandboxing and specify the actions the Zyxel Device takes when malicious or suspicious files are detected.

Click the **Sandboxing** icon for more information on the Zyxel Device's security features.

Figure 390 Configuration > Security Service > Sandboxing



The following table describes the labels in this screen.

Table 233 Configuration > Security Service > Sandboxing

LABEL	DESCRIPTION
General	
Enable Sandboxing	Select this option to turn on sandboxing on the Zyxel Device. Otherwise, deselect it.
Action For Malicious File	Specify whether the Zyxel Device deletes (**destroy**) or forwards (**allow**) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.
Log For Malicious File	These are the log options for malicious files: **no**: Do not create a log when a malicious file is detected. **log**: Create a log on the Zyxel Device when a malicious file is detected. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a malicious file is detected.
Action For Suspicious File	Specify whether the Zyxel Device deletes (**destroy**) or forwards (**allow**) suspicious files. Suspicious files are files given a medium score for malware characteristics by the Defend Center.
Log For Suspicious File	These are the log options for suspicious files: **no**: Do not create a log when a suspicious file is detected. **log**: Create a log on the Zyxel Device when a suspicious file is detected. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a suspicious file is detected.

Table 233 Configuration > Security Service > Sandboxing (continued)

LABEL	DESCRIPTION
Advanced Inspection	
Inspect Selected Downloaded Files	Select the check box to have the Zyxel Device hold the downloaded file for up to two seconds if the downloaded file has never been inspected before. The Zyxel Device will wait for the Defend Center's result and forward the file in two seconds. Sandbox detection may take longer than two seconds, so infected files could still possibly be forwarded to the user. Note: The Zyxel Device only checks the file types you selected for sandbox inspection. The scan result will be removed from the Zyxel Device cache after the Zyxel Device restarts.
File Submission Options	Specify the type of files to be sent for sandbox inspection.
Terms of Use	Click this link to see what data Zyxel collects from you and how it is used.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 32
Email Security

32.1 Overview

The email security feature can mark or discard spam (unsolicited commercial or junk email). Use the white list to identify legitimate email. Use the black list to identify spam email. The Zyxel Device can also check email against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

32.1.1 What You Can Do in this Chapter

- Use the **Email Security** screens (Section 32.3 on page 590) to turn email security on or off and manage email security policies. Also, you can enable and configure the mail scan functions and have the Zyxel Device check email against DNS Black Lists.
- Use the **Black/White List** screens (Section 32.4 on page 593) to set up a black list to identify spam and a white list to identify legitimate email.

32.1.2 What You Need to Know

White List

Configure white list entries to identify legitimate email. The white list entries have the Zyxel Device classify any email that is from a specified sender or uses a specified header field and header value as being legitimate (see Email Headers for more on mail headers). The email security feature checks an email against the white list entries before doing any other email security checking. If the email matches a white list entry, the Zyxel Device classifies the email as legitimate and does not perform any more email security checking on that individual email. A properly configured white list helps keep important email from being incorrectly classified as spam. The white list can also increases the Zyxel Device's email security speed and efficiency by not having the Zyxel Device perform the full email security checking process on legitimate email.

Black List

Configure black list entries to identify spam. The black list entries have the Zyxel Device classify any email that is from or forwarded by a specified IP address or uses a specified header field and header value as being spam. If an email does not match any of the white list entries, the Zyxel Device checks it against the black list entries. The Zyxel Device classifies an email that matches a black list entry as spam and immediately takes the configured action for dealing with spam. If an email matches a blacklist entry, the Zyxel Device does not perform any more email security checking on that individual email. A properly configured black list helps catch spam email and increases the Zyxel Device's email security speed and efficiency.

SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of email messages between servers. Email clients (also called email applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve email. Email clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many email applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The Zyxel Device's email security feature checks SMTP (TCP port 25) and POP3 (TCP port 110) emails by default. You can also specify custom SMTP and POP3 ports for the Zyxel Device to check.

Email Headers

Every email has a header and a body. The header is structured into fields and includes the addresses of the recipient and sender, the subject, and other information about the email and its journey. The body is the actual message text and any attachments. You can have the Zyxel Device check for specific header fields with specific values.

Email programs usually only show you the To:, From:, Subject:, and Date: header fields but there are others such as Received: and Content-Type:. To see all of an email's header, you can select an email in your email program and look at its properties or details. For example, in Microsoft's Outlook Express, select a mail and click **File > Properties > Details**. This displays the email's header. Click **Message Source** to see the source for the entire mail including both the header and the body.

Email Header Buffer Size

The Zyxel Device has a 5 K buffer for an individual email header. If an email's header is longer than 5 K, the Zyxel Device only checks up to the first 5 K.

DNSBL

A DNS Black List (DNSBL) is a server that hosts a list of IP addresses known or suspected of having sent or forwarded spam. A DNSBL is also known as a DNS spam blocking list. The Zyxel Device can check the routing addresses of email against DNSBLs and classify an email as spam if it was sent or forwarded by a computer with an IP address in the DNSBL.

Finding Out More

See Section 32.5 on page 595 for more background information on email security.

32.2 Before You Begin

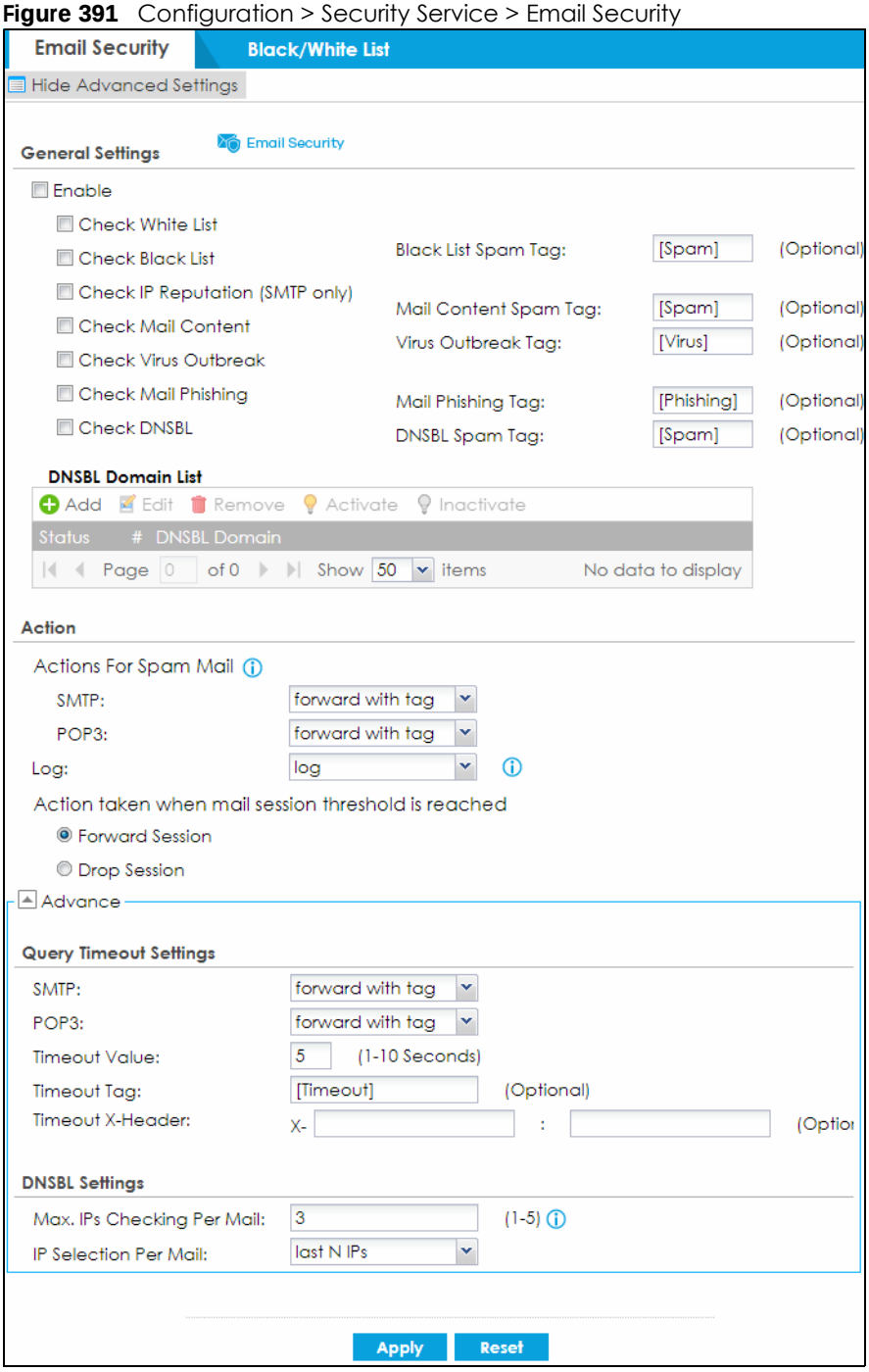
- Before using the email security features (IP Reputation, Mail Content Analysis and Virus Outbreak Detection) you must activate your email security Service license.
- Configure your zones before you configure email security.

32.3 The Email Security Screen

Click **Configuration > Security Service** > **Email Security** to open the **Email Security** screen. Use this screen to turn the email security feature on or off and manage email security policies. You can also select the action the Zyxel Device takes when the mail sessions threshold is reached.

Click the **Email Security** icon for more information on the Zyxel Device's security features.

Figure 391 Configuration > Security Service > Email Security



The following table describes the labels in this screen.

Table 234 Configuration > Security Service > Email Security

LABEL	DESCRIPTION
General Settings	
Enable	Select this check box to activate the settings in this section.
Check White List	Select this check box to check email against the white list. The Zyxel Device classifies email that matches a white list entry as legitimate (not spam).
Check Black List	Select this check box to check email against the black list. The Zyxel Device classifies email that matches a black list entry as spam.
Black List Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of emails that match the Zyxel Device's spam black list.
Check IP Reputation (SMTP Only)	Select this to use IP reputation to identify Spam or Unwanted Bulk Email by the sender's IP address.
Check Mail Content	Select this to identify spam email by content, such as malicious content.
Mail Content Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of emails that are determined to spam based on the mail content analysis. This tag is only added if the email security policy is configured to forward spam mail with a spam tag.
Check Virus Outbreak	Select this to scan emails for attached viruses.
Virus Outbreak Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of emails that are determined to have an attached viruses. This tag is only added if the email security policy is configured to forward spam mail with a spam tag.
Check Mail Phishing	Phishing is an act of tricking you into providing login or personal information with malicious emails or website links. Select this to identify emails sent from suspicious websites known for phishing.
Mail Phishing Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of emails that have suspicious websites links. This tag is only added if the email security action is configured to forward spam mail with a spam tag.
Check DNSBL	Select this check box to check email against the Zyxel Device's configured DNSBL domains. The Zyxel Device classifies email that matches a DNS black list as spam.
DNSBL Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of emails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the Zyxel Device. This tag is only added if the email security policy is configured to forward spam mail with a spam tag.
DNSBL Domain List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.

Table 234 Configuration > Security Service > Email Security

LABEL	DESCRIPTION
DNSBL Domain	This is the name of a domain that maintains DNSBL servers. Enter the domain that is maintaining a DNSBL.
Actions for Spam Mail	Use this section to set how the Zyxel Device is to handle spam mail.
SMTP	Select how the Zyxel Device is to handle spam SMTP mail. Select **drop** to discard spam SMTP mail. Select **forward** to allow spam SMTP mail to go through. Select **forward with tag** to add a spam tag to an SMTP spam mail's mail subject and send it on to the destination.
POP3	Select how the Zyxel Device is to handle spam POP3 mail. Select **forward** to allow spam POP3 mail to go through. Select **forward with tag** to add a spam tag to an POP3 spam mail's mail subject and send it on to the destination.
Log	Select whether to have the ZyXEL device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in this category.
Action taken when mail sessions threshold is reached	An email session is when an email client and email server (or two email servers) connect through the Zyxel Device. Select how to handle concurrent email sessions that exceed the maximum number of concurrent email sessions that the email security feature can handle. See the chapter of product specifications for the threshold. Select **Forward Session** to have the Zyxel Device allow the excess email sessions without any spam filtering. Select **Drop Session** to have the Zyxel Device drop mail connections to stop the excess email sessions. The email client or server will have to re-attempt to send or receive email later when the number of email sessions is under the threshold.
Query Timeout Settings	
SMTP	Select how the Zyxel Device is to handle SMTP mail query timeout. Select **drop** to discard SMTP mail. Select **forward** to allow SMTP mail to go through. Select **forward with tag** to add a tag to an SMTP query timeout mail's mail subject and send it on to the destination.
POP3	Select how the Zyxel Device is to handle POP3 mail query timeout. Select **forward** to allow POP3 mail to go through. Select **forward with tag** to add a tag to an POP3 query timeout mail's mail subject and send it on to the destination.
Timeout Value	Set how long the Zyxel Device waits for a reply from the mail scan server. If there is no reply before this time period expires, the Zyxel Device takes the action defined in the relevant **Actions when Query Timeout** field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of emails that the Zyxel Device forwards if queries to the mail scan servers time out.
Timeout X-Header	Specify the name and value for the X-Header to be added when queries to the mail scan servers time out.
Max. IPs Checking Per Mail	Set the maximum number of sender and relay server IP addresses in the mail header to check against the DNSBL domain servers.

Table 234 Configuration > Security Service > Email Security

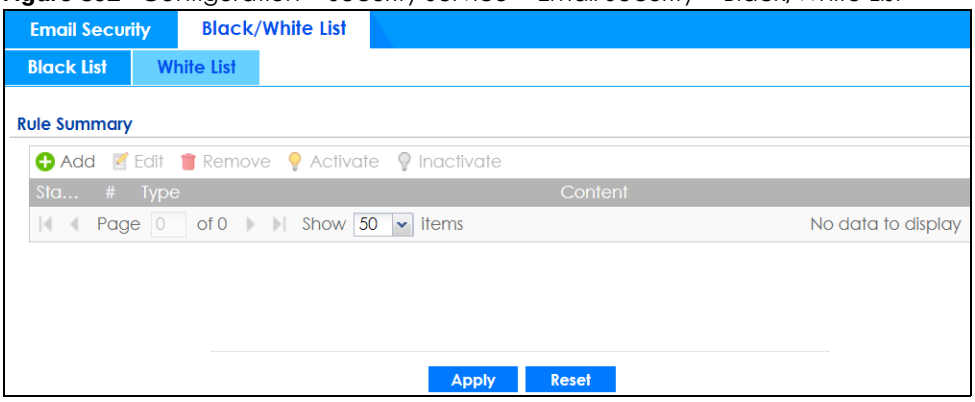
LABEL	DESCRIPTION
IP Selection Per Mail	Select **first N IPs** to have the Zyxel Device start checking from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail. Select **last N IPs** to have the Zyxel Device start checking from the last IP address in the mail header. This is the IP of the last server that forwarded the mail.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

32.4 The Black List / White List Screen

Click **Configuration > Security Service** > **Email Security > Black /White List** to display the **Black List / White List** screen.

Configure the black list to identify spam email. You can create black list entries based on the sender's or relay server's IP address or email address. You can also create entries that check for particular email header fields with specific values or specific subject text. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 392 Configuration > Security Service > Email Security > Black/White List



The following table describes the labels in this screen.

Table 235 Configuration > Security Service > Email Security > Black/White List

LABEL	DESCRIPTION
Rule Summary	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the email's subject, source or relay IP address, source email address, or header.

Table 235 Configuration > Security Service > Email Security > Black/White List (continued)

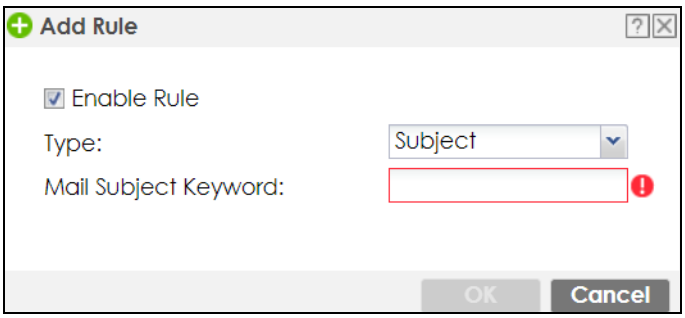
LABEL	DESCRIPTION
Content	This field displays the subject content, source or relay IP address, source email address, or header value for which the entry checks.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

32.4.1 The Black or White List Add/Edit Screen

In the **Black List** or **White List** screen, click the **Add** icon or an **Edit** icon to display the following screen.

Use this screen to configure an email security black list entry to identify spam email. You can create entries based on specific subject text, or the sender's or relay's IP address or email address. You can also create entries that check for particular header fields and values.

Figure 393 Configuration > Security Service > Email Security > Black/White List > Black List (or White List) > Add



The following table describes the labels in this screen.

Table 236 Configuration > Security Service > Email Security > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Enable Rule	Select this to have the Zyxel Device use this entry as part of the black or white list. To actually use the entry, you must also turn on the use of the list in the corresponding list screen, enable the email security feature in the email security general screen, and configure an email security policy to use the list.
Type	Use this field to base the entry on the email's subject, source or relay IP address, source email address, or header. Select **Subject** to have the Zyxel Device check email for specific content in the subject line. Select **IP Address** to have the Zyxel Device check email for a specific source or relay IP address. Select **IPv6 Address** to have the Zyxel Device check email for a specific source or relay IPv6 address. Select **E-Mail Address** to have the Zyxel Device check email for a specific source email address or domain name. Select **Mail Header** to have the Zyxel Device check email for specific header fields and values. Configure black list header entries to check for email from bulk mail programs or with content commonly used in spam. Configure white list header entries to allow certain header values that identify the email as being from a trusted source.

Table 236 Configuration > Security Service > Email Security > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Mail Subject Keyword	This field displays when you select the **Subject** type. Enter up to 63 ASCII characters of text to check for in email headers. Spaces are not allowed, although you could substitute a question mark (?). See Section 32.4.2 on page 595 for more details.
Sender or Mail Relay IP Address	This field displays when you select the **IP Address** type. Enter an IP address in dotted decimal notation.
Sender or Mail Relay IPv6 Address	This field displays when you select the **IPv6 Address** type. Enter an IPv6 address with prefix.
Netmask	This field displays when you select the **IP** type. Enter the subnet mask here, if applicable.
Sender E-Mail Address	This field displays when you select the **E-Mail** type. Enter a keyword (up to 63 ASCII characters). See Section 32.4.2 on page 595 for more details.
Mail Header Field Name	This field displays when you select the **Mail Header** type. Type the name part of an email header (the part that comes before the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter "Received" here.
Field Value Keyword	This field displays when you select the **Mail Header** type. Type the value part of an email header (the part that comes after the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter the mail server's domain here. See Section 32.4.2 on page 595 for more details.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

32.4.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an email subject, email address, or email header value.

- Use a question mark (?) to let a single character vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any email address that ends in def.com matches. So "mail.def.com" matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The Zyxel Device checks the first header with the name you specified in the entry. So if the email has more than one "Received" header, the Zyxel Device checks the first one.

32.5 Email Security Technical Reference

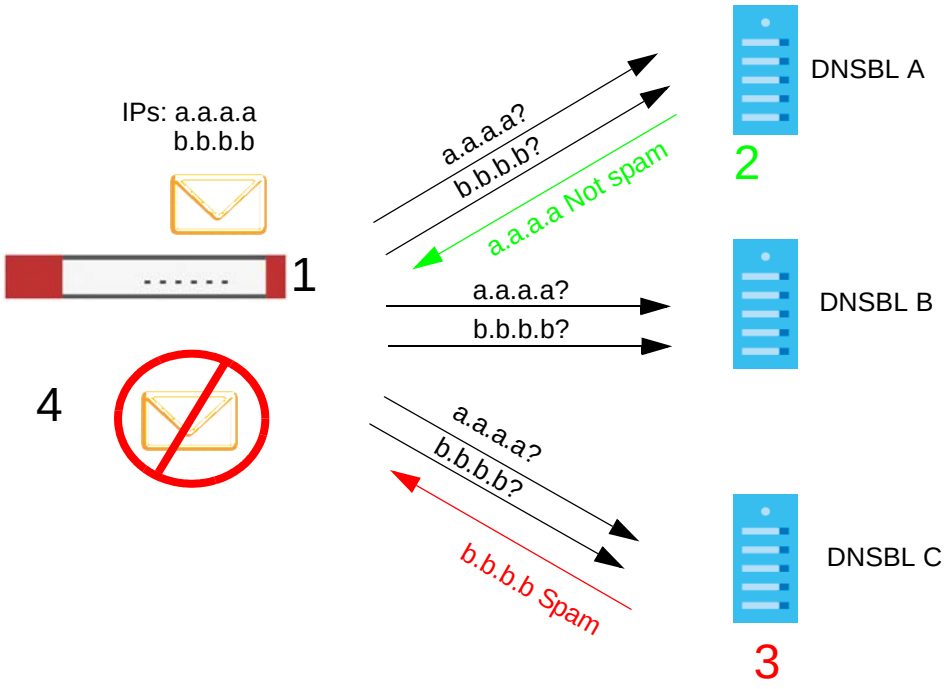
Here is more detailed email security information.

DNSBL

- The Zyxel Device checks only public sender and relay IP addresses, it does not check private IP addresses.
- The Zyxel Device sends a separate query (DNS lookup) for each sender or relay IP address in the email's header to each of the Zyxel Device's DNSBL domains at the same time.
- The DNSBL servers send replies as to whether or not each IP address matches an entry in their list. Each IP address has a separate reply.
- As long as the replies are indicating the IP addresses do not match entries on the DNSBL lists, the Zyxel Device waits until it receives at least one reply for each IP address.
- If the Zyxel Device receives a DNSBL reply that one of the IP addresses is in the DNSBL list, the Zyxel Device immediately classifies the email as spam and takes the email security policy's configured action for spam. The Zyxel Device does not wait for any more DNSBL replies.
- If the Zyxel Device receives at least one non-spam reply for each of an email's routing IP addresses, the Zyxel Device immediately classifies the email as legitimate and forwards it.
- Any further DNSBL replies that come after the Zyxel Device classifies an email as spam or legitimate have no effect.
- The Zyxel Device records DNSBL responses for IP addresses in a cache for up to 72 hours. The Zyxel Device checks an email's sender and relay IP addresses against the cache first and only sends DNSBL queries for IP addresses that are not in the cache.

Here is an example of an email classified as spam based on DNSBL replies.

Figure 394 DNSBL Spam Detection Example



1 The Zyxel Device receives an email that was sent from IP address a.a.a.a and relayed by an email server at IP address b.b.b.b. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address a.a.a.a. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address b.b.b.b.

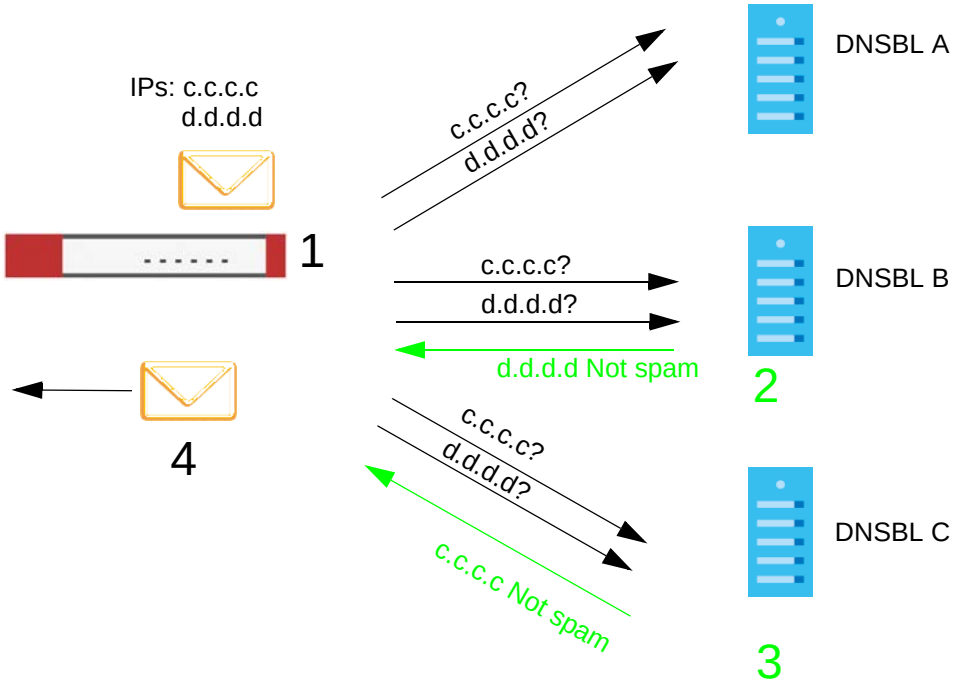
2 DNSBL A replies that IP address a.a.a.a does not match any entries in its list (not spam).

3 DNSBL C replies that IP address b.b.b.b matches an entry in its list.

4 The Zyxel Device immediately classifies the email as spam and takes the action for spam that you defined in the email security policy. In this example it was an SMTP mail and the defined action was to drop the mail. The Zyxel Device does not wait for any more DNSBL replies.

Here is an example of an email classified as legitimate based on DNSBL replies.

Figure 395 DNSBL Legitimate Email Detection Example



1 The Zyxel Device receives an email that was sent from IP address c.c.c.c and relayed by an email server at IP address d.d.d.d. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address c.c.c.c. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address d.d.d.d.

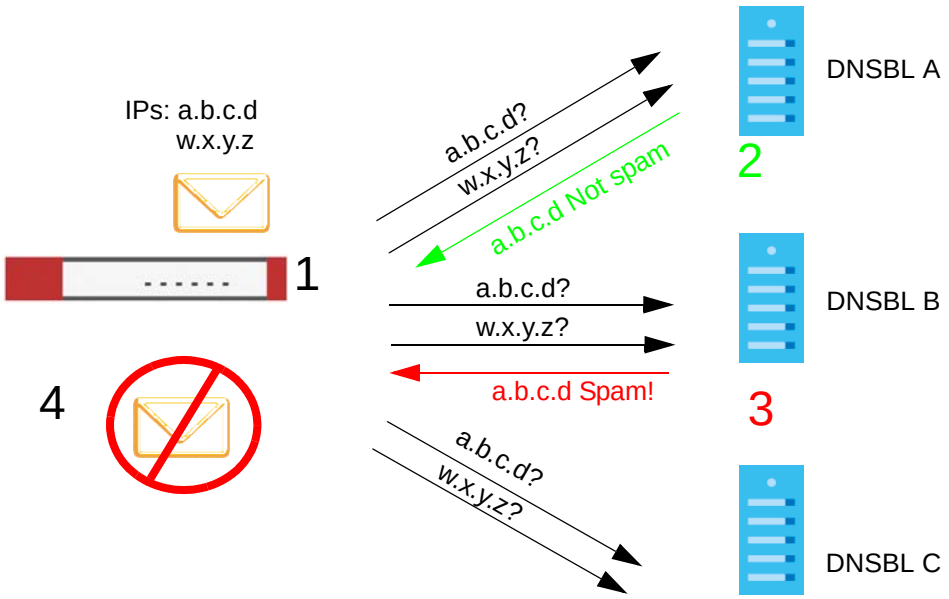
2 DNSBL B replies that IP address d.d.d.d does not match any entries in its list (not spam).

3 DNSBL C replies that IP address c.c.c.c does not match any entries in its list (not spam).

4 Now that the Zyxel Device has received at least one non-spam reply for each of the email's routing IP addresses, the Zyxel Device immediately classifies the email as legitimate and forwards it. The Zyxel Device does not wait for any more DNSBL replies.

If the Zyxel Device receives conflicting DNSBL replies for an email routing IP address, the Zyxel Device classifies the email as spam. Here is an example.

Figure 396 Conflicting DNSBL Replies Example



1 The Zyxel Device receives an email that was sent from IP address a.b.c.d and relayed by an email server at IP address w.x.y.z. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address a.b.c.d. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address w.x.y.z.

2 DNSBL A replies that IP address a.b.c.d does not match any entries in its list (not spam).

3 While waiting for a DNSBL reply about IP address w.x.y.z, the Zyxel Device receives a reply from DNSBL B saying IP address a.b.c.d is in its list.

4 The Zyxel Device immediately classifies the email as spam and takes the action for spam that you defined in the email security policy. In this example it was an SMTP mail and the defined action was to drop the mail. The Zyxel Device does not wait for any more DNSBL replies.

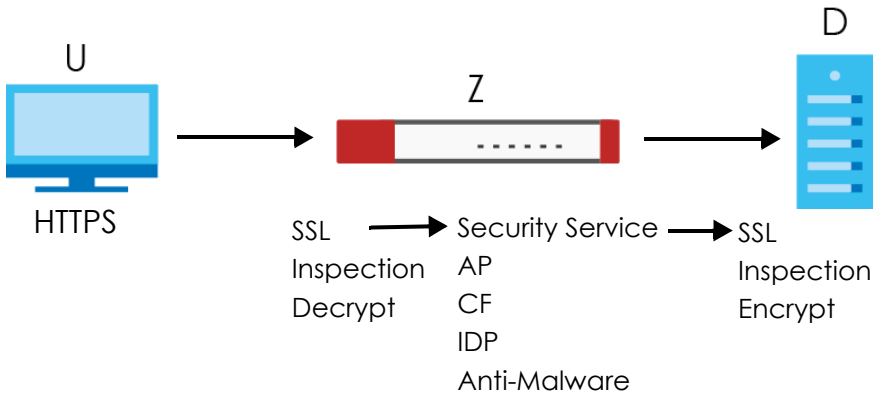
CHAPTER 33
SSL Inspection

33.1 Overview

Secure Socket Layer (SSL) traffic, such as https://www.google.com/HTTPS, FTPs, POP3s, SMTPs, etc. is encrypted, and cannot be inspected using Security Service profiles such as App Patrol, Content Filter, Intrusion, Detection and Prevention (IDP), or Anti-Malware. The Zyxel Device uses SSL Inspection to decrypt SSL traffic, sends it to the Security Service engines for inspection, then encrypts traffic that passes inspection and forwards it to the destination server, such as Google.

An example process is shown in the following figure. User **U** sends a HTTPS request (SSL) to destination server **D**, via the Zyxel Device, **Z**. The traffic matches an SSL Inspection profile in a security policy, so the Zyxel Device decrypts the traffic using SSL Inspection. The decrypted traffic is then inspected by the Security Service profiles in the same security profile that matched the SSL Inspection profile. If all is OK, then the Zyxel Device re-encrypts the traffic using SSL Inspection and forwards it to the destination server **D**. SSL traffic could be in the opposite direction for other examples.

Figure 397 SSL Inspection Overview



Note: Email security cannot be applied to traffic decrypted by SSL Inspection.

33.1.1 What You Can Do in this Chapter

- Use the **Security Service > SSL Inspection > Profile** screen (Section 33.2 on page 600) to view SSL Inspection profiles. Click the **Add** or **Edit** icon in this screen to configure the CA certificate, action and log in an SSL Inspection profile.
- Use the **Security Service > SSL Inspection > Exclude List** screens (Section 33.3 on page 605) to create a whitelist of destination servers to which traffic is passed through uninspected.

33.1.2 What You Need To Know

- Supported Cipher Suite
  - DES (Data Encryption Standard)

  - 3DES
  - AES (Advanced Encryption Standard)
- SSLv3/TLS1.0 (Transport Layer Security) Support
  - SSLv3/TLS1.0 is currently supported with option to pass or block SSLv2 traffic
- Traffic using TLS1.1 (Transport Layer Security) or TLS1.2 is downgraded to TLS1.0 for SSL Inspection
- No Compression Support Now
- No Client Authentication Request Support Now
- Finding Out More
  - See **Configuration** > **Object > Certificate > My Certificates** for information on creating certificates on the Zyxel Device.
  - See **Monitor > Security Statistics > SSL Inspection** to get usage data and easily add a destination server to the whitelist of exclusion servers.
  - See **Configuration** > **Security Policy > Policy Control > Policy** to bind an SSL Inspection profile to a traffic flow(s).

33.1.3 Before You Begin

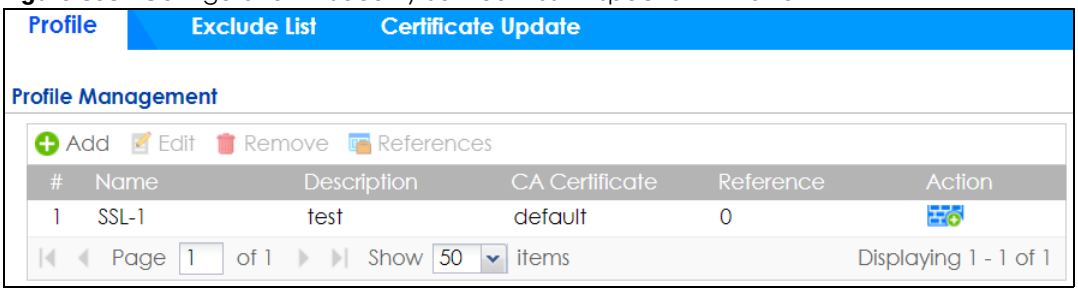
- If you don't want to use the default Zyxel Device certificate, then create a new certificate in **Object > Certificate > My Certificates**.
- Decide what destination servers to which traffic is sent directly without inspection. This may be a matter of privacy and legality regarding inspecting an individual's encrypted session, such as financial websites. This may vary by locale.

33.2 The SSL Inspection Profile Screen

An SSL Inspection profile is a template with pre-configured certificate, action and log.

Click **Configuration > Security Service > SSL Inspection > Profile** to open this screen.

Figure 398 Configuration > Security Service > SSL Inspection > Profile



The following table describes the fields in this screen.

Table 237 Configuration > Security Service > SSL Inspection > Profile

LABEL	DESCRIPTION
Profile Management	
Add	Click **Add** to create a new profile.
Edit	Select an entry and click this to be able to modify it.

Table 237 Configuration > Security Service > SSL Inspection > Profile (continued)

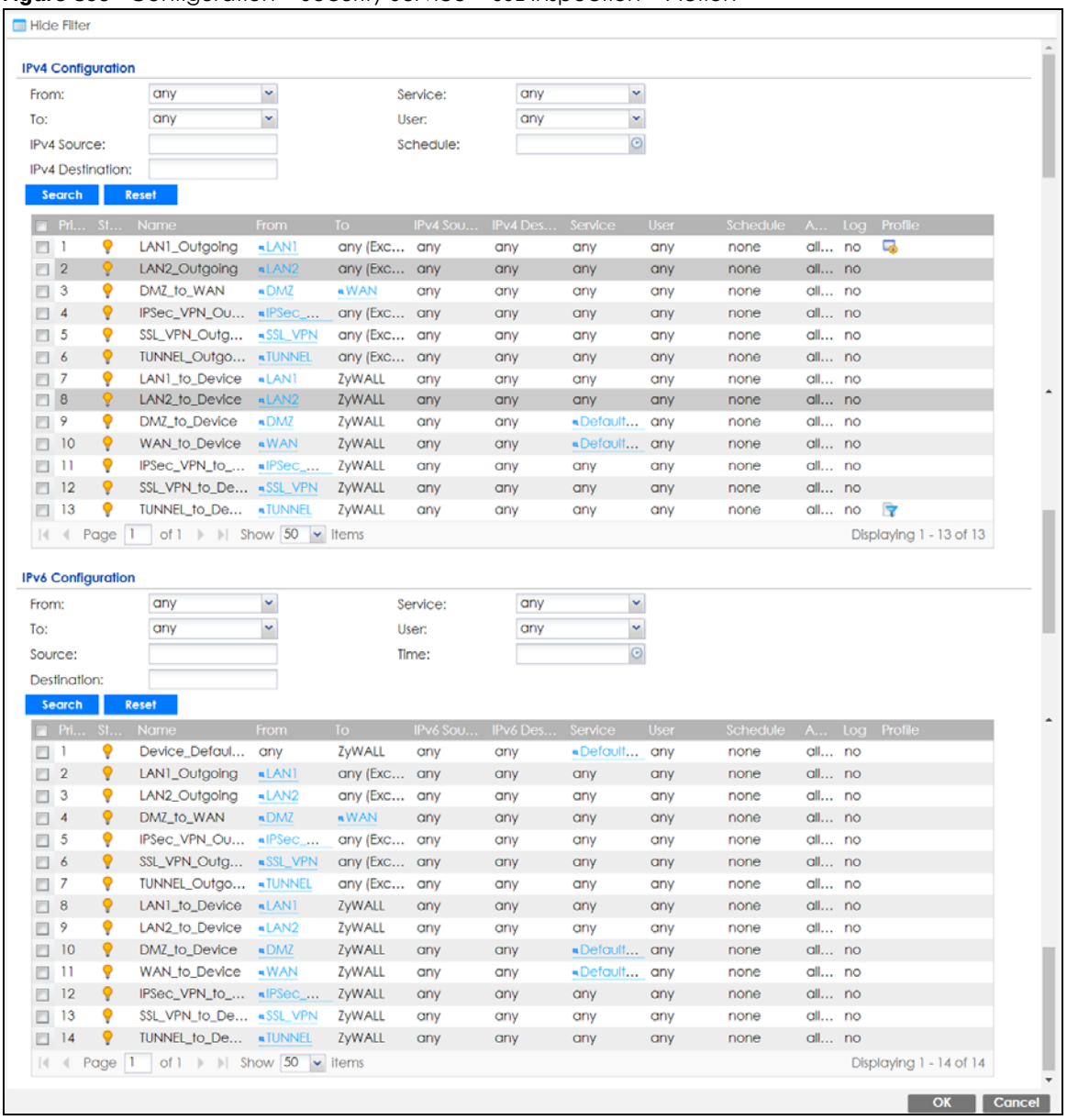
LABEL	DESCRIPTION
Remove	Select an entry and click this to delete it.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This is the entry's index number in the list.
Name	This displays the name of the profile.
Description	This displays the description of the profile.
CA Certificate	This displays the CA certificate being used in this profile.
Reference	This displays the number of times an object reference is used in a profile.
Action	Click this icon to apply the entry to a security policy. Go to the **Configuration > Security Policy > Policy Control** screen to check the result.

33.2.1 Apply to a Security Policy

Click the icon in the **Action** field to apply the entry to a security policy.

Go to the **Configuration > Security Policy > Policy Control** screen to check the result.

Figure 399 Configuration > Security Service > SSL Inspection > Action



The following table describes the labels in this screen.

Table 238 Configuration > Security Service > SSL Inspection > Action

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click **Show Filter** to display IPv4 and IPv6 (if enabled) security policy search filters.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. **any** means all zones.

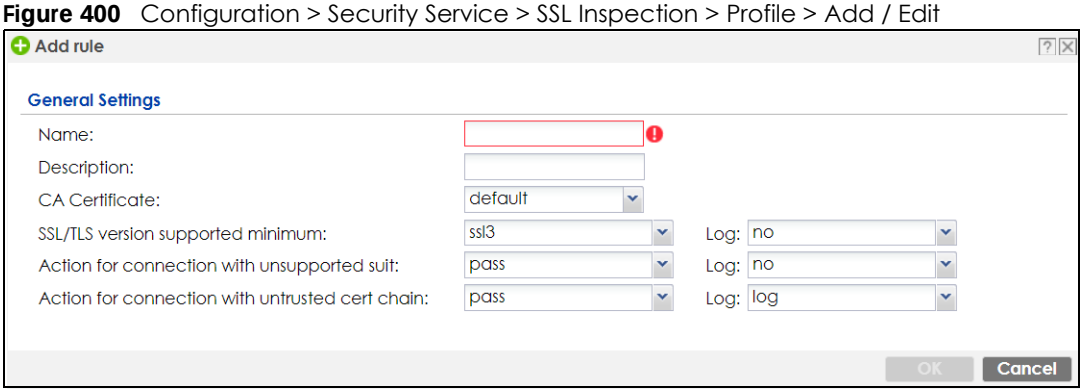
Table 238 Configuration > Security Service > SSL Inspection > Action

LABEL	DESCRIPTION
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. **Default** displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from **LAN** to **LAN** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From **any** displays all the Security Policies for traffic going to the selected **To Zone**. To **any** displays all the Security Policies for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the Security Policies. To **ZyWALL** policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. **none** means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (**deny**), permits the passage of packets (**allow**) or drops packets with notification (**reject**)
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or not (**no**) when the policy is matched to the criteria listed above.
Profile	This field shows you which Security Service profiles (application patrol, content filter, IDP, anti-malware, email security) apply to this Security policy. Click an applied Security Service profile icon to edit the profile directly.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

33.2.2 Add / Edit SSL Inspection Profiles

Click **Configuration > Security Service > SSL Inspection > Profile > Add** to create a new profile or select an existing profile and click **Edit** to change its settings.

Figure 400 Configuration > Security Service > SSL Inspection > Profile > Add / Edit



The following table describes the fields in this screen.

Table 239 Configuration > Security Service > SSL Inspection > Profile > Add / Edit

LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Enter additional information about this SSL Inspection entry. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
CA Certificate	This contains the default certificate and the certificates created in **Object > Certificate > My Certificates**. Choose the certificate for this profile.
SSL/TLS version supported minimum	SSL Inspection supports SSLv3, TLS1.0, TLS1.1, and TLS1.2 to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted traffic.
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Monitor > Log** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.

Table 239 Configuration > Security Service > SSL Inspection > Profile > Add / Edit (continued)

LABEL	DESCRIPTION
Action for Connection with unsupported suit	SSL Inspection supports these cipher suites: • DES • 3DES • AES Select to **pass** or **block** unsupported traffic (such as other cipher suites, compressed traffic, client authentication requests, and so on) that matches traffic bound to this policy here.
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Monitor > Log** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.
Action for connection with untrusted cert chain	A certificate chain is a certification process that involves the following certificates between the SSL/TLS server and a client. A certificate chain will fail if one of the following certificates is not correct. • A certificate owned by a user • The certificate signed by a certification authority • A root certificate Select to **pass**, **inspect**, or **block** an untrusted certification chain.
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Monitor > Log** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.
OK	Click **OK** to save your settings to the Zyxel Device, and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

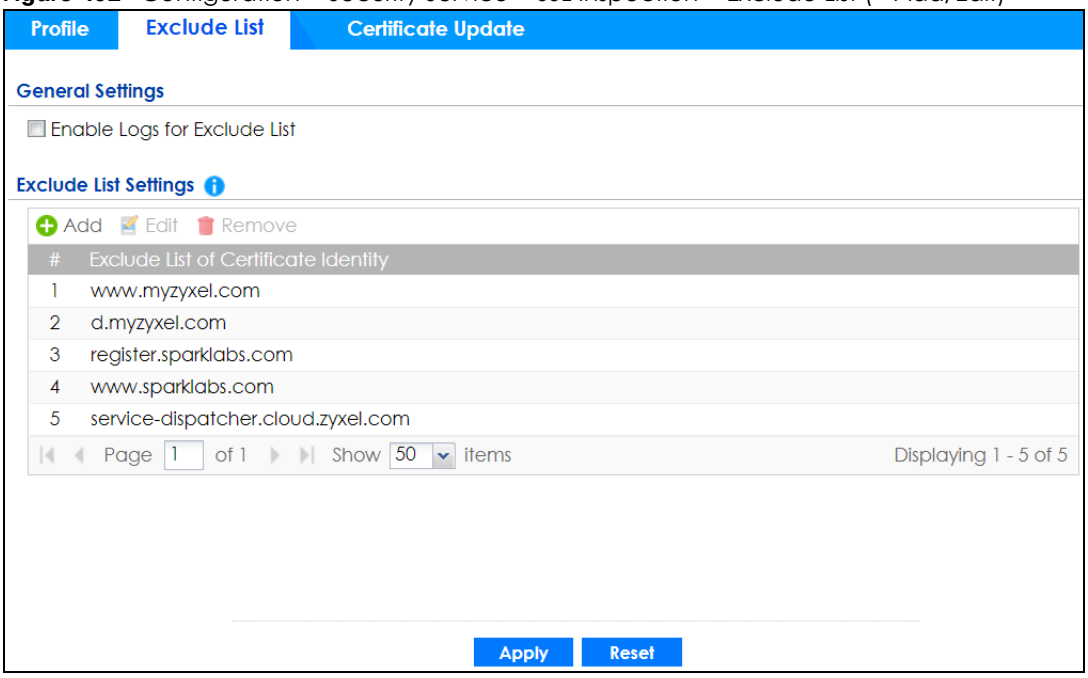
33.3 Exclude List Screen

There may be privacy and legality issues regarding inspecting a user's encrypted session. The legal issues may vary by locale, so it's important to check with your legal department to make sure that it's OK to intercept SSL traffic from your Zyxel Device users.

To ensure individual privacy and meet legal requirements, you can configure an exclusion list to exclude matching sessions to destination servers. This traffic is not intercepted and is passed through uninspected.

Click **Configuration > Security Service > SSL Inspection > Exclude List** to display the following screen. Use **Add** to put a new item in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 401 Configuration > Security Service > SSL Inspection > Exclude List (> Add/Edit)



The following table describes the fields in this screen.

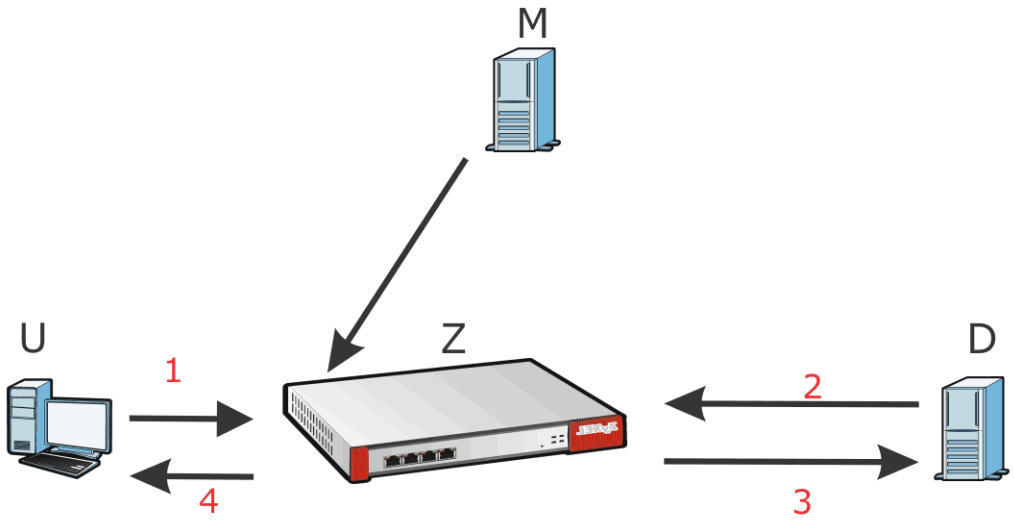
Table 240 Configuration > Security Service > SSL Inspection > Exclude List

LABEL	DESCRIPTION
General Settings	
Enable Logs for Exclude List	Click this to create a log for traffic that bypasses SSL Inspection.
Exclude List Settings	Use this part of the screen to create, edit, or delete items in the SSL Inspection exclusion list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Exclude List of Certificate Identity	SSL traffic to a server to be excluded from SSL Inspection is identified by its certificate. Identify the certificate in one of the following ways: • The Common Name (CN) of the certificate. The common name of the certificate can be created in the **Object > Certificate > My Certificates** screen. • Type an IPv4 or IPv6 address. For example, type 192.168.1.35, or 2001:7300:3500::1 • Type an IPv4/IPv6 in CIDR notation. For example, type 192.168.1.1/24, or 2001:7300:3500::1/64 • Type an IPv4/IPv6 address range. For example, type 192.168.1.1-192.168.1.35, or 2001:7300:3500::1-2001:7300:3500::35 • Type an email address. For example, type abc@zyxel.com.tw • Type a DNS name or a common name (wildcard char: '*', escape char: '\'). Use up to 127 case-insensitive characters (0-9a-zA-Z`~!@#$%^&*()-_=+[]{}\\\|;:',.<>/?). '*' can be used as a wildcard to match any string. Use '*' to indicate a single wildcard character. Alternatively, to automatically add an entry for existing SSL traffic to a destination server, go to **Monitor > Security Statistics > SSL Inspection > Certificate Cache List**, select an item and then click **Add to Exclude List**. The item will then appear here.
Apply	Click **Apply** to save your settings to the Zyxel Device.
Reset	Click **Reset** to return to the profile summary page without saving any changes.

33.4 Certificate Update Screen

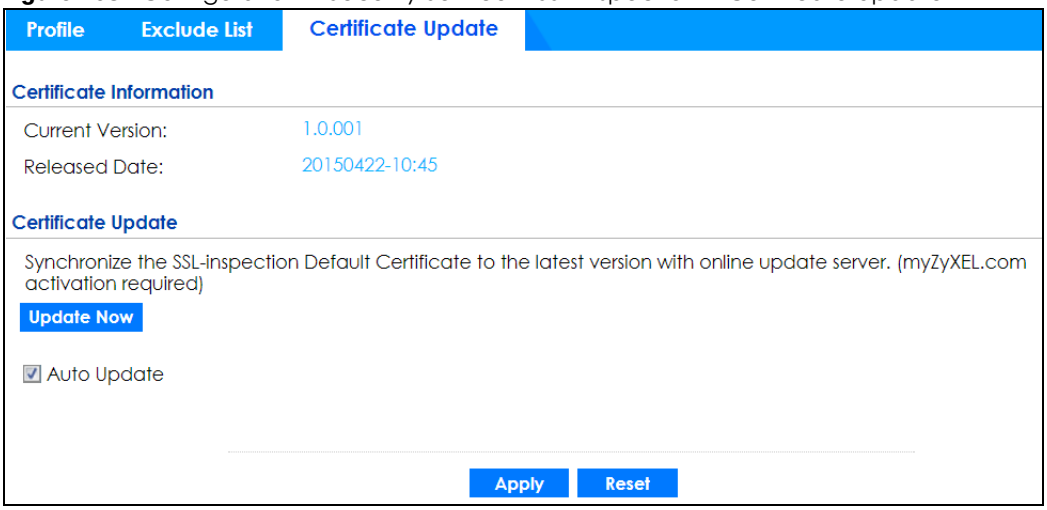
Use this screen to update the latest certificates of servers using SSL connections to the Zyxel Device network. User **U** sends an SSL request to destination server **D** (**1**), via the Zyxel Device, **Z**. D replies (**2**); **Z** intercepts the response from **D** and checks if the certificate has been previously signed. **Z** then replies to **D** (**3**) and also to **U** (**4**). D's latest certificate is stored at myZyxel (**M**) along with other server certificates and can be downloaded to the Zyxel Device.

Figure 402 SSL Inspection Certificate Update Overview



Click **Configuration > Security Service > SSL Inspection > Certificate Update** to display the following screen.

Figure 403 Configuration > Security Service > SSL Inspection > Certificate Update



The following table describes the fields in this screen.

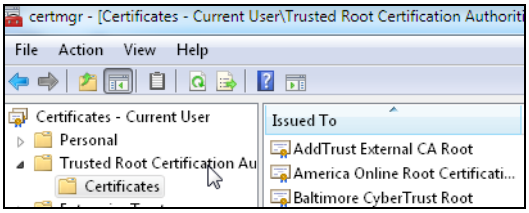
Table 241 Configuration > Security Service > SSL Inspection > Certificate Update

LABEL	DESCRIPTION
Certificate Information	
Current Version	This displays the current certificate set version.
Released Date	This field displays the date and time the current certificate set was released.
Certificate Update	You should have Internet access and have activated SSL Inspection on the Zyxel Device at myZyxel.
Update Now	Click this button to download the latest certificate set (Windows, MAC OS X, and Android) from the myZyxel and update it on the Zyxel Device.
Auto Update	Select this to automatically have the Zyxel Device update the certificate set when a new one becomes available on myZyxel.
Apply	Click **Apply** to save your settings to the Zyxel Device.
Reset	Click **Reset** to return to the profile summary page without saving any changes.

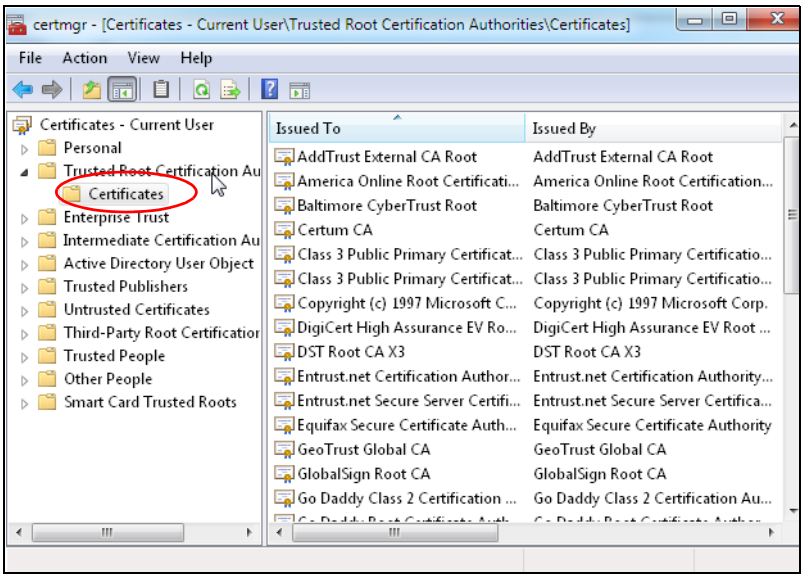
33.5 Install a CA Certificate in a Browser

Certificates used in SSL Inspection profiles should be installed in user web browsers. Do the following steps to install a certificate in a computer with a Windows operating system (PC). First, save the certificate to your computer.

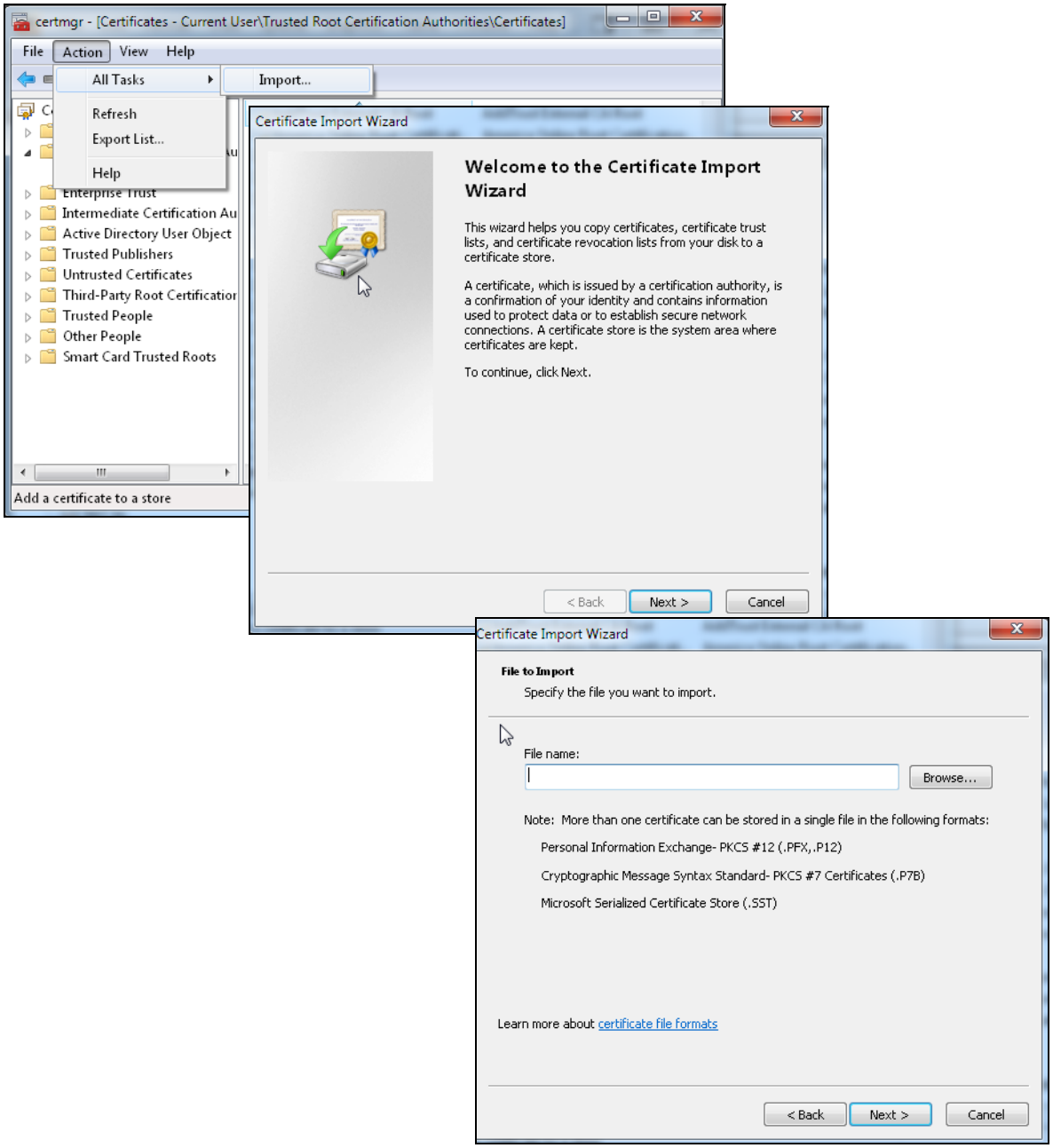
1 Run the certificate manager using certmgr.msc.



2 Go to **Trusted Root Certification Authorities > Certificates**.



3 From the main menu, select **Action > All Tasks > Import** and run the **Certificate Import Wizard** to install the certificate on the PC.



33.5.0.1 Firefox Browser

If you're using a Firefox browser, in addition to the above you need to do the following to import a certificate into the browser.

Click **Tools > Options > Advanced > Encryption > View Certificates**, click **Import** and enter the filename of the certificate you want to import. See the browser's help for further information.

CHAPTER 34
IP Exception

34.1 Overview

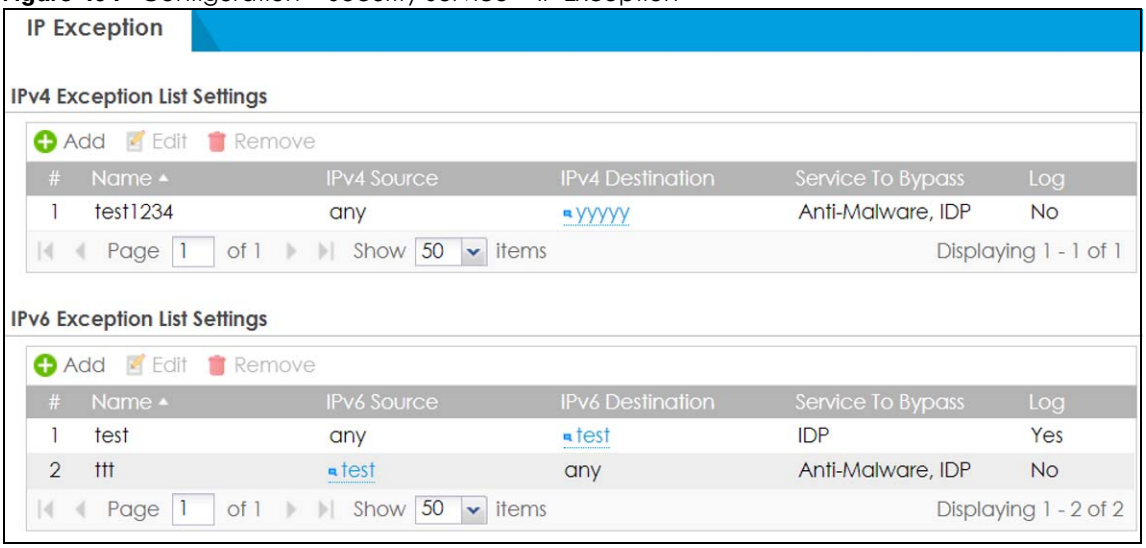
The Zyxel Device won't intercept nor inspect the incoming packets that match the rules in the IP exception list for the anti-malware and/or IDP (Intrusion, Detection, and Prevention) features.

34.2 The IP Exception Screen

Use this screen to view the IP exception list for the anti-malware and IDP (Intrusion, Detection, and Prevention) features. The Zyxel Device will exclude the incoming packets coming from the listed source IP address(es) and destined for the listed destination IP address(es). These packets won't be intercepted and will be passed through uninspected.

Click **Configuration > Security Service > IP Exception** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 404 Configuration > Security Service > IP Exception



The following table describes the fields in this screen.

Table 242 Configuration > Security Service > IP Exception

LABEL	DESCRIPTION
IPv4/IPv6 Exception List Settings	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.

Table 242 Configuration > Security Service > IP Exception (continued)

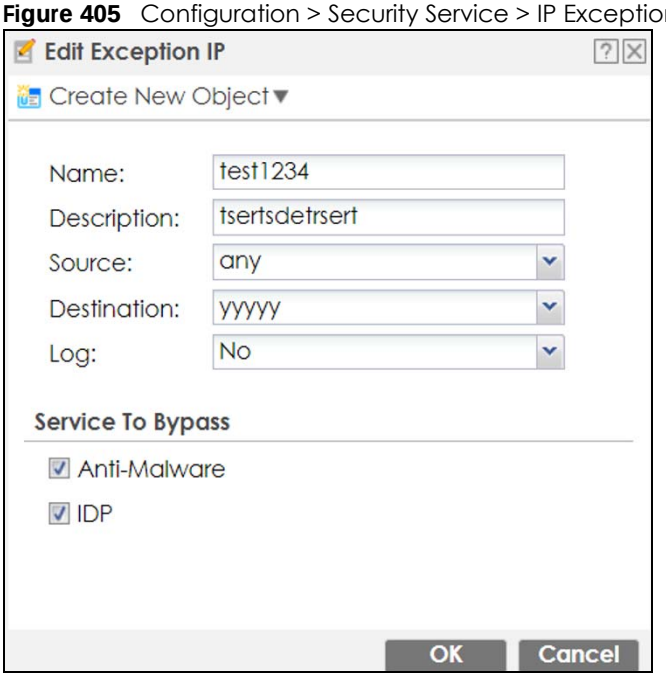
LABEL	DESCRIPTION
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Name	This field displays the descriptive name of this entry.
IPv4/IPv6 Source	This field displays the source IP address (or address object) of incoming traffic. It displays **any** if there is no restriction on the source IP address.
IPv4/IPv6 Destination	This field displays the destination IP address (or address object) of incoming traffic. It displays **any** if there is no restriction on the destination IP address.
Service to Bypass	This field displays to which feature (anti-malware and/or IDP) the entry applies.
Log	This field displays if the Zyxel Device will generate a log when the incoming traffic is in the exception list.

34.2.1 The IP Exception Add/Edit Screen

Use this screen to add or edit entries of IPv4 or IPv6 address in the IP exception list.

Click **Configuration > Security Service > IP Exception > Add/Edit** to display the following screen.

Figure 405 Configuration > Security Service > IP Exception > Add/Edit



The following table describes the fields in this screen.

Table 243 Configuration > Security Service > IP Exception > Add/Edit

LABEL	DESCRIPTION
Create New Object	Use this to configure any new settings objects that you need to use in this screen.
Name	Enter a descriptive name of this entry.
Description	Enter the description for this entry. You can use up to 60 printable ASCII characters.
Source	Select **any** or an address object of the source IP address for this entry. Select **any** so there's no restriction on the source IP address.

Table 243 Configuration > Security Service > IP Exception > Add/Edit (continued)

LABEL	DESCRIPTION
Destination	Select **any** or an address object of the destination IP address for this entry. Select **any** so there's no restriction on the destination IP address.
Log	Select **Yes** to have the Zyxel Device generate a log when the incoming traffic is in the exception list. Otherwise, select **No**.
Service to Bypass	Select **Anti-Malware** and/or **IDP** that the entry will apply to.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

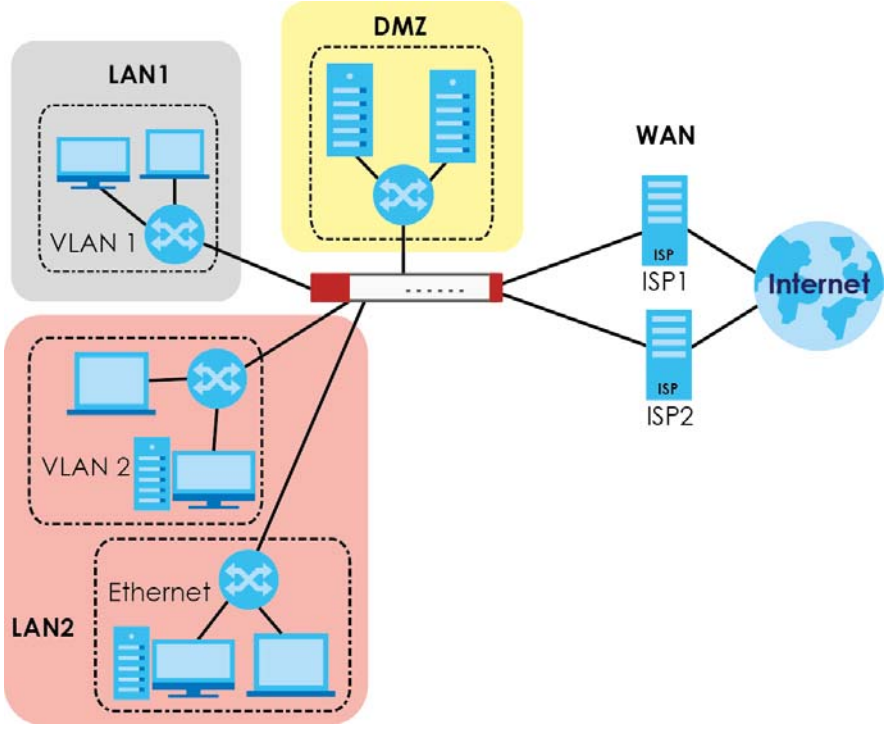
CHAPTER 35
Object

35.1 Zones Overview

Set up zones to configure network security and network policies in the Zyxel Device. A zone is a group of interfaces and/or VPN tunnels. The Zyxel Device uses zones instead of interfaces in many security and policy settings, such as Secure Policies rules, Security Service, and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 406 Example: Zones



Use the **Zone** screens (see Section 35.8.2 on page 670) to manage the Zyxel Device's zones.

35.1.1 What You Need to Know

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 406 on page 614, traffic between VLAN 2 and the Ethernet is intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 406 on page 614, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

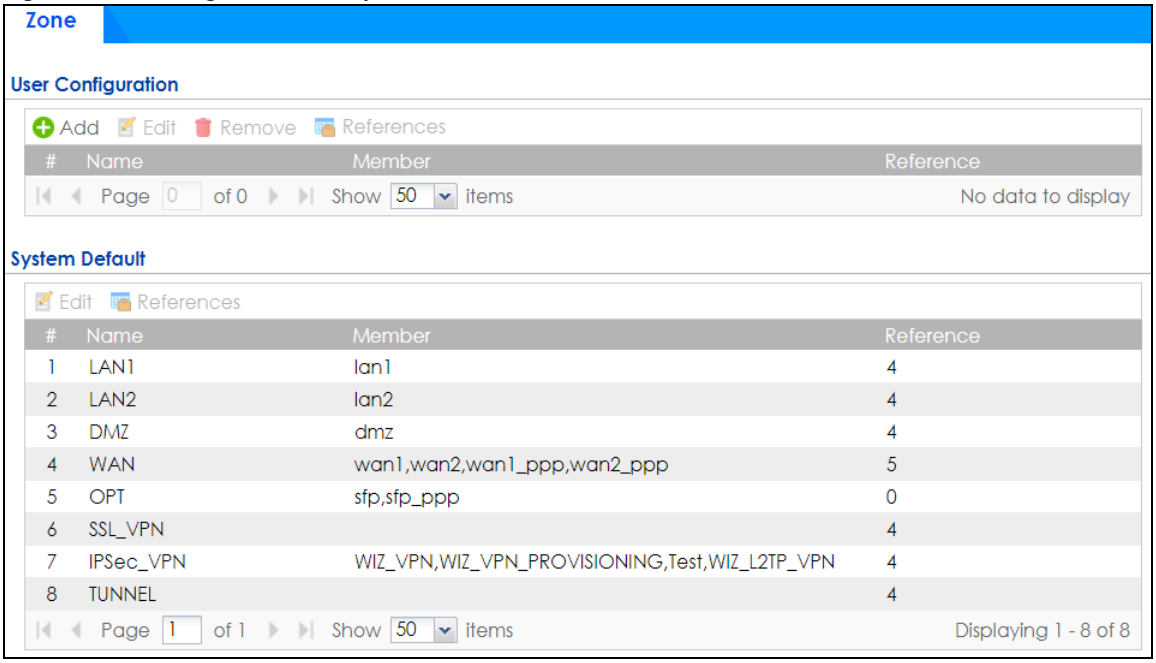
Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 406 on page 614, traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

35.1.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Configuration > Object > Zone**.

Figure 407 Configuration > Object > Zone



The following table describes the labels in this screen.

Table 244 Configuration > Object > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device comes with pre-configured **System Default** zones that you cannot delete. You can create your own **User Configuration** zones
Add	Click this to create a new, user-configured zone.

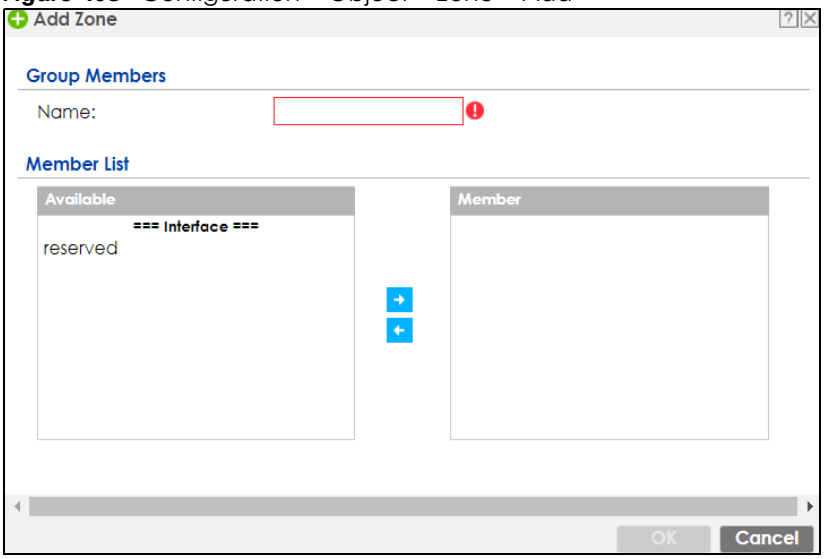
Table 244 Configuration > Object > Zone (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, 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. Click Refresh to update information in this screen.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

35.1.2.1 Zone Edit

The **Zone Edit** screen allows you to add or edit a zone. To access this screen, go to the **Zone** screen (see Section 35.8.2 on page 670), and click the **Add** icon or an **Edit** icon.

Figure 408 Configuration > Object > Zone > Add



The following table describes the labels in this screen.

Table 245 Configuration > Object > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	**Available** lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. **Member** lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.

Table 245 Configuration > Object > Zone > Add/Edit (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

35.2 User/Group Overview

This section describes how to set up user accounts, user groups, and user settings for the Zyxel Device. You can also set up rules that control when users have to log in to the Zyxel Device before the Zyxel Device routes traffic for them.

- The **User** screen (see Section 35.13.1 on page 713) provides a summary of all user accounts.
- The **Group** screen (see Section 35.2.3 on page 624) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups.
- The **Setting** screen (see Section 35.2.4 on page 625) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device. You can also use this screen to specify when users must log in to the Zyxel Device before it routes traffic for them.
- The **MAC Address** screen (see Section 35.2.5 on page 630) allows you to configure the MAC addresses or OUI (Organizationally Unique Identifier) of wireless clients for MAC authentication using the local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.

35.2.1 What You Need To Know

User Account

A user account defines the privileges of a user logged into the Zyxel Device. User accounts are used in security policies and application patrol, in addition to controlling access to configuration and services in the Zyxel Device.

User Types

These are the types of user accounts the Zyxel Device uses.

Table 246 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW

Table 246 Types of User Accounts (continued)

TYPE	ABILITIES	LOGIN METHOD(S)
ext-group-user	External group user account	WWW
guest-manager	Create dynamic guest accounts	WWW
dynamic-guest	Access network services	Hotspot Portal

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 35 on page 685 for more information about authentication methods.)

Ext-User Accounts

Set up an **ext-user** account if the user is authenticated by an external server and you want to set up specific policies for this user in the Zyxel Device. If you do not want to set up policies for this user, you do not have to set up an **ext-user** account.

All **ext-user** users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the Zyxel Device tries to use the local database to authenticate an **ext-user**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in those chapters in this guide.)

Note: If the Zyxel Device tries to authenticate an **ext-user** using the local database, the attempt always fails.

Once an **ext-user** user has been authenticated, the Zyxel Device tries to get the user type (see Table 246 on page 617) from the external server. If the external server does not have the information, the Zyxel Device sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the Zyxel Device checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the Zyxel Device.
3. Default user account for AD users (**ad-users**), LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the Zyxel Device.

See Setting up User Attributes in an External Server for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See Section 35.9.5.1 on page 679 for more on the group membership attribute.

Dynamic-Guest Accounts

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the Zyxel Device's local user database. A dynamic guest account has a dynamically-created user name and

password. A dynamic guest account user can access the Zyxel Device's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: **billing-users**, **ua-users** and **trial-users**.

billing-users are guest account created with the guest manager account or an external printer and paid by cash or created and paid via the on-line payment service. **ua-users** are users that log in from the user agreement page. **trial-users** are free guest accounts that are created with the Free Time function.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

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

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

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the Zyxel Device to use the network services it provides. The Zyxel Device automatically routes packets for everyone. If you want to restrict network services that certain users can use via the Zyxel Device, you can require them to log in to the Zyxel Device first. The Zyxel Device is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See Section 35.2.6 on page 632 for a user-aware login example.

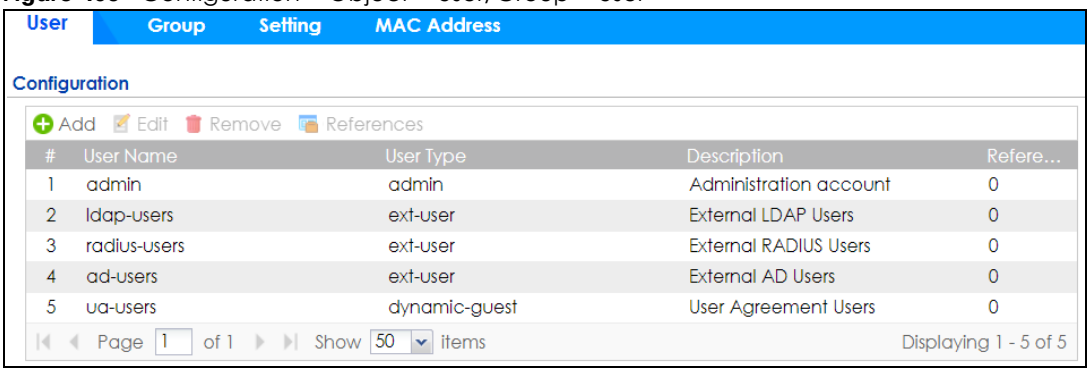
Finding Out More

- See Section 35.2.6 on page 632 for some information on users who use an external authentication server in order to log in.
- The Zyxel Device supports TTLS using PAP so you can use the Zyxel Device's local user database to authenticate users with WPA or WPA2 instead of needing an external RADIUS server.

35.2.2 User/Group User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group**.

Figure 409 Configuration > Object > User/Group > User



The following table describes the labels in this screen.

Table 247 Configuration > Object > User/Group > User

LABEL	DESCRIPTION
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 user.
User Name	This field displays the user name of each user.
User Type	This field displays the types of user accounts the Zyxel Device uses: • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **dynamic-guest** - this user has access to the Zyxel Device's services but cannot look at the configuration. • **user** - this user has access to the Zyxel Device's services and can also browse user-mode commands (CLI). • **guest** - this user has access to the Zyxel Device's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 618 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 618 for more information about this type. • **guest-manager** - this user can log in via the web configurator login screen and create dynamic guest accounts using the **Account Generator** screen that pops up.
Description	This field displays the description for each user.
Reference	This displays the number of times an object reference is used in a profile.

35.2.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

35.2.2.2 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)

- _ [underscores]
- - [dashes]

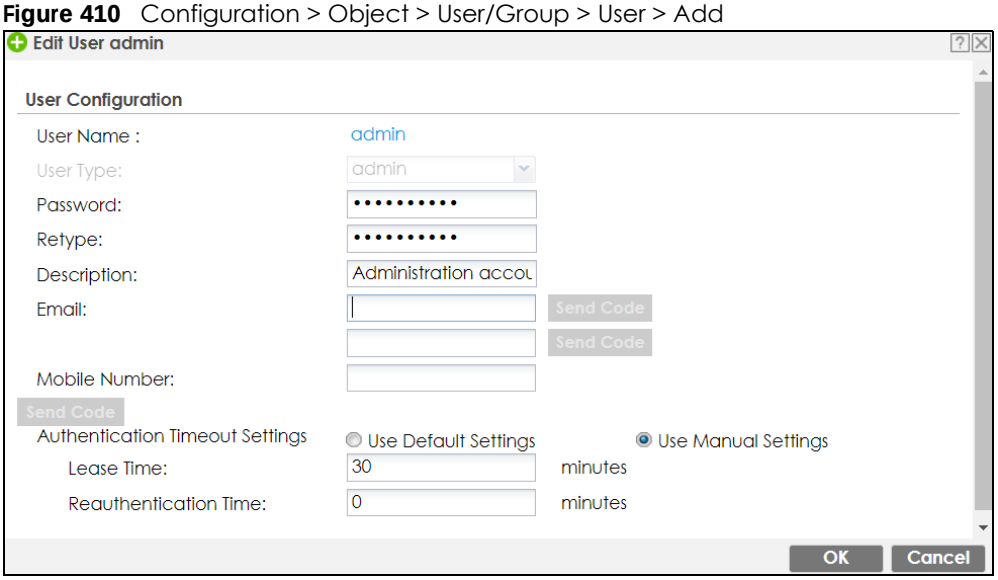
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• shutdown	• sshd
• sync	• uucp	• zyxel		

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

Figure 410 Configuration > Object > User/Group > User > Add



The following table describes the labels in this screen.

Table 248 Configuration > Object > User/Group > User > Add

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 35.2.2.2 on page 620.
User Type	This field displays the types of user accounts the Zyxel Device uses: • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this user has access to the Zyxel Device's services and can also browse user-mode commands (CLI). • **guest** - this user has access to the Zyxel Device's services but cannot look at the configuration. • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 618 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 618 for more information about this type.
Password	This field is not available if you select the **ext-user** or **ext-group-user** type. Enter a password of from 1 to 64 characters for this user account. If you selected **Enable Password Complexity** in **Configuration > Object > User/Group > Setting**, it must consist of at least 8 characters and at most 64. At least 1 character must be a number, at least 1 a lower case letter, at least 1 an upper case letter and at least 1 a special character from the keyboard, such as !@#$%^&*()_+.
Retype	This field is not available if you select the **ext-user** or **ext-group-user** type.
Group Identifier	This field is available for a **ext-group-user** type user account. Specify the value of the AD or LDAP server's **Group Membership Attribute** that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a **ext-group-user** type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Email	Type one or more valid email addresses for this user so that email messages can be sent to this user if required. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com.
Mobile Number	Type a valid mobile telephone number for this user so that SMS messages can be sent to this user if required. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-].

Table 248 Configuration > Object > User/Group > User > Add (continued)

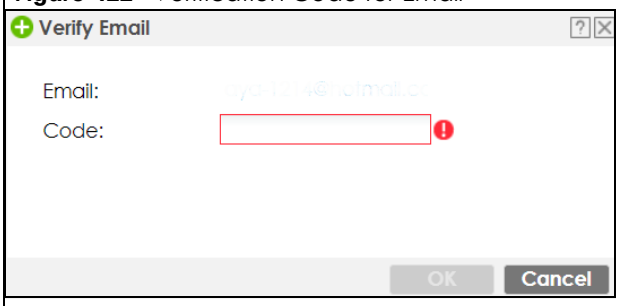
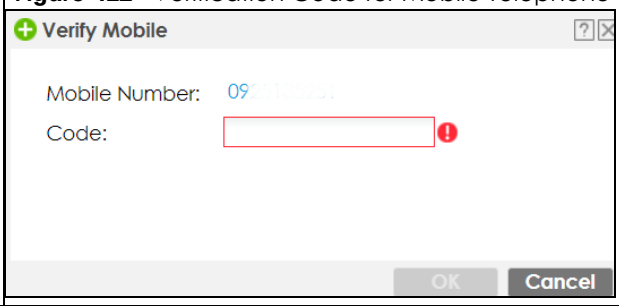
LABEL	DESCRIPTION
Send Code	This button is available when the user type is **admin** or **limited-admin**. Click this and an authorization email or SMS message with a code of six digits will be sent to the email addresses or mobile telephone number you put in. Enter the verification code to verify your email addresses or mobile telephone number. **Figure 411** Verification Code for Email  **Figure 412** Verification Code for Mobile Telephone Number 
Authentication Timeout Settings	If you want the system to use default settings, select **Use Default Settings**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.
Lease Time	If you select **Use Default Settings** in the **Authentication Timeout Settings** field, the default lease time is shown. If you select **Use Manual Settings**, you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 35.2.4 on page 625), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select **Use Default Settings** in the **Authentication Timeout Settings** field, the default lease time is shown. If you select **Use Manual Settings**, you need to type the number of minutes this user can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
User VLAN ID	This field is available for a **ext-group-user** type user account. Select this option to enable dynamic VLAN assignment on the Zyxel Device. When a user is authenticated successfully, all data traffic from this user is tagged with the VLAN ID number you specify here. This allows you to assign a user of the **ext-group-user** type to a specific VLAN based on the user credentials instead of using an AAA server.

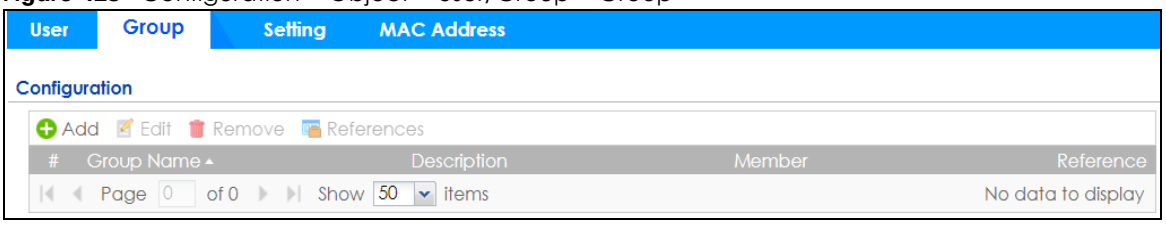
Table 248 Configuration > Object > User/Group > User > Add (continued)

LABEL	DESCRIPTION
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the **User Name** field and click **Test**.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.2.3 User/Group Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Group**.

Figure 413 Configuration > Object > User/Group > Group



The following table describes the labels in this screen. See Section 35.2.3.1 on page 624 for more information as well.

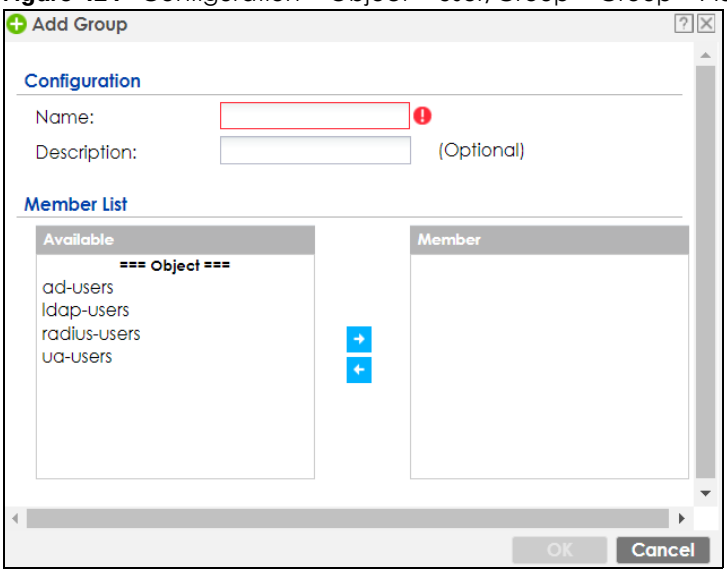
Table 249 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
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. Removing a group does not remove the user accounts in the group.
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 user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

35.2.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see Section 35.2.3 on page 624), and click either the **Add** icon or an **Edit** icon.

Figure 414 Configuration > Object > User/Group > Group > Add



The following table describes the labels in this screen.

Table 250 Configuration > Object > User/Group > Group > Add

LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The **Member** list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the **Available** list that you want to be members of this group and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.2.4 User/Group Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device. You can also use this screen to specify when users must log in to the Zyxel Device before it routes traffic for them.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Setting**.

Figure 415 Configuration > Object > User/Group > Setting

User | Group | Setting | MAC Address

User Default Setting

Default Authentication Timeout Settings

Edit

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	user	1440	1440
4	guest	1440	1440
5	ext-user	1440	1440
6	ext-group-user	1440	1440

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

Miscellaneous Settings

Allow renewing lease time automatically

Enable user idle detection

User idle timeout: 3 (1-60 minutes)

Login Security

Password must changed every (days) 180 (1-365 days)

Password reset link(FQDN/IP): Default myrouter

Enable Password Complexity

Complexity requirement:
* Minimun password length should be of 8 characters.
* Include at least 1 Upper case alphabetic characters.
* Include at least 1 Lower case alphabetic characters.
* Include at least 1 numeric character.
* Include at least 1 special characters like '@','$','!'...

User Logon Settings

Limit the number of simultaneous logons for administration account

Maximum number per administration account: 1 (1-128)

Limit the number of simultaneous logons for access account

Maximum number per access account: 1 (1-128)

User Lockout Settings

Enable logon retry limit

Maximum retry count: 5 (1-99)

Lockout period: 30 (1-65535 minutes)

Apply Reset

The following table describes the labels in this screen.

Table 251 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.

Table 251 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the Zyxel Device supports. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this user has access to the Zyxel Device's services but cannot look at the configuration • **guest** - this user has access to the Zyxel Device's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 618 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 618 for more information about this type.
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 35.2.4 on page 625), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Miscellaneous Settings	
Allow renewing lease time automatically	Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the **Updating lease time automatically** check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the Zyxel Device to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The Zyxel Device automatically logs out the access user once the **User idle timeout** has been reached.
User idle timeout	This is applicable for access users. This field is effective when **Enable user idle detection** is checked. Type the number of minutes each access user can be logged in and idle before the Zyxel Device automatically logs out the access user.
Login Security	
Password must changed every (days):	Enter how often users must change their password when they log into the Zyxel Device. You can choose from once a day to once a year.
Password reset link (FQDN/IP):	Associate the password expiration to a specific Zyxel Device. **Default** is this Zyxel Device (myrouter) or select **Custom** and enter the IP address or Fully Qualified Domain Name (FQDN).
Enable Password Complexity	Select this to enforce the following conditions in a user password. Requiring a strong password is good for security. The conditions are that the password must consist of at least 8 characters and at most 64. At least 1 character must be a number, at least 1 a lower case letter, at least 1 an upper case letter and at least 1 a special character from the keyboard, such as !@#$%^&*()_+.

Table 251 Configuration > Object > User/Group > Setting (continued)

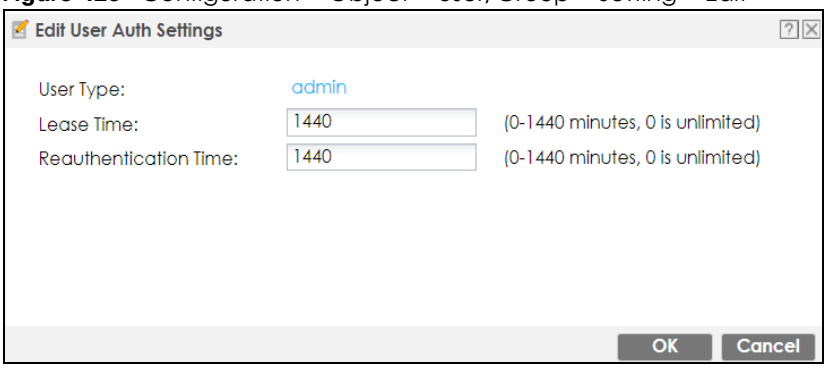
LABEL	DESCRIPTION
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user.
Limit the number of simultaneous logons for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	This field is effective when **Limit ... for access account** is checked. Type the maximum number of simultaneous logins by each access user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.2.4.1 Default User Authentication Timeout Settings Edit Screens

The **Default Authentication Timeout Settings Edit** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User/Group > Setting** screen (see Section 35.2.4 on page 625), and click one of the **Default Authentication Timeout Settings** section's **Edit** icons.

Figure 416 Configuration > Object > User/Group > Setting > Edit



The following table describes the labels in this screen.

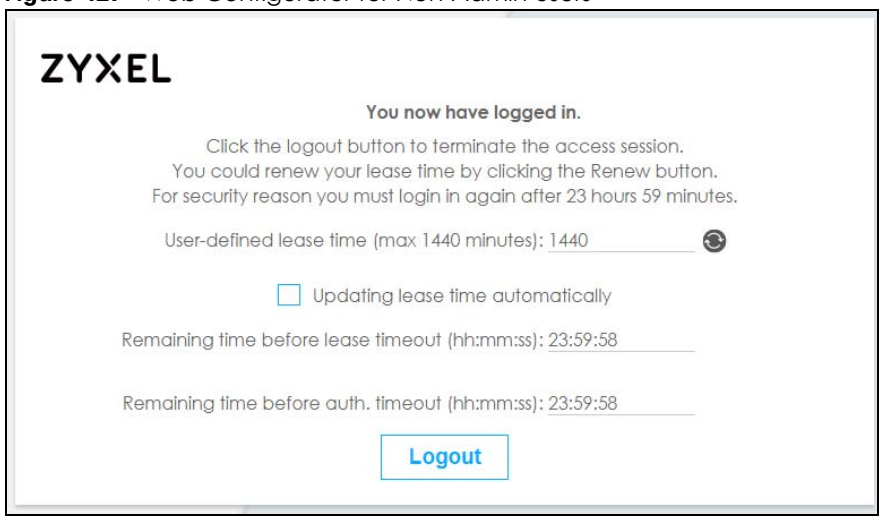
Table 252 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it. • **dynamic-guest** - this user has access to the Zyxel Device's services but cannot look at the configuration. • **user** - this user has access to the Zyxel Device's services but cannot look at the configuration. • **guest** - this user has access to the Zyxel Device's services but cannot look at the configuration. • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 618 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 618 for more information about this type. • **guest-manager** - this user can log in via the web configurator login screen and create dynamic guest accounts using the **Account Generator** screen that pops up.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 35.2.4 on page 625), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.2.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the Zyxel Device. Instead, after access users log into the Zyxel Device, the following screen appears.

Figure 417 Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 253 Web Configurator for Non-Admin Users

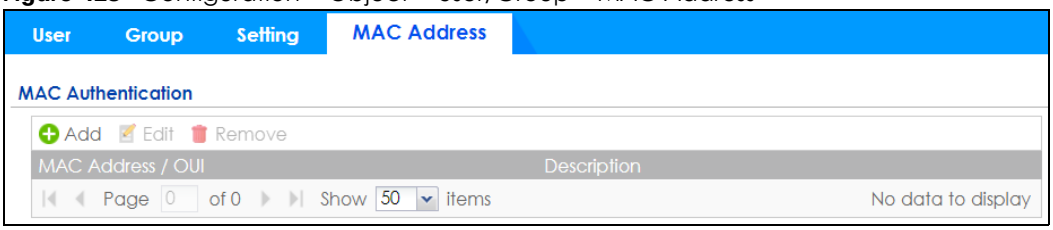
LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the Zyxel Device automatically logs them out. The Zyxel Device sets this amount of time according to the: • **User-defined lease time** field in this screen • **Lease time** field in the **User Add/Edit** screen (see Section 35.2.5.1 on page 631) • **Lease time** field in the **Setting** screen (see Section 35.2.4 on page 625).
Updating lease time automatically	This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 35.2.4 on page 625.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the **Renew** button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the Zyxel Device automatically logs the access user out, regardless of the lease time.

35.2.5 User/Group MAC Address Summary Screen

This screen shows the MAC addresses of wireless clients, which can be authenticated by their MAC addresses using the local user database. Click **Configuration > Object > User/Group > MAC Address** to open this screen.

Note: You need to configure an SSID security profile's MAC authentication settings to have the AP use the Zyxel Device's local database to authenticate wireless clients by their MAC addresses.

Figure 418 Configuration > Object > User/Group > MAC Address



The following table describes the labels in this screen.

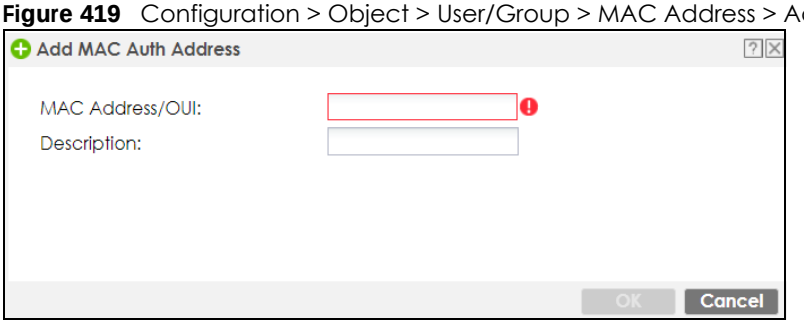
Table 254 Configuration > Object > User/Group > MAC Address

LABEL	DESCRIPTION
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.
MAC Address/ OUI	This field displays the MAC address or OUI (Organizationally Unique Identifier of computer hardware manufacturers) of wireless clients using MAC authentication with the Zyxel Device local user database.
Description	This field displays a description of the device identified by the MAC address or OUI.

35.2.5.1 MAC Address Add/Edit Screen

This screen allows you to create a new allowed device or edit an existing one. To access this screen, go to the **MAC Address** screen (see Section 35.2.5 on page 630), and click either the **Add** icon or an **Edit** icon.

Figure 419 Configuration > Object > User/Group > MAC Address > Add



The following table describes the labels in this screen.

Table 255 Configuration > Object > User/Group > MAC Address > Add

LABEL	DESCRIPTION
MAC Address/ OUI	Type the MAC address (six hexadecimal number pairs separated by colons or hyphens) or OUI (three hexadecimal number pairs separated by colons or hyphens) to identify specific wireless clients for MAC authentication using the Zyxel Device local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
Description	Enter an optional description of the wireless device(s) identified by the MAC or OUI. You can use up to 60 characters, punctuation marks, and spaces.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.2.6 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 256 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	**User Type**. Possible Values: admin, limited-admin, dynamic-guest, user, guest.
leaseTime	**Lease Time**. Possible Values: 1-1440 (minutes).
reauthTime	**Reauthentication Time**. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 420 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 421 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts.

35.3 AP Profile Overview

This section shows you how to configure preset profiles for the Access Points (APs) connected to your Zyxel Device's wireless network.

- The **Radio** screen (Section 35.3.1 on page 633) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 35.3.2 on page 639) configures three different types of profiles for your networked APs.

35.3.0.1 What You Need To Know

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

Wireless Profiles

At the heart of all wireless AP configurations on the Zyxel Device are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 32 radio profiles on the Zyxel Device.
- **SSID** - This profile type defines the properties of a single wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 32 SSID profiles on the Zyxel Device.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 32 security profiles on the Zyxel Device.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 32 MAC filtering profiles on the Zyxel Device.

SSID

The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the wireless network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.

IEEE 802.1x

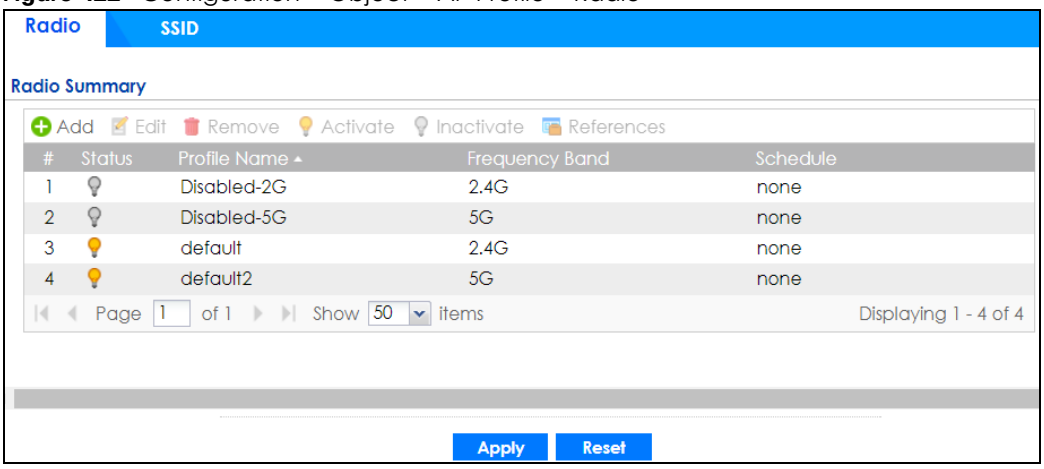
The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

35.3.1 Radio Screen

This screen allows you to create radio profiles for the APs on your network. A radio profile is a list of settings that a supported managed AP (NWA5121-N for example) can use to configure either one of its two radio transmitters. To access this screen click **Configuration > Object > AP Profile**.

Note: You can have a maximum of 32 radio profiles on the Zyxel Device.

Figure 422 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

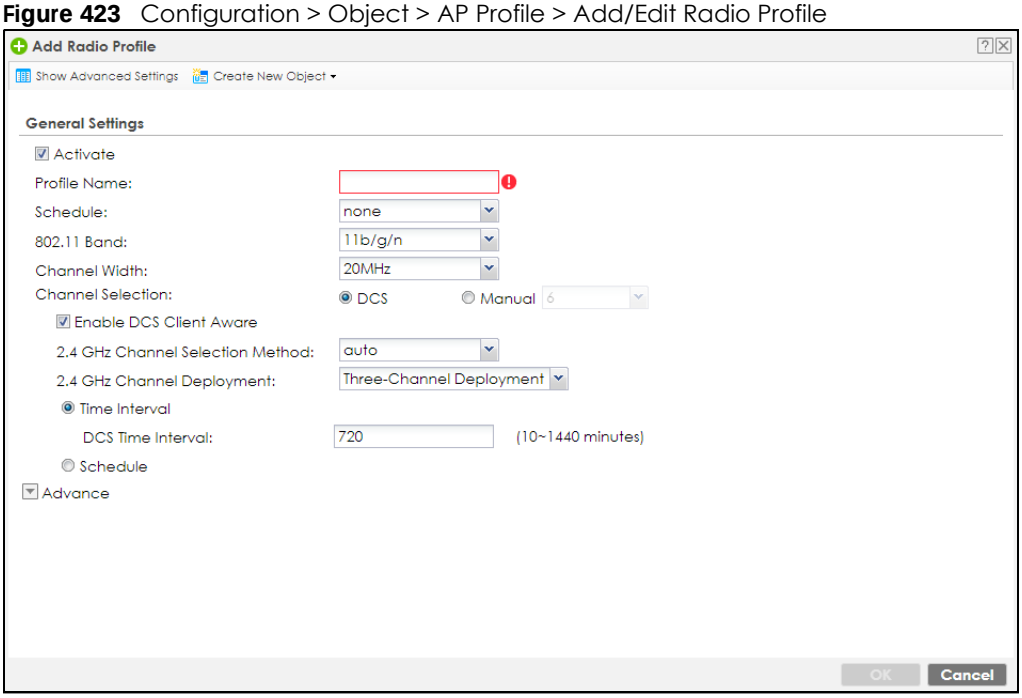
Table 257 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
References	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific profile.
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 radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Schedule	This field displays the schedule object which defines when this radio profile can be used.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.3.1.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

Figure 423 Configuration > Object > AP Profile > Add/Edit Radio Profile



The following table describes the labels in this screen.

Table 258 Configuration > Object > AP Profile > Add/Edit Radio Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the **Advanced Settings** in this window.
Create New Object	Use this to configure any new settings objects that you need to use in this screen.
General Settings	
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
Schedule	This field displays the schedule object which defines when this radio profile can be used.
802.11 Band	Select how to let wireless clients connect to the AP. • **11b/g**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the AP. The AP adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **11b/g/n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the AP. The transmission rate of your AP might be reduced. • **11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the AP. • **11a/n**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the AP. The transmission rate of your AP might be reduced. • **11ac**: allows only IEEE802.11ac compliant WLAN devices to associate with the AP. Note: If you select **11ac** but the WLAN devices in the network do not support IEEE 802.11ac, the Zyxel Device automatically sets the AP to use **11a/n**.

Table 258 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Channel Width	Select the wireless channel bandwidth you want the AP to use. A standard 20 MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Because not all devices support 40 MHz and/or 80 MHz channels, select **20/40MHz** or **20/40/80MHz** to allow the AP to adjust the channel bandwidth automatically. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Note: If the environment has poor signal-to-noise (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	Select the wireless channel which this radio profile should use. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned. Select **DCS** to have the AP automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices. Select **Manual** and specify the channels the AP uses.
Enable DCS Client Aware	This field is available when you set **Channel Selection** to **DCS**. Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.
2.4 GHz Channel Selection Method	This field is available when you set **Channel Selection** to **DCS**. Select **auto** to have the AP search for available channels automatically in the 2.4 GHz band. The available channels vary depending on what you select in the **2.4 GHz Channel Deployment** field. Select **manual** and specify the channels the AP uses in the 2.4 GHz band.
Channel ID	This field is available only when you set **Channel Selection** to **DCS** and set **2.4 GHz Channel Selection Method** to **manual**. Select the check boxes of the channels that you want the AP to use.
Time Interval	Select this option to have the AP survey the other APs within its broadcast radius at the end of the specified time interval.
DCS Time Interval	This field is available when you set **Channel Selection** to **DCS**. Enter a number of minutes. This regulates how often the AP surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the AP will then dynamically select the next available clean channel or a channel with lower interference.
Schedule	Select this option to have the AP survey the other APs within its broadcast radius at a specific time on selected days of the week.

Table 258 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Start Time	Specify the time of the day (in 24-hour format) to have the AP use DCS to automatically scan and find a less-used channel.
Week Days	Select each day of the week to have the AP use DCS to automatically scan and find a less-used channel.
2.4 GHz Channel Deployment	This field is available only when you set **Channel Selection** to **DCS** and set **2.4 GHz Channel Selection Method** to **auto**. Select **Three-Channel Deployment** to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum. Note: For US and Canada models, country code is fixed to US or Canada respectively and is not user selectable.
Enable 5 GHz DFS Aware	This field is available only when you select **11a**, **11a/n** or **11ac** in the **802.11 Band** field. Select this if your APs are operating in an area known to have RADAR devices. This allows the device to downgrade its frequency to below 5 GHz in the event a RADAR signal is detected, thus preventing it from interfering with that signal. Enabling this forces the AP to select a non-DFS channel.
5 GHz Channel Selection Method	This shows **auto** and allows the AP to search for available channels automatically in the 5 GHz band.
Advanced Settings	
Country Code	Select the country code of APs that are connected to the Zyxel Device to be the same as where the Zyxel Device is located/installed. The available channels vary depending on the country you select. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. Note: For US and Canada models, country code is fixed to US or Canada respectively and is not user selectable.
Guard Interval	This field is available only when the channel width is **20/40MHz** or **20/40/80MHz**. Set the guard interval for this radio profile to either **Short** or **Long**. The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.
A-MPDU Limit	Enter the maximum frame size to be aggregated.
A-MPDU Subframe	Enter the maximum number of frames to be aggregated each time.

Table 258 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
A-MSDU Limit	Enter the maximum frame size to be aggregated.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Enable Signal Threshold	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -76 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the Zyxel Device disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -90 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP
Multicast Settings	Use this section to set a transmission mode and maximum rate for multicast traffic.
Transmission Mode	Set how the AP handles multicast traffic. Select **Multicast to Unicast** to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select **Fixed Multicast Rate** to send wireless multicast traffic at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate (Mbps)	If you set the multicast transmission mode to fixed multicast rate, set the data rate for multicast traffic here. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.

Table 258 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.3.2 SSID Screen

The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

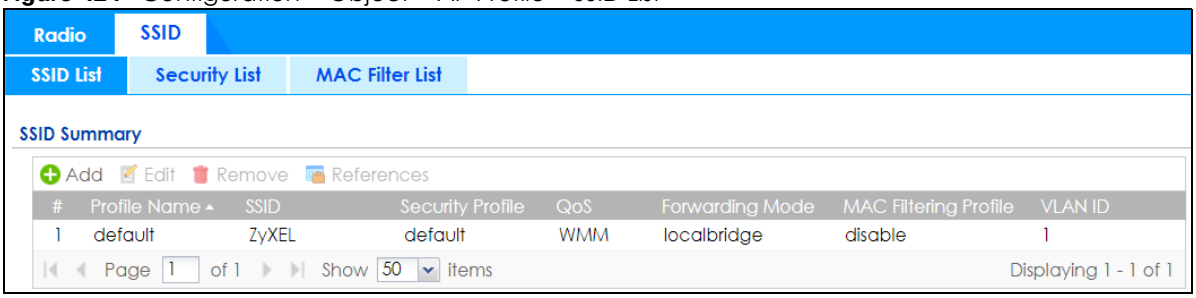
35.3.2.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click **Configuration > Object > AP Profile > SSID**.

Note: You can have a maximum of 32 SSID profiles on the Zyxel Device.

Figure 424 Configuration > Object > AP Profile > SSID List



The following table describes the labels in this screen.

Table 259 Configuration > Object > AP Profile > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile.
References	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.

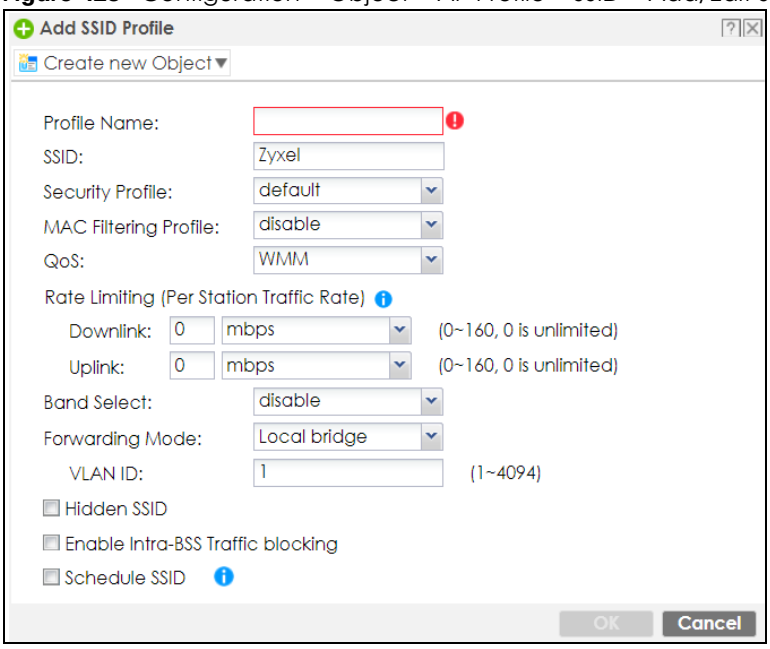
Table 259 Configuration > Object > AP Profile > SSID List (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	This field indicates which (if any) MAC Filter Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

35.3.2.2 Add/Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the **Add** button or select an SSID profile from the list and click the **Edit** button.

Figure 425 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile



The following table describes the labels in this screen.

Table 260 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.

Table 260 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The **disable** setting means no MAC filtering is used.
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: **disable**: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. **WMM**: Enables automatic tagging of data packets. The Zyxel Device assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. **WMM_VOICE**: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. **WMM_VIDEO**: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. **WMM_BEST_EFFORT**: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. **WMM_BACKGROUND**: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.
Rate Limiting (Per Station Traffic Rate)	Define the maximum incoming and outgoing transmission data rate per wireless station
Downlink:	Define the maximum incoming transmission data rate (either in Mbps or Kbps) on a per-station basis.
Uplink:	Define the maximum outgoing transmission data rate (either in Mbps or Kbps) on a per-station basis.
Band Select:	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings. Select **standard** to have the AP try to connect the wireless clients to the same SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are still allowed. Otherwise, select **disable** to turn off this feature.
Stop Threshold	This field is not available when you disable **Band Select**. Select this option and set the threshold number of the connected wireless clients at which the Zyxel Device disables the band select feature.
Balance Ratio	This field is not available when you disable **Band Select**. Select this option and set a ratio of the wireless clients using the 5 GHz band to the wireless clients using the 2.4 GHz band.
Forwarding Mode	Select a forwarding mode (**Tunnel** or **Local bridge**) for traffic from this SSID.

Table 260 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
VLAN ID	If you selected **Local Bridge** forwarding mode, enter the VLAN ID that will be used to tag all traffic originating from this SSID if the VLAN is different from the native VLAN. All the wireless station's traffic goes through the associated AP's gateway.
VLAN Interface	If you selected the **Tunnel** forwarding mode, select a VLAN interface. All the wireless station's traffic is forwarded to the Zyxel Device first.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID.
Schedule SSID	Select this option and set whether the SSID is enabled or disabled on each day of the week. You also need to select the hour and minute (in 24-hour format) to specify the time period of each day during which the SSID is enabled/enabled.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

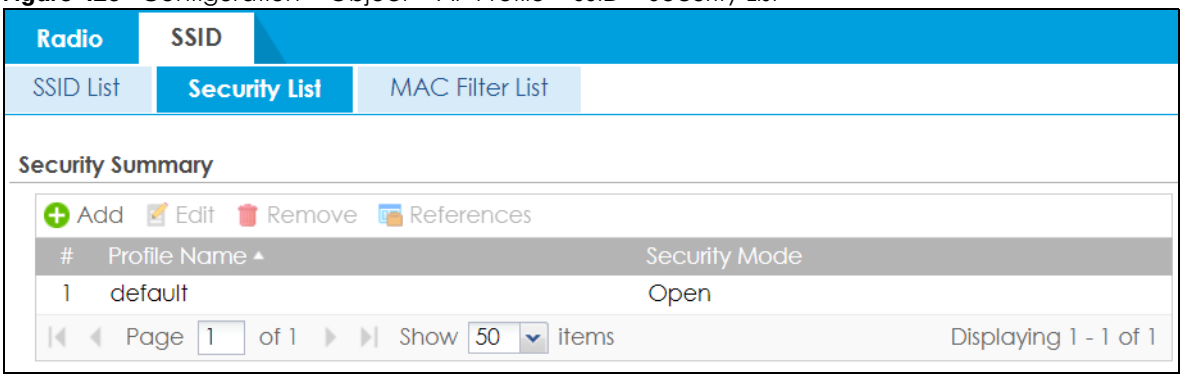
35.3.2.3 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

Note: You can have a maximum of 32 security profiles on the Zyxel Device.

Figure 426 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 261 Configuration > Object > AP Profile > SSID > Security List

LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.

Table 261 Configuration > Object > AP Profile > SSID > Security List (continued)

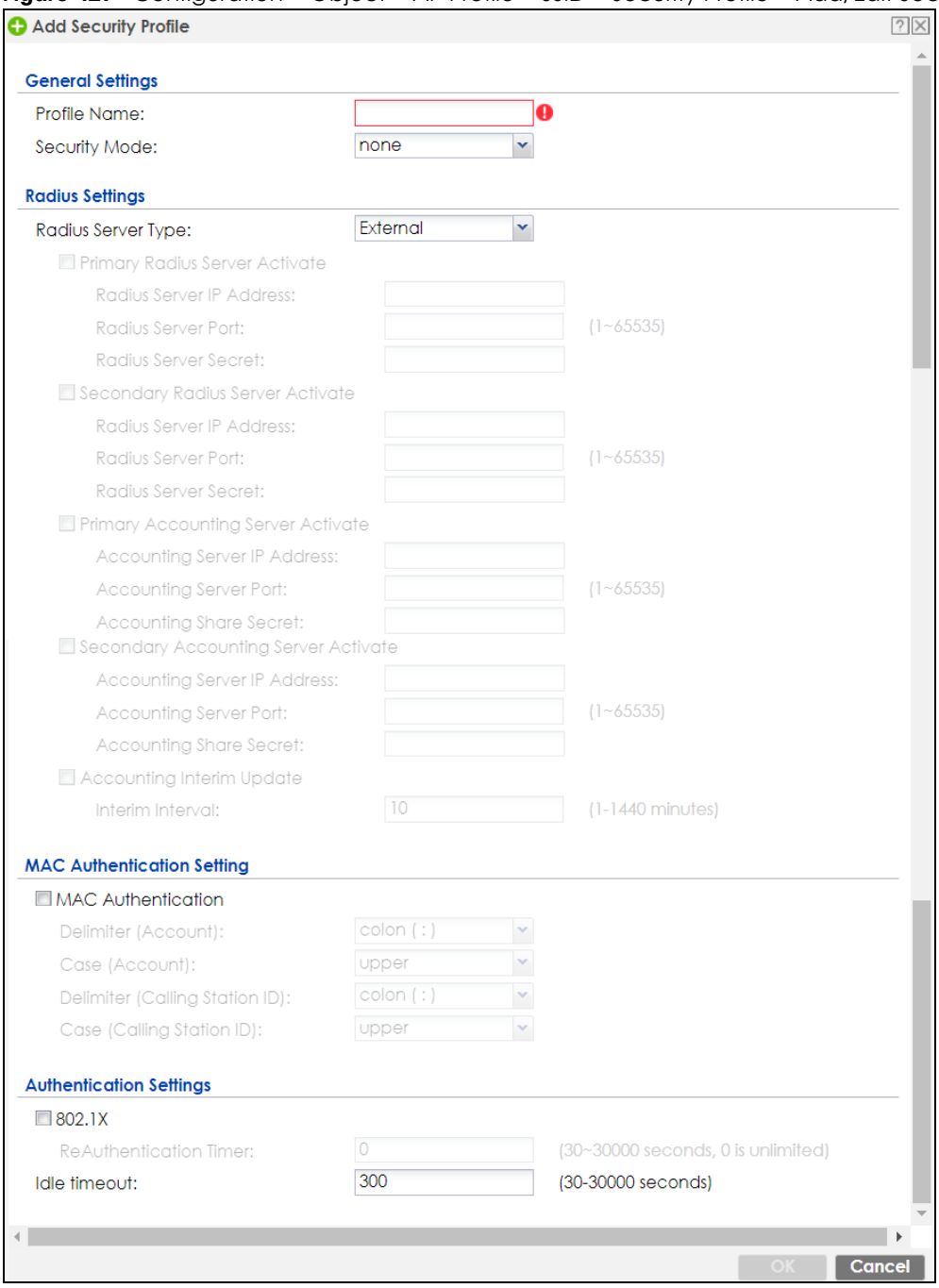
LABEL	DESCRIPTION
References	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

35.3.2.4 Add/Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

Note: This screen's options change based on the **Security Mode** selected. Only the default screen is displayed here.

Figure 427 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile



The following table describes the labels in this screen.

Table 262 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: **none**, **wep**, **wpa2**, or **wpa2-mix**.
Fast Roaming Settings	IEEE 802.11r fast roaming, which is also known as Fast BSS Transition (FT), allows wireless clients to quickly move from one AP to another in a WiFi network that uses WPA2 with 802.1x authentication. Information from the original association is passed to the target AP when the client roams. The client doesn't need to perform the whole 802.1x authentication process. Messages exchanged between the target AP and client are reduced and performed using one of the two methods: • Over-the-DS: The wireless client communicates with the target AP via the current AP. The communication is sent to the target AP through the wired Ethernet connection. • Over-the-Air: The wireless client communicates directly with the target AP.
802.11r	Select this to turn on IEEE 802.11r fast roaming on the AP (Zyxel Device). This is good for wireless clients that transport a lot of real-time interactive traffic, such as voice and video. Wireless clients should also support WPA2 and fast roaming to associate with the AP (Zyxel Device) and roam seamlessly.
Radius Server Type	Select **Internal** to use the Zyxel Device's internal authentication database, or **External** to use an external RADIUS server for authentication.
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the AP. The key must be the same on the external accounting server and your AP. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external accounting server. Select this to have the AP send accounting update messages to the accounting server at the interval you specify.
Interim Interval	Specify the time interval for how often the AP is to send an interim update message with current client statistics to the accounting server.
MAC Authentication	Select this to use an external server or the Zyxel Device's local database to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. An external server can use the wireless client's account (username/password) or Calling Station ID for MAC authentication. Configure the ones the external server uses.
Delimiter (Account)	Select the separator the external server uses for the two-character pairs within account MAC addresses.

Table 262 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Case (Account)	Select the case (**upper** or **lower**) the external server requires for letters in the account MAC addresses.
Delimiter (Calling Station ID)	RADIUS servers can require the MAC address in the Calling Station ID RADIUS attribute. Select the separator the external server uses for the pairs in calling station MAC addresses.
Case (Calling Station ID)	Select the case (**upper** or **lower**) the external server requires for letters in the calling station MAC addresses.
802.1X	Select this to enable 802.1x secure authentication.
Auth. Method	This field is available only when you set the RADIUS server type to **Internal**. Select an authentication method if you have created any in the **Configuration > Object > Auth. Method** screen.
Reauthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
The following fields are available if you set **Security Mode** to **wep**.	
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are **Open** or **Share** key.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select **WEP-64**: • Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each **Key** used. or • Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each **Key** used. If you select **WEP-128**: • Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each **Key** used. or • Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each **Key** used.
Key 1~4	Based on your **Key Length** selection, enter the appropriate length hexadecimal or ASCII key.
The following fields are available if you set **Security Mode** to **wpa**, **wpa2** or **wpa2-mix**.	
PSK	Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • **tkip** - This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.

Table 262 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

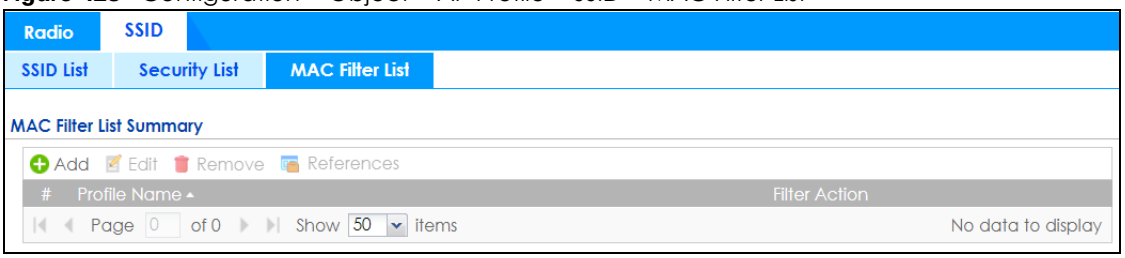
LABEL	DESCRIPTION
Management Frame Protection	This field is available only when you select **wpa2** or **wpa2-mix** in the **Security Mode** field and set **Cipher Type** to **aes**. Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. Select **Optional** if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select **Required** and wireless clients must support MFP in order to join the AP's wireless network.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.3.2.5 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Note: You can have a maximum of 32 MAC filtering profiles on the Zyxel Device.

Figure 428 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

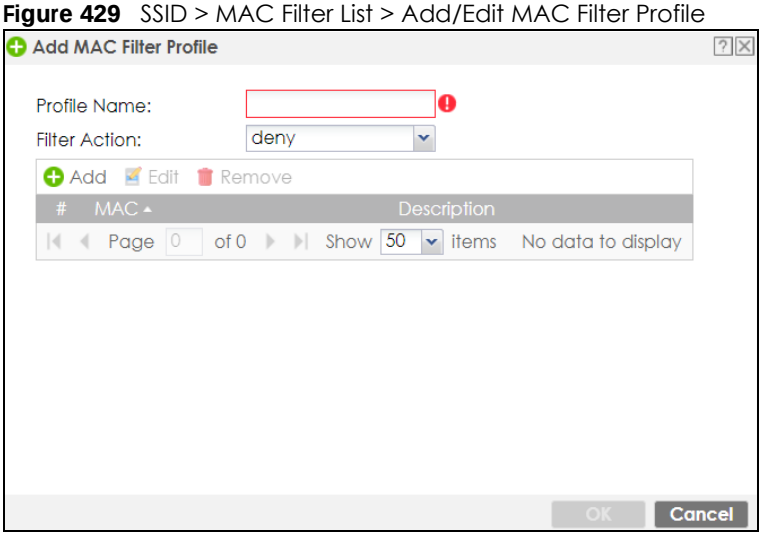
Table 263 Configuration > Object > AP Profile > SSID > MAC Filter List

LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
References	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

35.3.2.6 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Figure 429 SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 264 SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select **allow** to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select **deny** to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific profile.
MAC	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.4 MON Profile

35.4.1 Overview

This screen allows you to set up monitor mode configurations that allow your connected APs to scan for other wireless devices in the vicinity. Once detected, you can use the **Rogue AP** screen (Section 8.4 on page 205) to classify them as either rogue or friendly and then manage them accordingly.

The **MON Profile** screen (Section 35.4.2 on page 649) creates preset monitor mode configurations that can be used by the APs.

35.4.1.1 What You Need To Know

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

Active Scan

An active scan is performed when an 802.11-compatible wireless monitoring device is explicitly triggered to scan a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies by sending probe request frames.

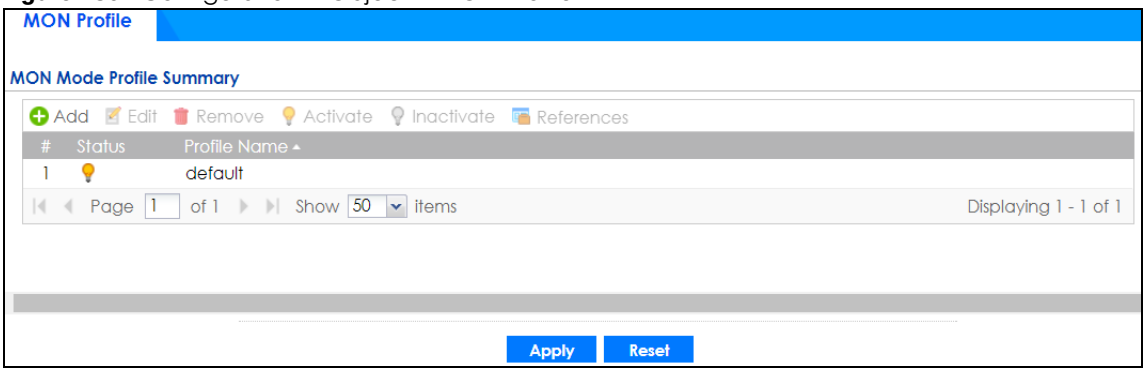
Passive Scan

A passive scan is performed when an 802.11-compatible monitoring device is set to periodically listen to a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies.

35.4.2 Configuring MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, login to the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 430 Configuration > Object > MON Profile



The following table describes the labels in this screen.

Table 265 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
References	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific user.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.

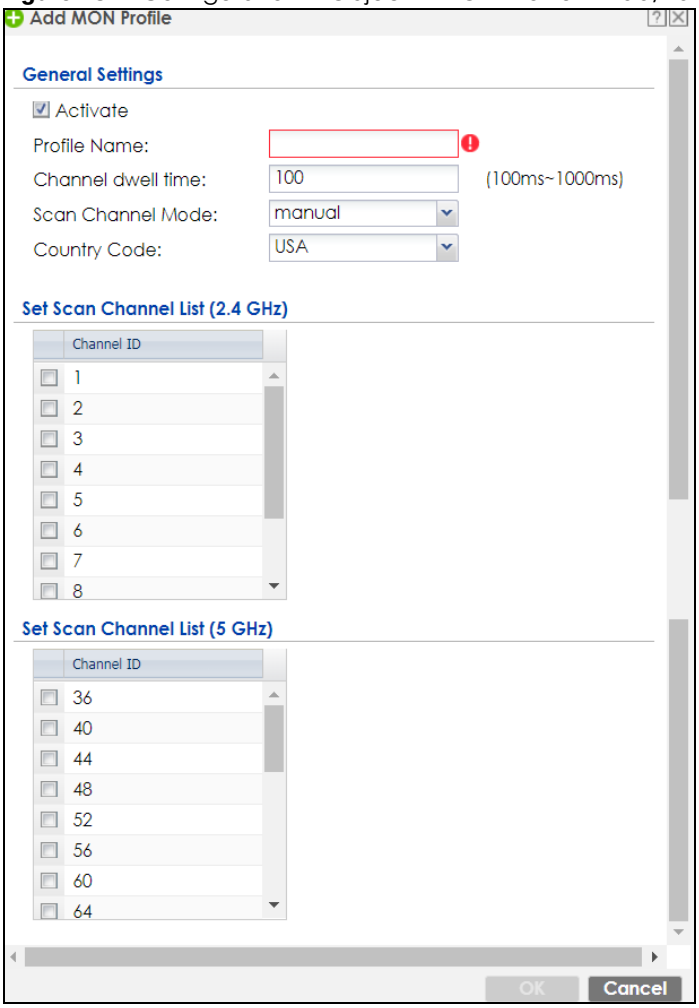
Table 265 Configuration > Object > MON Profile (continued)

LABEL	DESCRIPTION
Profile Name	This field indicates the name assigned to the monitor profile.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.4.3 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select and existing monitor mode profile and click the **Edit** button.

Figure 431 Configuration > Object > MON Profile > Add/Edit MON Profile



The following table describes the labels in this screen.

Table 266 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.

Table 266 Configuration > Object > MON Profile > Add/Edit MON Profile (continued)

LABEL	DESCRIPTION
Channel dwell time	Enter the interval (in milliseconds) before the AP switches to another channel for monitoring.
Scan Channel Mode	Select **auto** to have the AP switch to the next sequential channel once the **Channel dwell time** expires. Select **manual** to set specific channels through which to cycle sequentially when the **Channel dwell time** expires. Selecting this options makes the **Scan Channel List** options available.
Country Code	Select the country code of APs that are connected to the Zyxel Device to be the same as where the Zyxel Device is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. Note: For US and Canada models, country code is fixed to US or Canada respectively and is not user selectable.
Set Scan Channel List (2.4 GHz)	Move a channel from the **Available channels** column to the **Channels selected** column to have the APs using this profile scan that channel when **Scan Channel Mode** is set to manual. These channels are limited to the 2 GHz range (802.11 b/g/n).
Set Scan Channel List (5 GHz)	Move a channel from the **Available channels** column to the **Channels selected** column to have the APs using this profile scan that channel when **Scan Channel Mode** is set to manual. These channels are limited to the 5 GHz range (802.11 a/n).
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

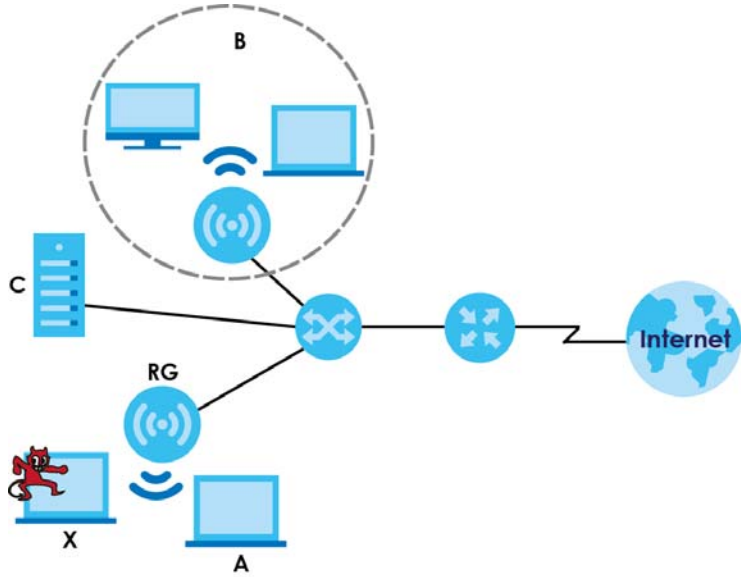
35.4.4 Technical Reference

The following section contains additional technical information about the features described in this chapter.

Rogue APs

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network, or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Figure 432 Rogue AP Example



In the example above, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Friendly APs

If you have more than one AP in your wireless network, you should also configure a list of "friendly" APs. Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from recognized networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points.

35.5 ZyMesh Overview

This section shows you how to configure ZyMesh profiles for the Zyxel Device to apply to the managed APs.

ZyMesh is a Zyxel proprietary protocol that creates wireless mesh links between managed APs to expand the wireless network. Managed APs can provide services or forward traffic between the Zyxel Device and wireless clients. ZyMesh also allows the Zyxel Device to use CAPWAP to automatically update the configuration settings on the managed APs (in repeater mode) through wireless connections. The managed APs (in repeater mode) are provisioned hop by hop.

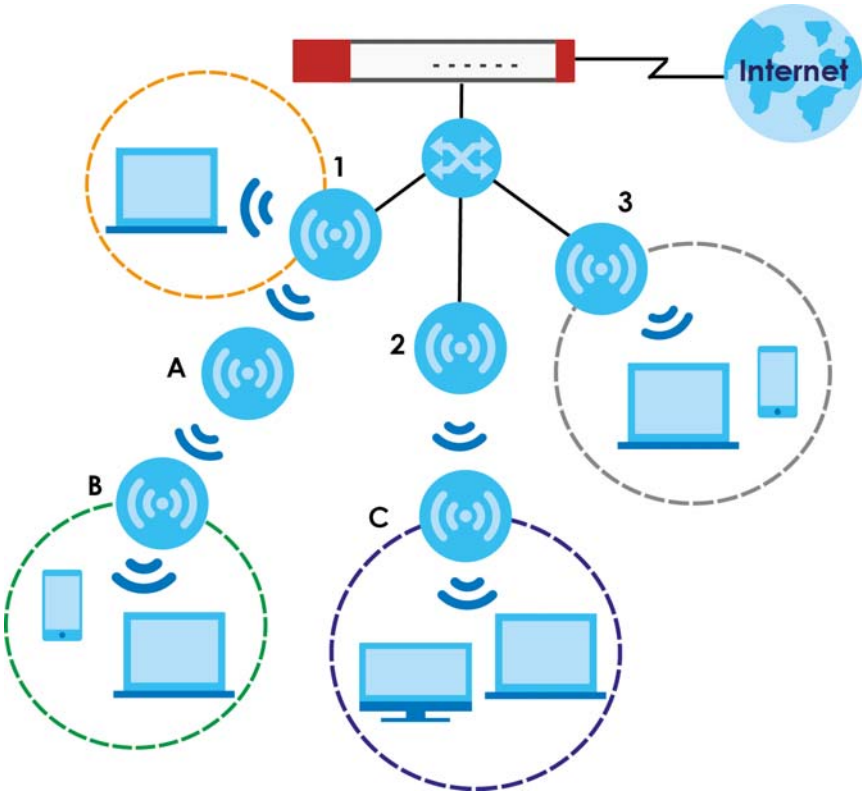
The managed APs in a ZyMesh must use the same SSID, channel number and pre-shared key. A manged AP can be either a root AP or repeater in a ZyMesh.

Note: All managed APs should be connected to the Zyxel Device directly to get the configuration file before being deployed to build a ZyMesh. Ensure you restart the managed AP after you change its operating mode using the **Configuration > Wireless > AP Management** screen (see Section 8.3 on page 193).

- Root AP: a managed AP that can transmit and receive data from the Zyxel Device via a wired Ethernet connection.
- Repeater: a managed AP that transmits and/or receives data from the Zyxel Device via a wireless connection through a root AP.

Note: When managed APs are deployed to form a ZyMesh for the first time, the root AP must be connected to an AP controller (the Zyxel Device).

In the following example, managed APs **1** and **2** act as a root AP and managed APs **A**, **B** and **C** are repeaters.



The maximum number of hops (the repeaters between a wireless client and the root AP) you can have in a ZyMesh varies according to how many wireless clients a managed AP can support.

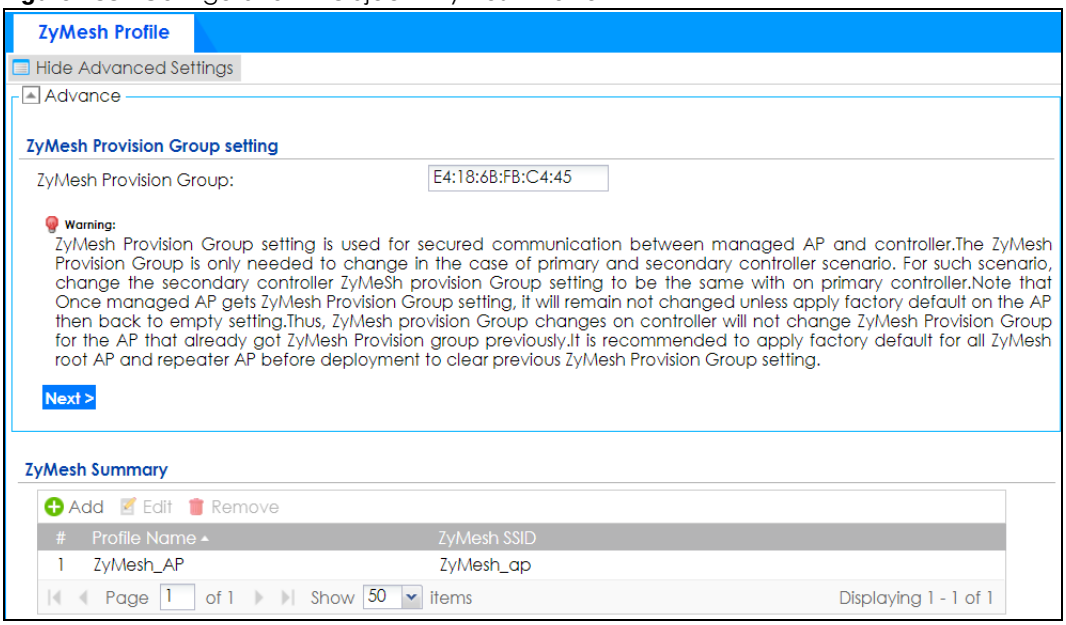
Note: A ZyMesh link with more hops has lower throughput.

Note: When the wireless connection between the root AP and the repeater is up, in order to prevent bridge loops, the repeater would not be able to transmit data through its Ethernet port(s). The repeater then could only receive power from a PoE device if you use PoE to provide power to the managed AP via an 8-ping Ethernet cable.

35.5.1 ZyMesh Profile

This screen allows you to manage and create ZyMesh profiles that can be used by the APs. To access this screen, click **Configuration > Object > ZyMesh Profile**.

Figure 433 Configuration > Object > ZyMesh Profile



The following table describes the labels in this screen.

Table 267 Configuration > Object > ZyMesh Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to display a greater or lesser number of configuration fields.
ZyMesh Provision Group	By default, this shows the MAC address used by the Zyxel Device's first Ethernet port. Say you have two AP controllers (Zyxel Devices) in your network and the primary AP controller is not reachable. You may want to deploy the second/backup AP controller in your network to replace the primary AP controller. In this case, it is recommended that you enter the primary AP controller's **ZyMesh Provision Group** MAC address in the second AP controller's **ZyMesh Provision Group** field. If you didn't change the second AP controller's MAC address, managed APs in an existing ZyMesh can still access the networks through the second AP controller and communicate with each other. But new managed APs will not be able to communicate with the managed APs in the existing ZyMesh, which is set up with the primary AP controller's MAC address. To allow all managed APs to communicate in the same ZyMesh, you can just set the second AP controller to use the primary AP controller's MAC address. Otherwise, reset all managed APs to the factory defaults and set up a new ZyMesh with the second AP controller's MAC address.
Next	Click this button and follow the on-screen instructions to update the AP controller's MAC address.
Add	Click this to add a new profile.
Edit	Click this to edit the selected profile.
Remove	Click this to remove the selected profile.
#	This field is a sequential value, and it is not associated with a specific profile.

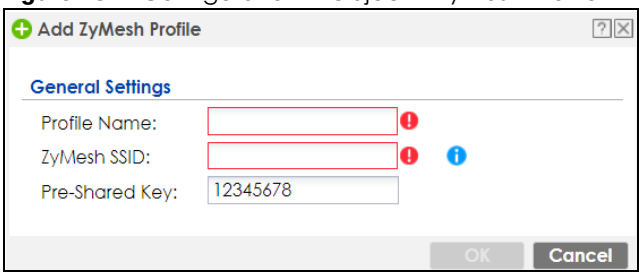
Table 267 Configuration > Object > ZyMesh Profile (continued)

LABEL	DESCRIPTION
Profile Name	This field indicates the name assigned to the profile.
ZyMesh SSID	This field shows the SSID specified in this ZyMesh profile.

35.5.2 Add/Edit ZyMesh Profile

This screen allows you to create a new ZyMesh profile or edit an existing one. To access this screen, click the **Add** button or select and existing profile and click the **Edit** button.

Figure 434 Configuration > Object > ZyMesh Profile > Add/Edit ZyMesh Profile



The following table describes the labels in this screen.

Table 268 Configuration > Object > ZyMesh Profile > Add/Edit ZyMesh Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name.
ZyMesh SSID	Enter the SSID with which you want the managed AP to connect to a root AP or repeater to build a ZyMesh link. Note: The ZyMesh SSID is hidden in the outgoing beacon frame so a wireless device cannot obtain the SSID through scanning using a site survey tool.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. The key is used to encrypt the wireless traffic between the APs.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.6 Address/Geo IP Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

- The **Address** screen (Section 35.6.2 on page 656) provides a summary of all addresses in the Zyxel Device. Use the **Address Add/Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen (Section 35.6.3 on page 660) and the **Address Group Add/Edit** screen, to maintain address groups in the Zyxel Device.
- Use the **Geo IP** screen (Section 35.6.4 on page 662) to update the database of country-to-IP address mappings and to manually configure country-to-IP address mappings.

35.6.1 What You Need To Know

Address objects and address groups are used in dynamic routes, security policies, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

35.6.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects:

- **HOST** - the object uses an **IP Address to define a** host address
- **RANGE** - the object uses a range address defined by a **Starting IP Address** and an **Ending IP Address**
- **SUBNET** - the object uses a network address defined by a **Network** IP address and **Netmask** subnet mask
- **INTERFACE IP** - the object uses the IP address of one of the Zyxel Device's interfaces
- **INTERFACE SUBNET** - the object uses the subnet mask of one of the Zyxel Device's interfaces
- **INTERFACE GATEWAY** - the object uses the gateway IP address of one of the Zyxel Device's interfaces
- **GEOGRAPHY** - the object uses the IP addresses of a country to represent a country

FQDN - the object uses a FQDN (Fully Qualified Domain Name). An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. mail.myZyxel.com.tw is also an FQDN, where "mail" is the host, "myZyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.

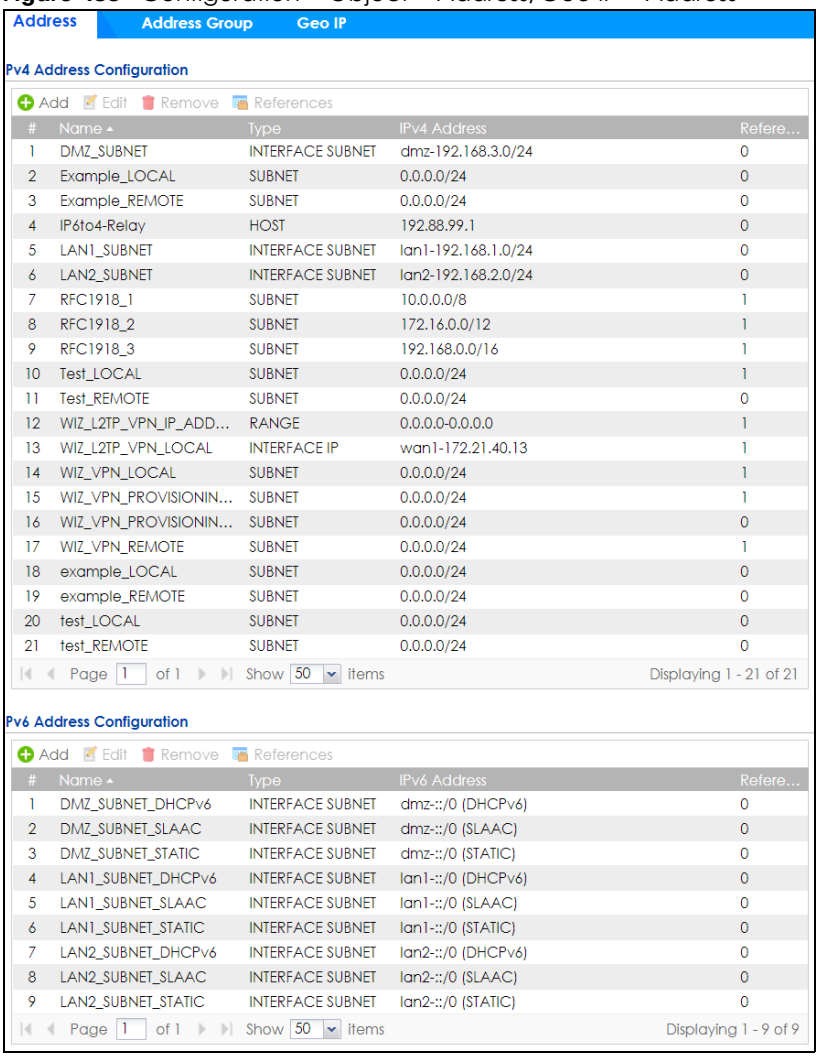
Table 269 FQDN Example

HTTP://	WWW.	ZYXEL.	COM
	host name	second-level domain name	top-level domain name
	FQDN		
Uniform Resource Locator (URL)			

In an address FQDN object, you can also use one wildcard. For example, *.zyxel.com. An FQDN is resolved to its IP address using the DNS server configured on the Zyxel Device.

The **Address** screen provides a summary of all addresses in the Zyxel Device. To access this screen, click **Configuration > Object** > **Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 435 Configuration > Object > Address/Geo IP > Address



The following table describes the labels in this screen. See Section 35.6.2.1 on page 658 for more information as well.

Table 270 Configuration > Object > Address/Geo IP > Address

LABEL	DESCRIPTION
IPv4 Address Configuration	
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 address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the Zyxel Device's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the Zyxel Device's interfaces, the name of the interface displays first followed by the object's current address settings.

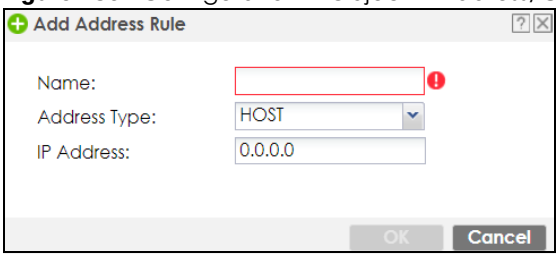
Table 270 Configuration > Object > Address/Geo IP > Address (continued)

LABEL	DESCRIPTION
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Configuration	
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 address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the Zyxel Device's interfaces.
IPv6 Address	This field displays the IPv6 addresses represented by each address object. If the object's settings are based on one of the Zyxel Device's interfaces, the name of the interface displays first followed by the object's current address settings.
Reference	This displays the number of times an object reference is used in a profile.

35.6.2.1 IPv4 Address Add/Edit Screen

The **Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 35.6.2 on page 656), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Configuration** section.

Figure 436 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4) t



The following table describes the labels in this screen.

Table 271 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.

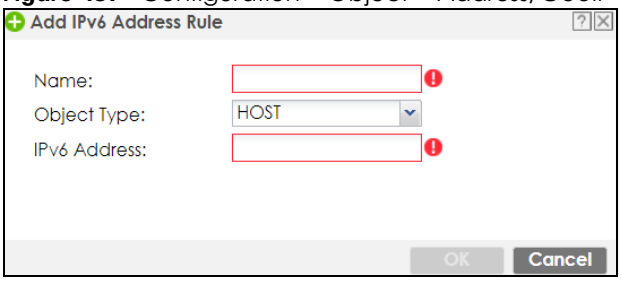
Table 271 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)

LABEL	DESCRIPTION
Ending IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents.
Region	If you selected **GEOGRAPHY** as the **Address Type**, use this field to select a country or continent. A **GEOGRAPHY** object uses the data from the country-to-IP/continent-to-IP address database. Go to the **Configuration** > **Object** > **Address/Geo IP** > **Geo IP** screen to configure the custom country-to-IP/continent-to-IP address mappings for a **GEOGRAPHY** object.
Country	If you selected **Geography** as the **Address Type**, use this field to select a country.
FQDN	If you selected **FQDN** as the **Address Type**, use this field to enter a fully qualified domain name.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.6.2.2 IPv6 Address Add/Edit Screen

The **Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 35.6.2 on page 656), and click either the **Add** icon or an **Edit** icon in the **IPv6 Address Configuration** section.

Figure 437 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)



The following table describes the labels in this screen.

Table 272 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Object Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
IPv6 Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.

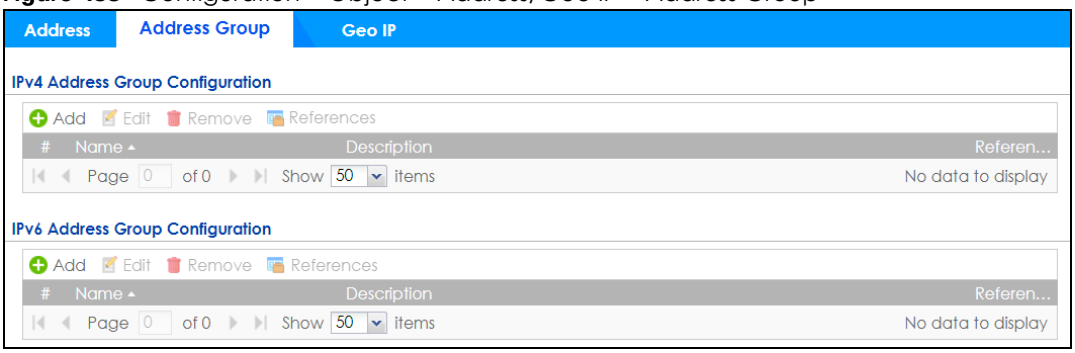
Table 272 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)

LABEL	DESCRIPTION
IPv6 Starting Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
IPv6 Ending Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
IPv6 Address Prefix	This field is only available if the **Address Type** is **SUBNET**. This field cannot be blank. Enter the IPv6 address prefix that the Zyxel Device uses for the LAN IPv6 address.
Interface	If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents.
IPv6 Address Type	Select whether the IPv6 address is a link-local IP address (**LINK LOCAL**), static IP address (**STATIC**), an IPv6 StateLess Address Auto Configuration IP address (**SLAAC**), or is obtained from a DHCPv6 server (**DHCPv6**).
Region	If you selected **Geography** as the **Address Type**, use this field to select a country or continent.
FQDN	If you selected **FQDN** as the **Address Type**, use this field to enter a fully qualified domain name.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.6.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Configuration > Object** > **Address/Geo IP > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 438 Configuration > Object > Address/Geo IP > Address Group



The following table describes the labels in this screen. See Section 35.6.3.1 on page 661 for more information as well.

Table 273 Configuration > Object > Address/Geo IP > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
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 address group.
Name	This field displays the name of each address group.

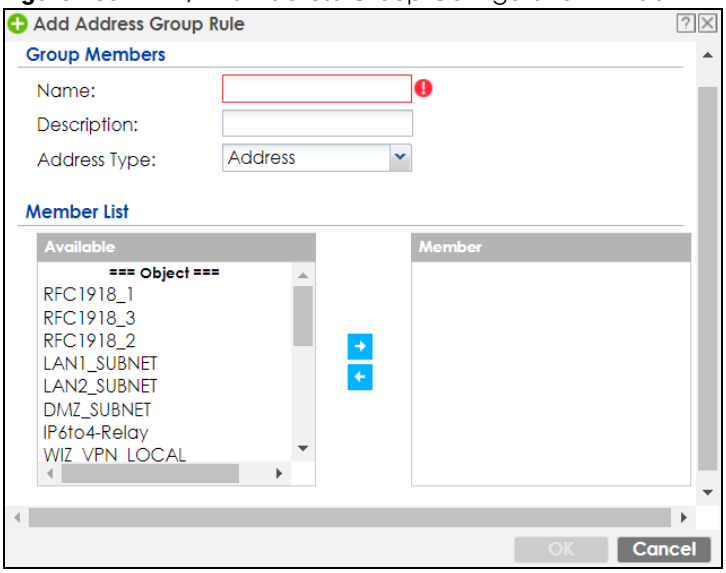
Table 273 Configuration > Object > Address/Geo IP > Address Group (continued)

LABEL	DESCRIPTION
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Group Configuration	
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 address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.

35.6.3.1 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see Section 35.6.3 on page 660), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Group Configuration** or **IPv6 Address Group Configuration** section.

Figure 439 IPv4/IPv6 Address Group Configuration > Add



The following table describes the labels in this screen.

Table 274 IPv4/IPv6 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.

Table 274 IPv4/IPv6 Address Group Configuration > Add (continued)

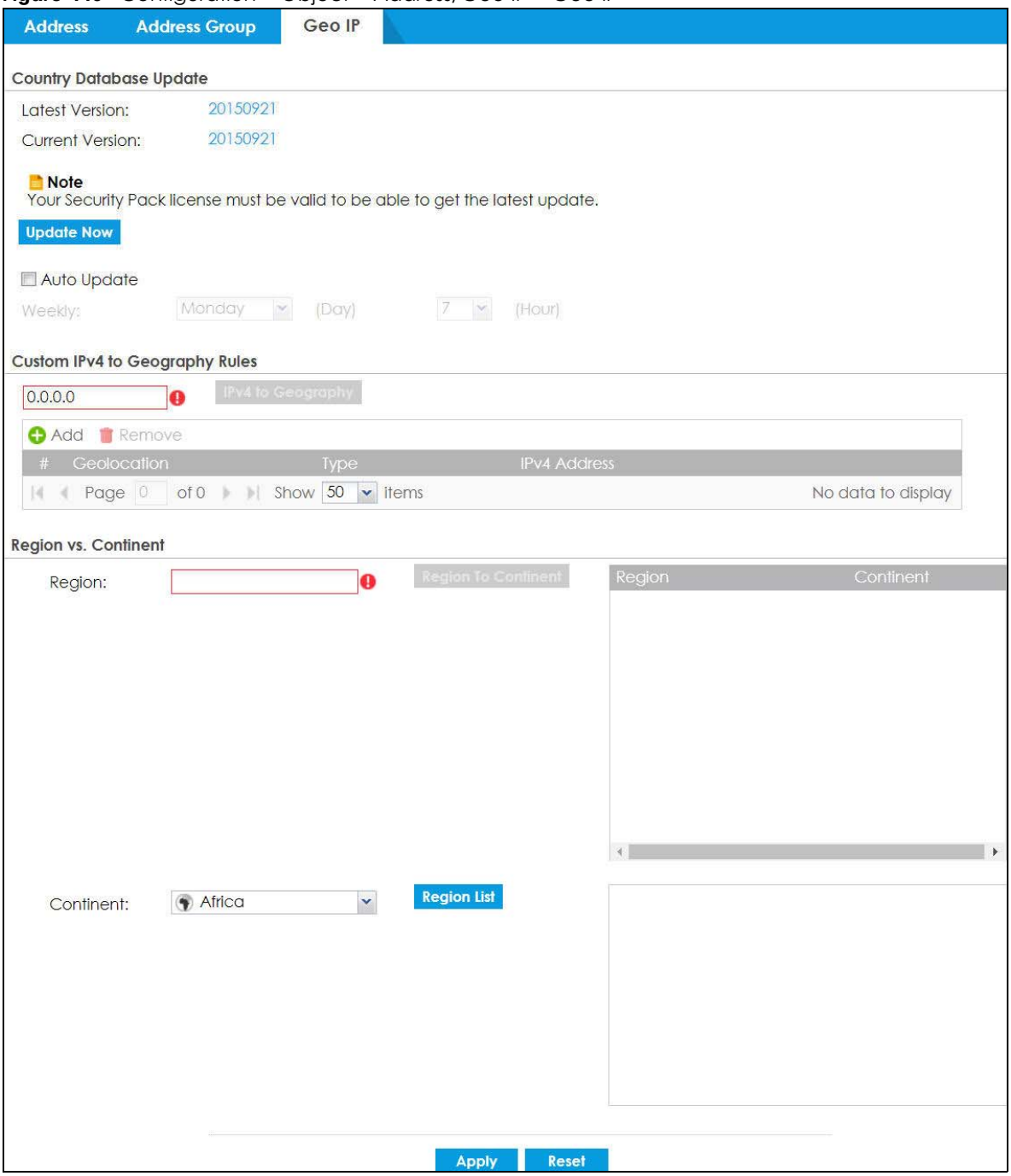
LABEL	DESCRIPTION
Address Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
Member List	The **Member** list displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list. Note: Only objects of the same address type can be added to a address group.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.6.4 Geo IP Summary Screen

Use this screen to update the database of country-to-IP and continent-to-IP address mappings and manually configure custom country-to-IP and continent-to-IP address mappings in geographic address objects. You can then use geographic address objects in security policies to forward or deny traffic to whole countries or regions.

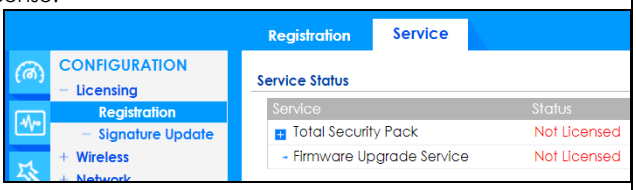
Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 440 Configuration > Object > Address/Geo IP > Geo IP



The following table describes the labels in this screen.

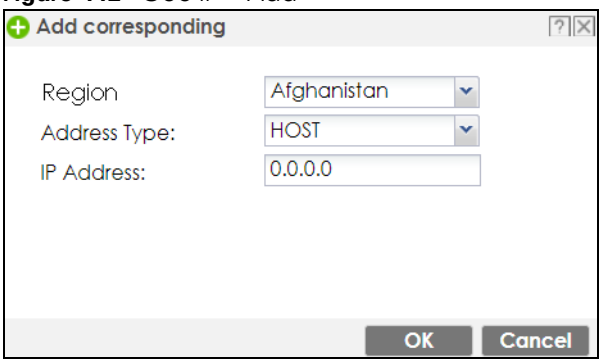
Table 275 Configuration > Object > Address/Geo IP > Geo IP

LABEL	DESCRIPTION
Country Database Update	
Latest Version	This is the latest country-to-IP address database version on myZyxel. You need to have a registered Content Filter Service license. 
Current Version	This is the country-to-IP address database version currently on the Zyxel Device.
Update Now	Click this to check for the latest country-to-IP address database version on myZyxel. The latest version is downloaded to the Zyxel Device and replaces the current version if it is newer. There are logs to show the update status. You need to have a registered Content Filter Service license.
Auto Update	If you want the Zyxel Device to check weekly for the latest country-to-IP address database version on myZyxel, select the checkbox, choose a day and time each week and then click **Apply**. The default day and time displayed is the Zyxel Device current day and time.
Custom IPv4/IPv6 to Geography Rules	
IPv4/IPv6 to Geography	Enter an IP address, then click this button to query which country this IP address belongs to.
Add	Click this to create a new entry.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Geolocation	This field displays the name of the country or region that is associated with this IP address.
Type	This field displays whether this address object is **HOST**, **RANGE** or **SUBNET.**
IPv4/IPv6 Address	This field displays the IPv4/IPv6 addresses represented by the type of address object.
Region vs. Continent	
Region	Enter a country name, then click the **Region to Continent** button to query which continent this country belongs to.
Continent	Select a continent, then click the **Region List** button to query which countries belong to the continent.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.6.4.1 Add Custom IPv4/IPv6 Address to Geography Screen

This screen allows you to create a new geography-to-IP address mapping. To access this screen, go to the **Geo IP** screen (see Section 35.6.4 on page 662), and click the **Add** icon in the **Custom IPv4 to Geography Rules** or **Custom IPv6 to Geography Rules** section.

Figure 441 Geo IP > Add



The following table describes the labels in this screen.

Table 276 Geo IP > Add

LABEL	DESCRIPTION
Region	Select the country or continent that maps to this IP address.
Address Type	Select the type of address you want to create. Choices are: **HOST**, **RANGE**, **SUBNET**.
IP Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
IP Starting Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
IP Ending Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network / Netmask	These fields are only available if the IPv4 **Address Type** is **SUBNET**. They cannot be blank. Enter the network IP and subnet mask that defines the IPv4 subnet.
IPv6 Address Prefix	This field is only available if the IPv6 **Address Type** is **SUBNET**. This field cannot be blank. Enter the IPv6 address prefix that the Zyxel Device uses for the LAN IPv6 address.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.7 Service Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

- Use the **Service** screens (Section 35.7.2 on page 666) to view and configure the Zyxel Device's list of services and their definitions.
- Use the **Service Group** screens (Section 35.7.2 on page 666) to view and configure the Zyxel Device's list of service groups.

35.7.1 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, security policies, and IDP profiles.

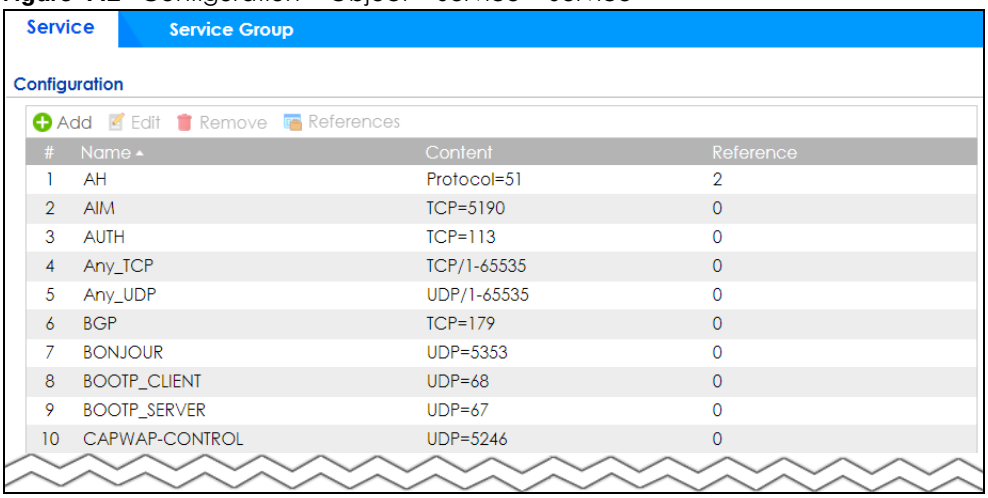
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

35.7.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 442 Configuration > Object > Service > Service



The following table describes the labels in this screen.

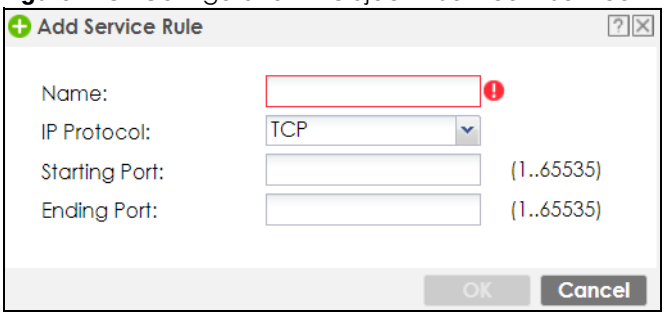
Table 277 Configuration > Object > Service > Service

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 service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.
Reference	This displays the number of times an object reference is used in a profile.

35.7.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see Section 35.7.2 on page 666), and click either the **Add** icon or an **Edit** icon.

Figure 443 Configuration > Object > Service > Service > Edit



The following table describes the labels in this screen.

Table 278 Configuration > Object > Service > Service > Edit

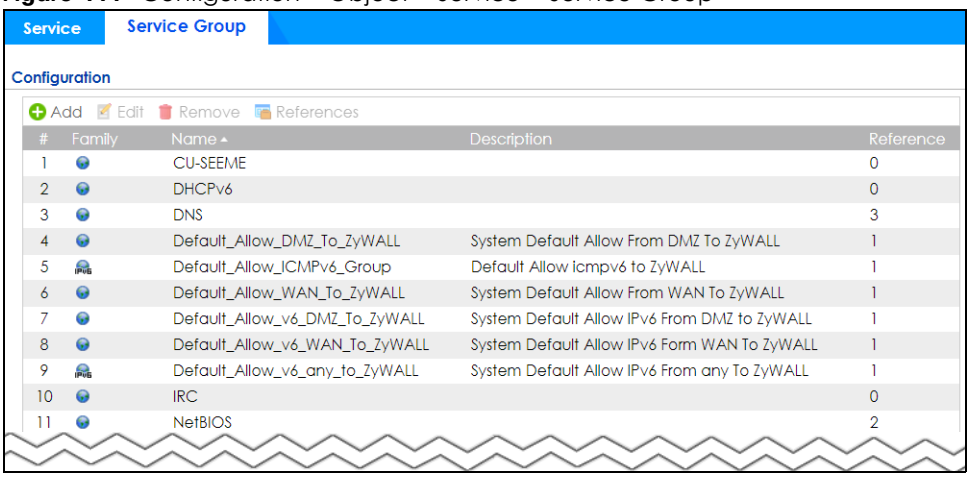
LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **User Defined**.
Starting Port Ending Port	This field appears if the **IP Protocol** is **TCP** or **UDP**. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the **IP Protocol** is **ICMP** or **ICMPv6**. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the **IP Protocol** is **User Defined**. Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.7.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the Web Configurator, and click **Configuration > Object** > **Service** > **Service Group**.

Figure 444 Configuration > Object > Service > Service Group



The following table describes the labels in this screen. See Section 35.7.3.1 on page 669 for more information as well.

Table 279 Configuration > Object > Service > Service Group

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.

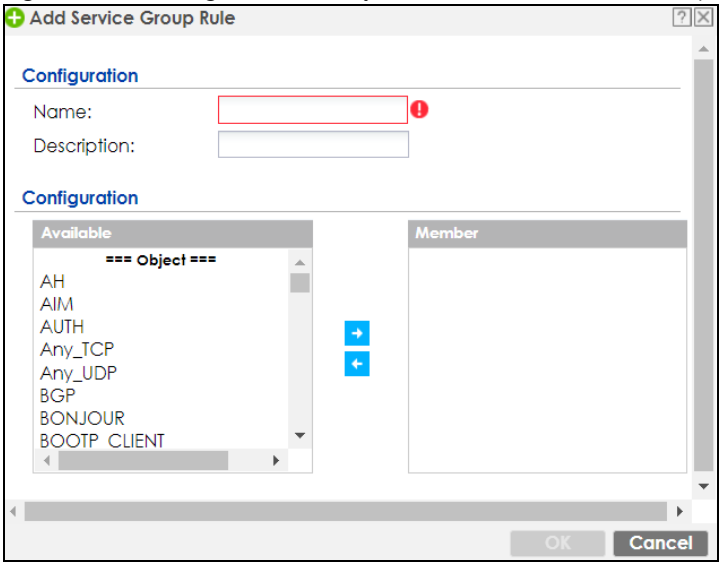
Table 279 Configuration > Object > Service > Service Group (continued)

LABEL	DESCRIPTION
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 service group.
Family	This field displays the Server Group supported type, which is according to your configurations in the **Service Group Add/Edit** screen. There are 3 types of families: • : Supports IPv4 only • : Supports IPv6 only • : Supports both IPv4 and IPv6
Name	This field displays the name of each service group. By default, the Zyxel Device uses services starting with "Default_Allow_" in the security policies to allow certain services to connect to the Zyxel Device.
Description	This field displays the description of each service group, if any.
Reference	This displays the number of times an object reference is used in a profile.

35.7.3.1 The Service Group Add/Edit Screen

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see Section 35.7.3 on page 668), and click either the **Add** icon or an **Edit** icon.

Figure 445 Configuration > Object > Service > Service Group > Edit



The following table describes the labels in this screen.

Table 280 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.

Table 280 Configuration > Object > Service > Service Group > Edit (continued)

LABEL	DESCRIPTION
Configuration	The **Member** list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.8 Schedule Overview

Use schedules to set up one-time and recurring schedules for policy routes, security policies, application patrol, and content filtering. The Zyxel Device supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the Zyxel Device.

Note: Schedules are based on the Zyxel Device's current date and time.

- Use the **Schedule** summary screen (Section 35.8.2 on page 670) to see a list of all schedules in the Zyxel Device.
- Use the **One-Time Schedule Add/Edit** screen (Section 35.8.2.1 on page 671) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen (Section 35.8.2.2 on page 672) to create or edit a recurring schedule.
- Use the Schedule Group screen (Section 35.8.3 on page 673) to merge individual schedule objects as one object.

35.8.1 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

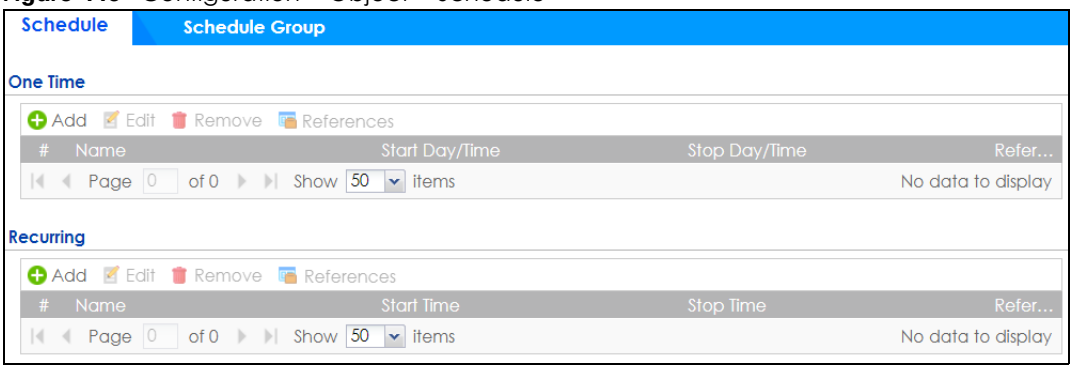
Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

35.8.2 The Schedule Screen

The **Schedule** screen provides a summary of all schedules in the Zyxel Device. To access this screen, click **Configuration > Object** > **Schedule**.

Figure 446 Configuration > Object > Schedule



The following table describes the labels in this screen. See Section 35.8.2.1 on page 671 and Section 35.8.2.2 on page 672 for more information as well.

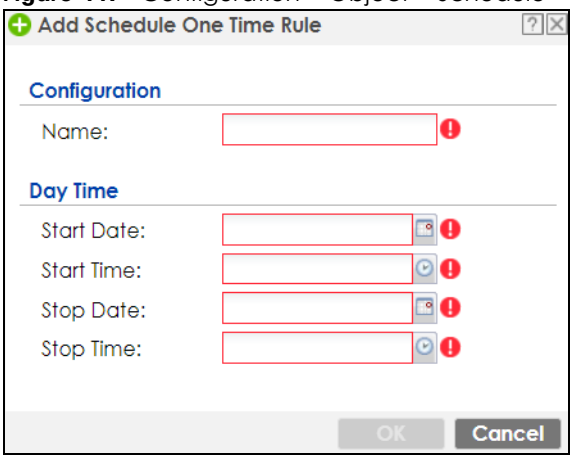
Table 281 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
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 schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.
Recurring	
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 schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.

35.8.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 35.8.2 on page 670), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 447 Configuration > Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

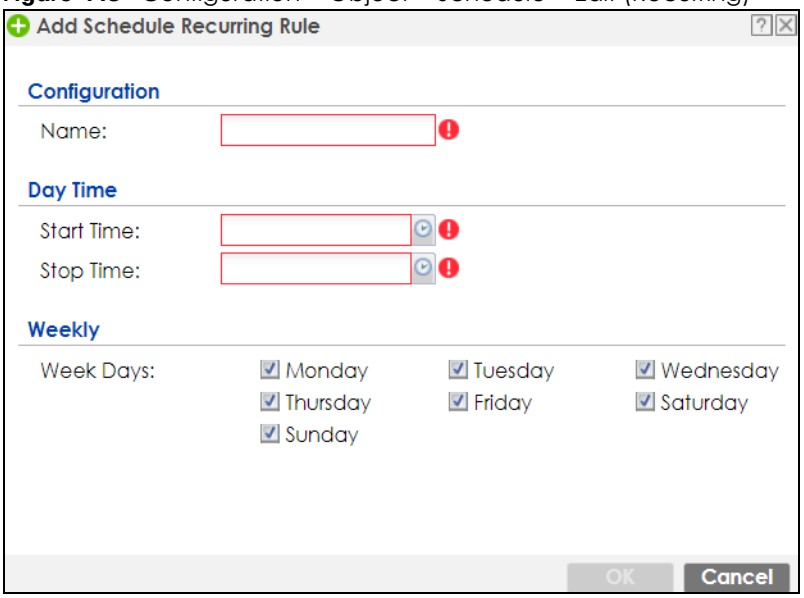
Table 282 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Day Time	
StartDate	Specify the year, month, and day when the schedule begins. • **Year** - 1900 - 2999 • **Month** - 1 - 12 • **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. • **Hour** - 0 - 23 • **Minute** - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. • **Year** - 1900 - 2999 • **Month** - 1 - 12 • **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. • **Hour** - 0 - 23 • **Minute** - 0 - 59
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.8.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 35.8.2 on page 670), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 448 Configuration > Object > Schedule > Edit (Recurring)



The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

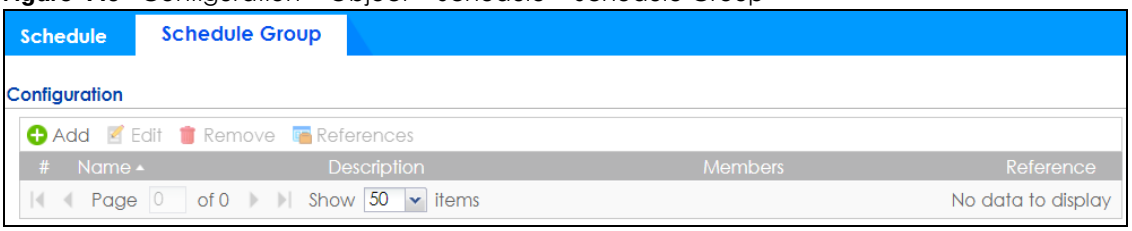
Table 283 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. • **Hour** - 0 - 23 • **Minute** - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. • **Hour** - 0 - 23 • **Minute** - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

35.8.3 The Schedule Group Screen

The **Schedule Group** screen provides a summary of all groups of schedules in the Zyxel Device. To access this screen, click **Configuration > Object** > **Schedule >Group**.

Figure 449 Configuration > Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

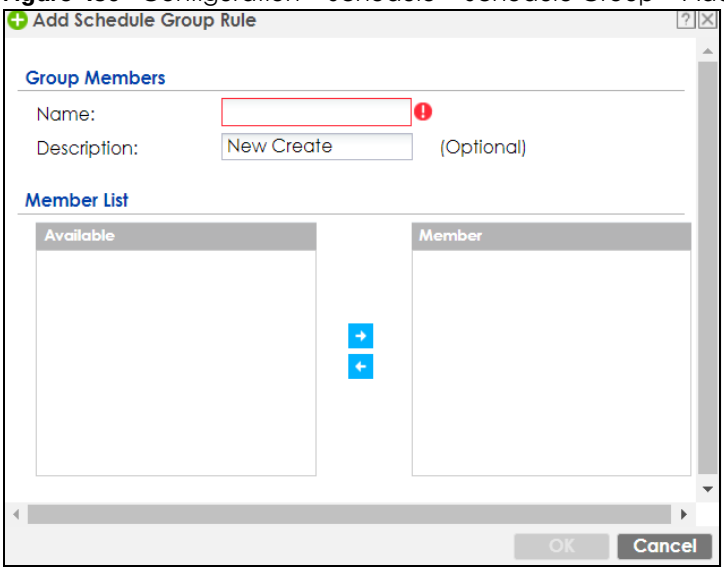
Table 284 Configuration > Object > Schedule > Schedule Group

LABEL	DESCRIPTION
Configuration	
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 schedule.
Name	This field displays the name of the schedule group, which is used to refer to the schedule.
Description	This field displays the description of the schedule group.
Members	This field lists the members in the schedule group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

35.8.3.1 The Schedule Group Add/Edit Screen

The **Schedule Group Add/Edit** screen allows you to define a schedule group or edit an existing one. To access this screen, go to the **Schedule** screen (see), and click either the **Add** icon or an **Edit** icon in the **Schedule Group** section.

Figure 450 Configuration > Schedule > Schedule Group > Add



The following table describes the fields in the above screen.

Table 285 Configuration > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	The **Member** list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

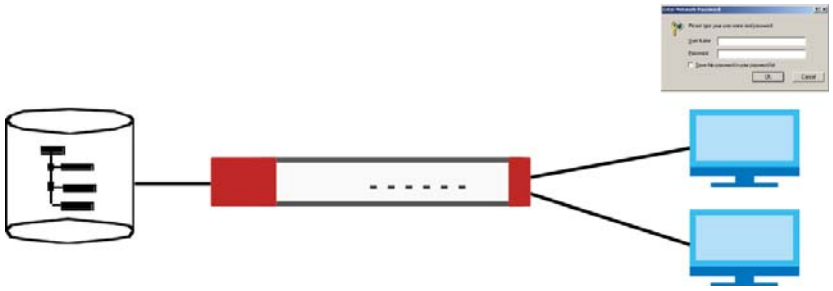
35.9 AAA Server Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You use AAA server objects in configuring ext-group-user user objects and authentication method objects (see Chapter 35 on page 685).

35.9.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the Zyxel Device) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 451 Example: Directory Service Client and Server



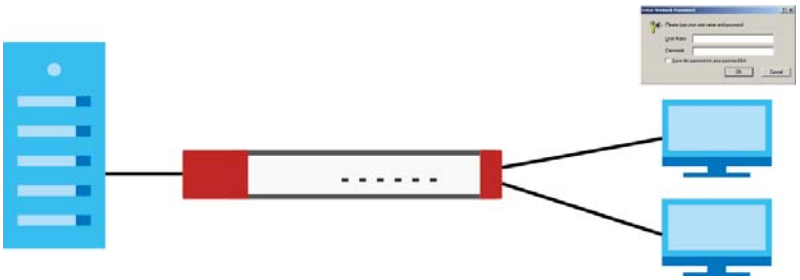
The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The Zyxel Device tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the Zyxel Device checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

35.9.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 452 RADIUS Server Network Example



35.9.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a Zyxel Device OTP package in order to use this feature. The package contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1. Install the ASAS server software on a computer.
2. Create user accounts on the Zyxel Device and in the ASAS server.
3. Import each token's database file (located on the included CD) into the server.
4. Assign users to OTP tokens (on the ASAS server).
5. Configure the ASAS as a RADIUS server in the Zyxel Device's **Configuration > Object > AAA Server** screens.
6. Give the OTP tokens to (local or remote) users.
   - Use the **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) screens (Section 35.9.5 on page 678) to configure Active Directory or LDAP server objects.
   - Use the **Configuration > Object > AAA Server > RADIUS** screen (Section 35.9.2 on page 676) to configure the default external RADIUS server to use for user authentication.

35.9.4 What You Need To Know

AAA Servers Supported by the Zyxel Device

The following lists the types of authentication server the Zyxel Device supports.

- Local user database

  The Zyxel Device uses the built-in local user database to authenticate administrative users logging into the Zyxel Device's Web Configurator or network access users logging into the network through the Zyxel Device. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

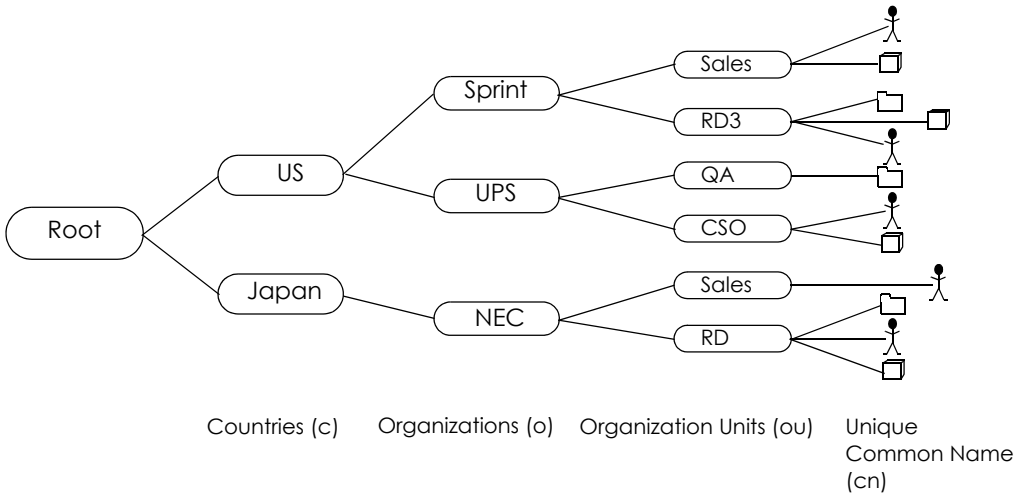
  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 453 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("`cn=domain1.com`, `ou=Sales, o=MyCompany`" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany`, `c=UK` where `o` means organization and `c` means country.

Bind DN

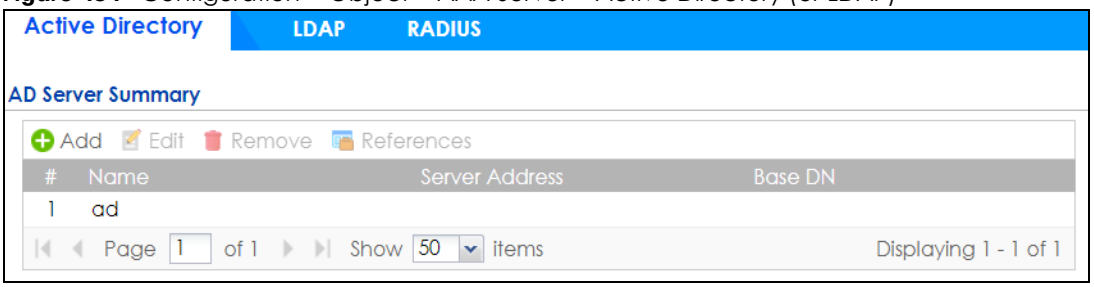
A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=zywallAdmin` allows the Zyxel Device to log into the LDAP/AD server using the user name of `zywallAdmin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the Zyxel Device will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

35.9.5 Active Directory or LDAP Server Summary

Use the **Active Directory** or **LDAP** screen to manage the list of AD or LDAP servers the Zyxel Device can use in authenticating users.

Click **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen.

Figure 454 Configuration > Object > AAA Server > Active Directory (or LDAP)



The following table describes the labels in this screen.

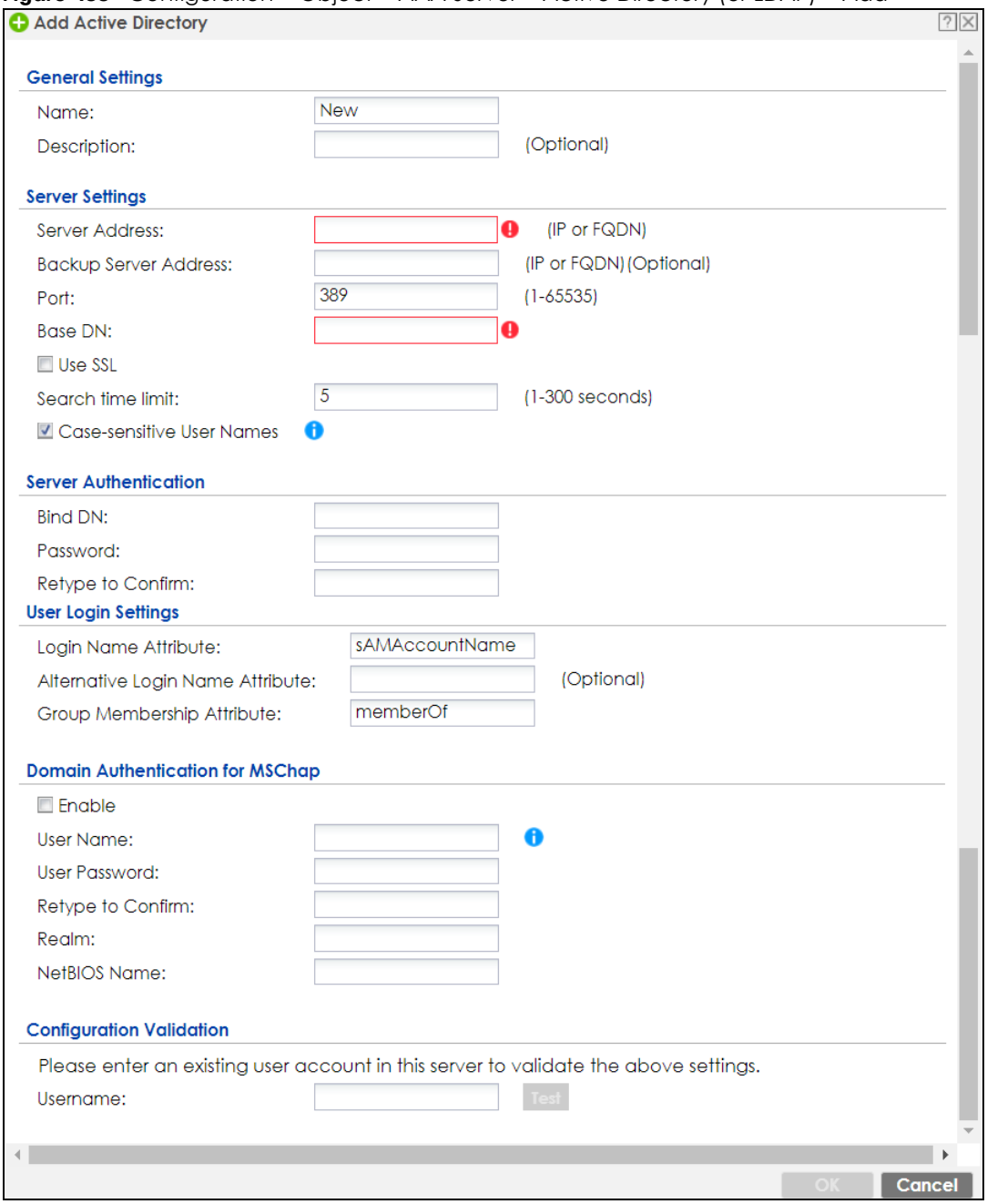
Table 286 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
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 AD or LDAP server.
Name	This field displays the name of the Active Directory.
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, `o=Zyxel, c=US`.

35.9.5.1 Adding an Active Directory or LDAP Server

Click **Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 455 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add



The following table describes the labels in this screen.

Table 287 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.

Table 287 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

LABEL	DESCRIPTION
Port	Specify the port number on the AD or LDAP server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, `o=Zyxel, c=US`. This is only for **LDAP**.
Use SSL	Select **Use SSL** to establish a secure connection to the AD or LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the usernames.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the Zyxel Device to bind (or log in) to the AD or LDAP server.
Retype to Confirm	Retype your new password for confirmation.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example “name” or “email address”.
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example “name” or “email address”.
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create a **ext-group-user** user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”.
Domain Authentication for MSChap	Select the **Enable** checkbox to enable domain authentication for MSChap. This is only for **Active Directory**.
User Name	Enter the user name for the user who has rights to add a machine to the domain. This is only for **Active Directory**.
User Password	Enter the password for the associated user name. This is only for **Active Directory**.
Retype to Confirm	Retype your new password for confirmation. This is only for **Active Directory**.
Realm	Enter the realm FQDN. This is only for **Active Directory**.
NetBIOS Name	Type the NetBIOS name. This field is optional. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN which allows local computers to find computers on the remote network and vice versa.

Table 287 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

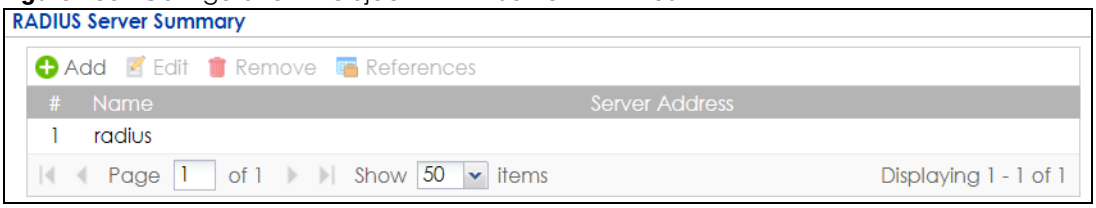
LABEL	DESCRIPTION
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account's user name in the **Username** field and click **Test**.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

35.9.6 RADIUS Server Summary

Use the **RADIUS** screen to manage the list of RADIUS servers the Zyxel Device can use in authenticating users.

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen.

Figure 456 Configuration > Object > AAA Server > RADIUS



The following table describes the labels in this screen.

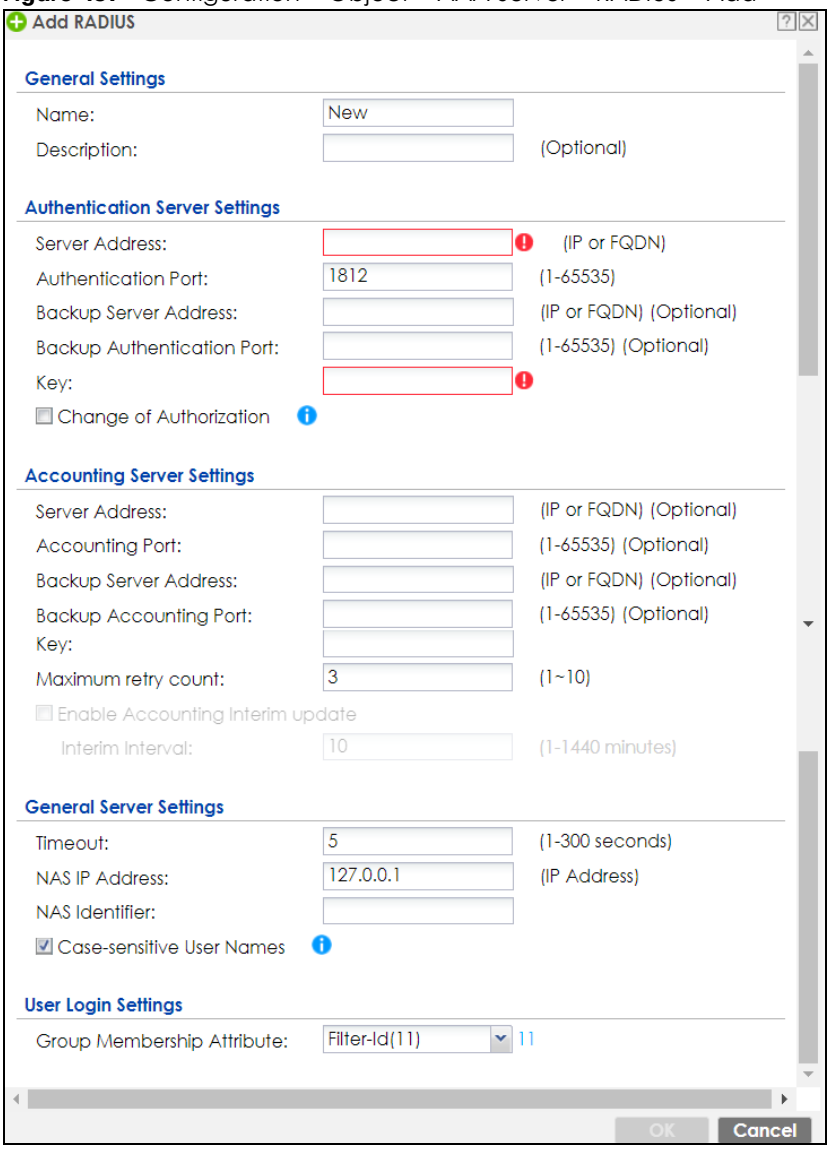
Table 288 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
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 displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the AD or LDAP server.

35.9.6.1 Adding a RADIUS Server

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 457 Configuration > Object > AAA Server > RADIUS > Add



The following table describes the labels in this screen.

Table 289 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535.

Table 289 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Change of Authorization	The external RADIUS server can change its authentication policy and send CoA (Change of Authorization) or RADIUS Disconnect messages in order to terminate the subscriber's service. Select this option to allow the Zyxel Device to disconnect wireless clients based on the information (such as client's user name and MAC address) specified in CoA or RADIUS Disconnect messages sent by the RADIUS server.
Server Address	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the RADIUS accounting server.
Accounting Port	Specify the port number on the RADIUS server to which the Zyxel Device sends accounting information. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup accounting server, enter its address here.
Backup Accounting Port	Specify the port number on the RADIUS server to which the Zyxel Device sends accounting information. Enter a number between 1 and 65535.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Maximum Retry Count	At times the Zyxel Device may not be able to use the primary RADIUS accounting server. Specify the number of times the Zyxel Device should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the Zyxel Device will attempt to use the secondary RADIUS server. For example, you set this field to 3. If the Zyxel Device does not get a response from the primary RADIUS server, it tries again up to three times. If there is no response, the Zyxel Device tries the secondary RADIUS server up to three times. If there is also no response from the secondary RADIUS server, the Zyxel Device stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.
Enable Accounting Interim Update	This field is configurable only after you configure a RADIUS accounting server address. Select this to have the Zyxel Device send subscriber status updates to the RADIUS server at the interval you specify.
Interim Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the RADIUS server.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
NAS IP Address	Type the IP address of the NAS (Network Access Server).
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the Network Access Server identifier attribute with a specific value, enter it here.
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.

Table 289 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the Zyxel Device is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a **ext-group-user** user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

35.10 Auth. Method Overview

Authentication method objects set how the Zyxel Device authenticates wireless, HTTP/HTTPS clients, and peer IPSec routers (extended authentication) clients. Configure authentication method objects to have the Zyxel Device use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the Zyxel Device are authenticated locally.

- Use the **Configuration > Object > Auth. Method** screens (Section 35.10.3 on page 686) to create and manage authentication method objects.
- Use the **Configuration > Object > Auth. Method > Two-Factor Authentication** screen (Section 35.10.4 on page 688) to configure double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel, Web Configurator, SSH, or Telnet.

35.10.1 Before You Begin

Configure AAA server objects before you configure authentication method objects.

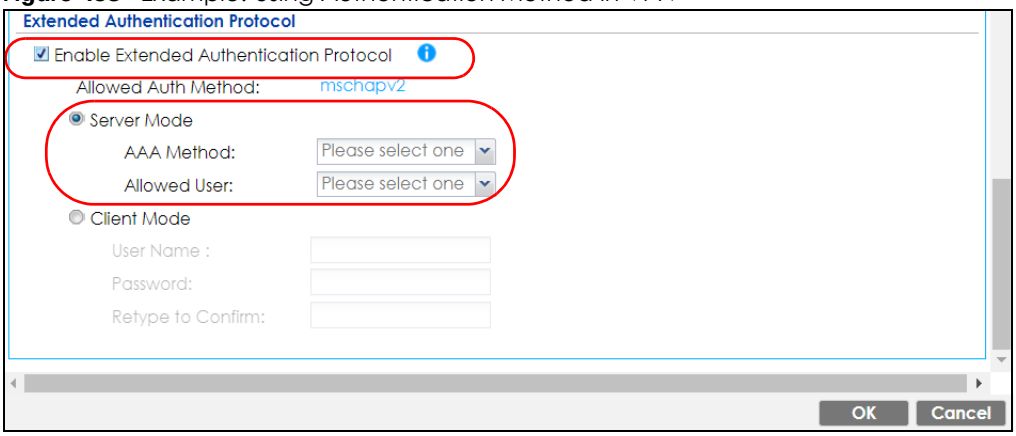
35.10.2 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

1. Access the **Configuration > VPN > IPSec VPN > VPN Gateway** > **Edit** screen.
2. Click **Show Advance Setting** and select **Enable Extended Authentication**.
3. Select **Server Mode** and select an authentication method object from the drop-down list box.
4. Click **OK** to save the settings.

Figure 458 Example: Using Authentication Method in VPN

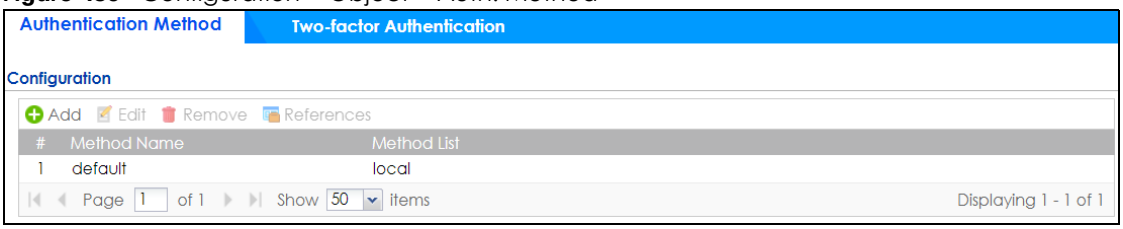


35.10.3 Authentication Method Objects

Click **Configuration > Object > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication method objects.

Figure 459 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 290 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
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 displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.

35.10.3.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

1 Click **Configuration > Object > Auth. Method**.

2 Click **Add**.

3 Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".

4 Click **Add** to insert an authentication method in the table.

5 Select a server object from the **Method List** drop-down list box.

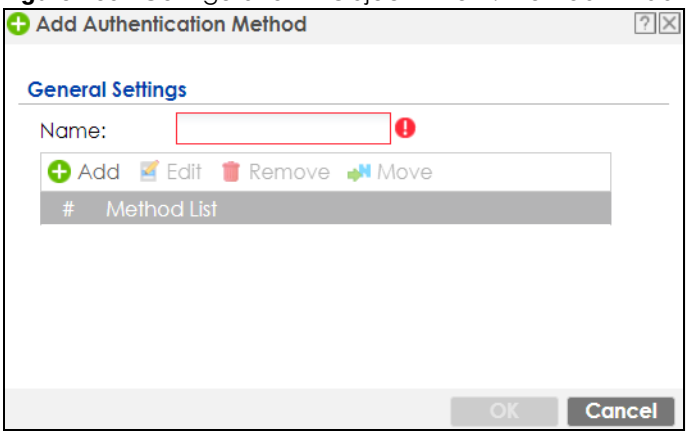
6 You can add up to four server objects to the table. The ordering of the **Method List** column is important. The Zyxel Device authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the Zyxel Device does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.

Note: You can NOT select two server objects of the same type.

7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 460 Configuration > Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 291 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_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 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.
Move	To change a method'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. The ordering of your methods is important as Zyxel Device authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.

Table 291 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Method List	Select a server object from the drop-down list box. You can create a server object in the **AAA Server** screen. The Zyxel Device authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the Zyxel Device does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

35.10.4 Two-Factor Authentication VPN Access

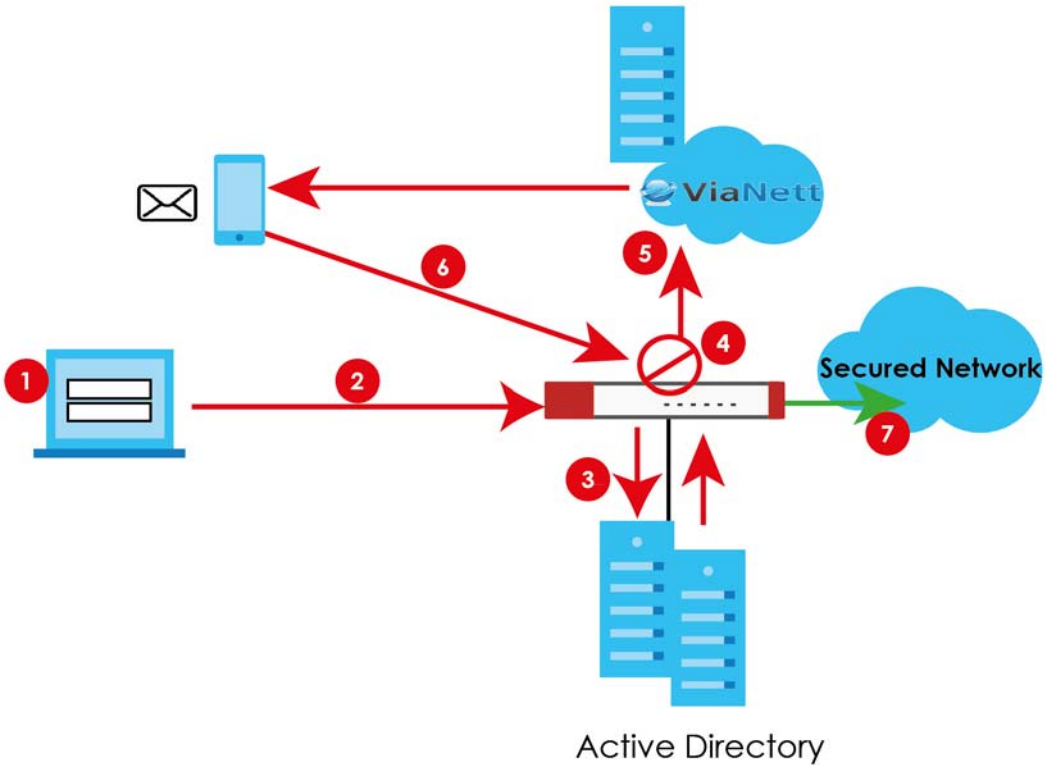
Use two-factor authentication to have double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel, Web Configurator, SSH, or Telnet.

The first layer is the VPN client/Zyxel Device's login user name / password and the second layer is an authorized SMS (via mobile phone number) or email address.

35.10.4.1 Overview

This section introduces how two-factor authentication works.

Figure 461 Two-Factor Authentication



Via a VPN tunnel

1. A user runs a VPN client and logs in with the user name and password for this VPN tunnel.
2. The VPN tunnel is created from the VPN client device to the Zyxel Device.
3. The Zyxel Device requests the user's user-name, password and mobile phone number or email address from the Active Directory, RADIUS server or local Zyxel Device database in order to authenticate this user's use of the VPN tunnel (factor 1). If they are not found, then the Zyxel Device terminates the VPN tunnel.
4. If all correct credentials are found, then the Zyxel Device will request the Cloud SMS system to send an authorization SMS or email to the client requesting VPN access (factor 2).
5. The client should access the authorization link sent via SMS or email by the Cloud SMS system within a specified deadline (**Valid Time**).
6. If the authorization is correct and received on time, then the client can have VPN access to the secured network. If the authorization deadline has expired, then the client will have to run the VPN client again. If authorization credentials are incorrect or if the SMS/email was not received, then the client must check with the network administrator.

Via the Web Configurator, SSH, or Telnet

1. An admin user is trying to log into the Zyxel Device using the Web Configurator, SSH, or Telnet.
2. The Zyxel Device requests the admin user's user-name, password and mobile phone number or email address from the Active Directory, RADIUS server or local Zyxel Device database in order to authenticate this admin user.
3. If all correct credentials are found, then the Zyxel Device will request the Cloud SMS system to send an authorization SMS or email to the admin user.
4. The admin user should access the authorization link sent via SMS or email by the Cloud SMS system within a specified deadline (**Valid Time**).
5. If the authorization is correct and received on time, then the client can access to the secured network. If the authorization deadline has expired, then the admin user will have to try again. If authorization credentials are incorrect or if the SMS/email was not received, then the admin user must check with the network administrator.

35.10.4.2 Pre-configuration

Before configuration, you must:

- Set up the user's user-name, password and email address or mobile number in the Active Directory, RADIUS server or local Zyxel Device database
- Configure the VPN tunnel for this user on the Zyxel Device
- Have an account with ViaNett to be able to send SMS/email authorization requests
- Enable **HTTP** and/or **HTTPS** in **System > WWW > Service Control**
- Enable SSH and/or Telnet in **System > SSH** and/or **System > TELNET**
- Configure **SMS** in **System > Notification > SMS.**

- Add **HTTP**, **HTTPS, SSH,** and/or, **TELNET** in the **Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL** service group.

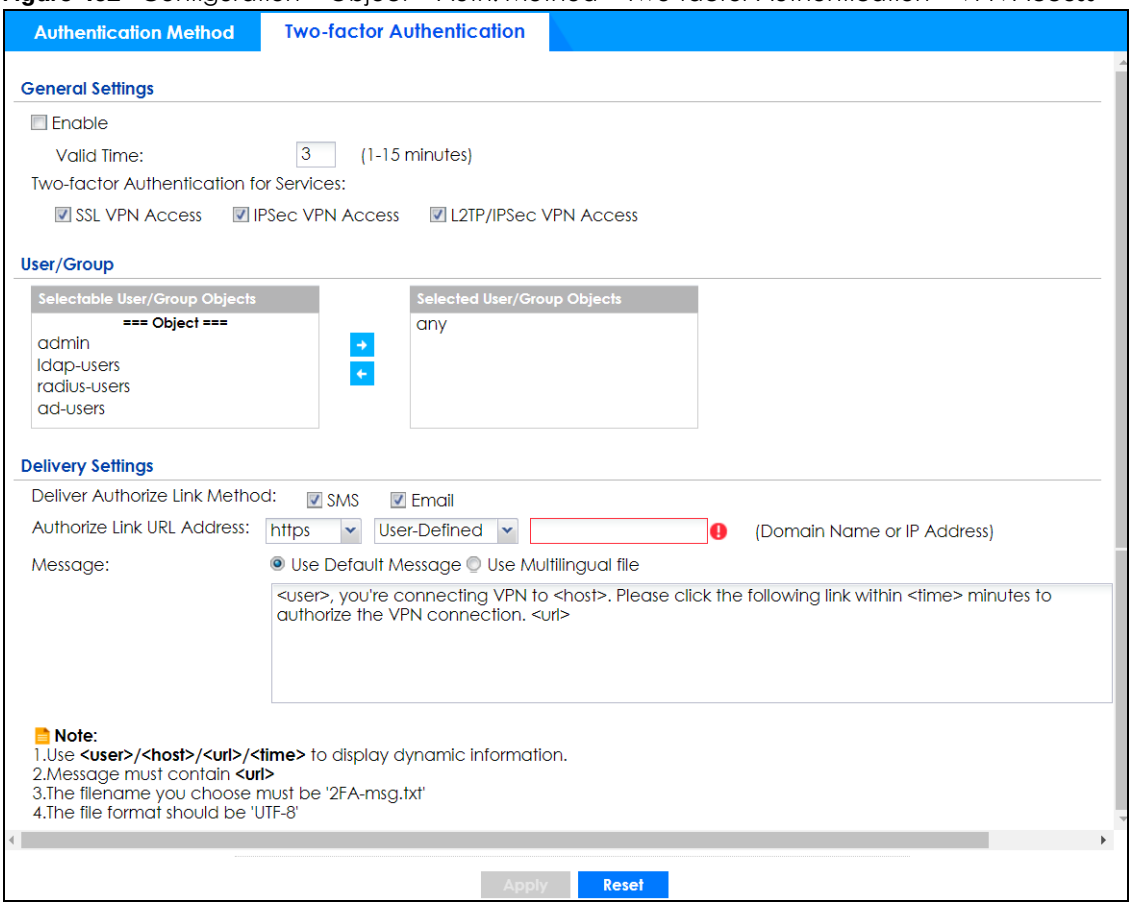
Two-Factor authentication may fail if one of the above is not configured or:

- The user did not receive the authorization SMS or email. Check if the mobile telephone number or email address of the user in the Active Directory, RADIUS Server or local Zyxel Device database is configured correctly
- ViaNett Authentication failed and no SMS was sent. Check that SMS is enabled and credentials are correct in **System > Notification > SMS**.
- Mail server authentication failed. Check if the **System > Notification > Mail Server** settings are correct.
- The authorization timed out. Extend the Valid Time in **Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access**.

Use this screen to select the users and VPN service(s) that requires two-factor authentication.

Go to **Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access** and configure the following screen as shown.

Figure 462 Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access



The following table describes the labels in this screen.

Table 292 Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access

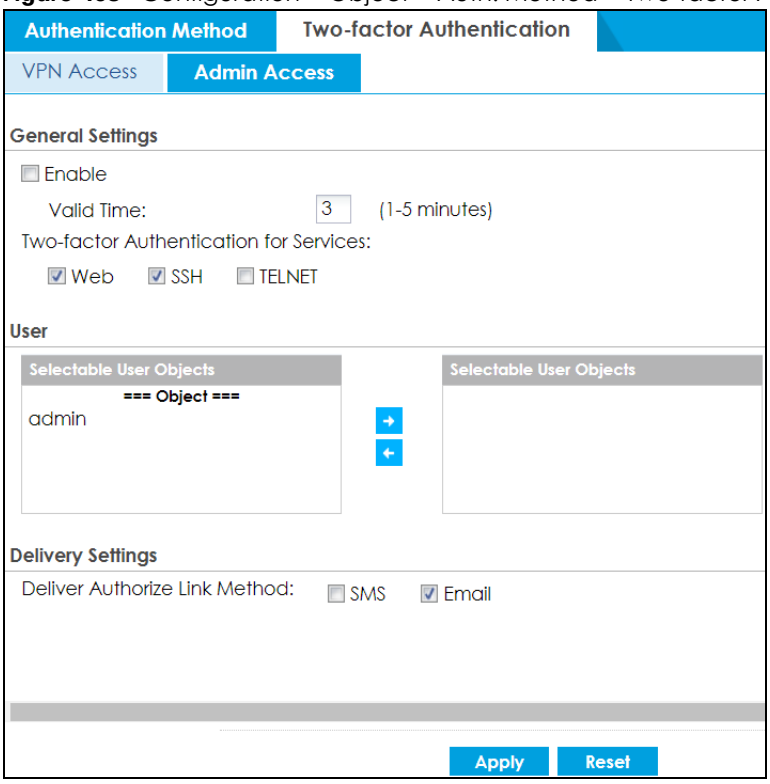
LABEL	DESCRIPTION
General Settings	
Enable	Select the check box to require double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel.
Valid Time	Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection.
Two-factor Authentication for Services:	Select which kinds of VPN tunnels require Two-Factor Authentication. You should have configured the VPN tunnel first. • SSL VPN Access • IPSec VPN Access • L2TP/IPSec VPN Access
User/Group	This list displays the names of the users and user groups that can be selected for two-factor authentication. The order of members is not important. Select users and groups from the **Selectable User/Group Objects** list that require two-factor authentication for VPN access to a secured network behind the Zyxel Device and move them to the **Selected User/Group Objects** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Similarly, move user/groups that do not you do not require two-factor authentication back to the **Selectable User/Group Objects** list.
Delivery Settings	Use this section to configure how to send an SMS or email for authorization.
Deliver Authorize Link Method:	Select one or both methods: • SMS: **Object > User/Group > User** must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • Email: **Object > User/Group > User** must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com
Authorize Link URL Address:	Configure the link that the user will receive in the SMS or email. The user must be able to access the link. • **http/https**: you must enable **HTTP** or **HTTPS** in **System > WWW > Service Control** • **From Interface/User-Defined:** select the Zyxel Device WAN interface (**wan1/2**) or select **User-Defined** and then enter an IP address.
Message	You can either create a default message in the text box or upload a message file (**Use Multilingual file**) from your computer. The message file must be named '2FA-msg.txt' and be in UTF-8 format. To create the file, click **Download the default 2FA-msg.txt example** and edit the file for your needs. (If you make a mistake, use **Restore Customized File to Default** to restore your customized file to the default.) Use **Select a File Path** to locate the final file on your computer and then click **Upload** to transfer it to the Zyxel Device. The message in either the text box or the file must contain the <url> variable within angle brackets, while the <user>, <host>, and <time> variables are optional.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.10.5 Two-Factor Authentication Admin Access

Use this screen to select the service (**Web**, **SSH**, and **TELNET**) that requires two-factor authentication for the admin user.

Go to **Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access** and configure the following screen as shown.

Figure 463 Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access



The following table describes the labels in this screen.

Table 293 Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access

LABEL	DESCRIPTION
General Settings	
Enable	Select the check box to require double-layer security to access a secured network behind the Zyxel Device via the Web Configurator, SSH, or Telnet.
Valid Time	Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for logins via the Web Configurator, SSH, or Telnet.
Two-factor Authentication for Services:	Select which services require Two-Factor Authentication for the admin user. • Web • SSH • TELNET
User	This list displays the names of the users and user groups that can be selected for two-factor authentication. The order of members is not important. Select users and groups from the **Selectable User Objects** list that require two-factor authentication for VPN access to a secured network behind the Zyxel Device and move them to the **Selected User Objects** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Similarly, move user/groups that do not you do not require two-factor authentication back to the **Selectable User Objects** list.
Delivery Settings	Use this section to configure how to send an SMS or email for authorization.

Table 293 Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access

LABEL	DESCRIPTION
Deliver Authorize Link Method:	Select one or both methods: • SMS: **Object > User/Group > User** must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • Email: **Object > User/Group > User** must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

35.11 Certificate Overview

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

- Use the **My Certificates** screens (see Section 35.11.3 on page 696 to Section 35.11.3.3 on page 704) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the **Trusted Certificates** screens (see Section 35.11.4 on page 705 to Section 35.11.4.2 on page 709) to save CA certificates and trusted remote host certificates to the Zyxel Device. The Zyxel Device trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

35.11.1 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Zyxel Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Zyxel Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the Zyxel Device act as a certification authority and sign its own certificates.

Factory Default Certificate

The Zyxel Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

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.

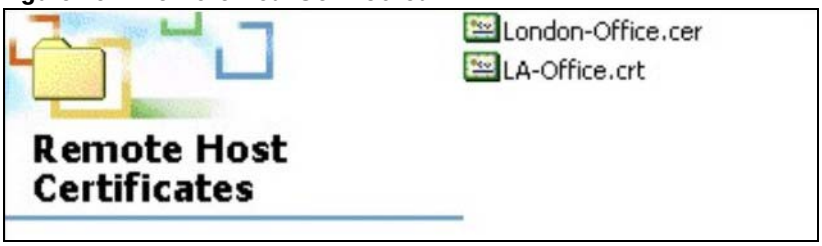
35.11.2 Verifying a Certificate

Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

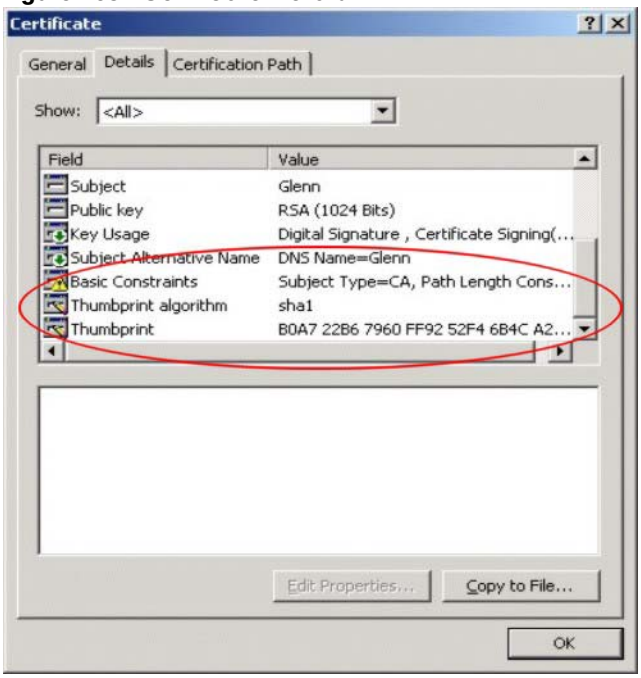
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 464 Remote Host Certificates



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 465 Certificate Details

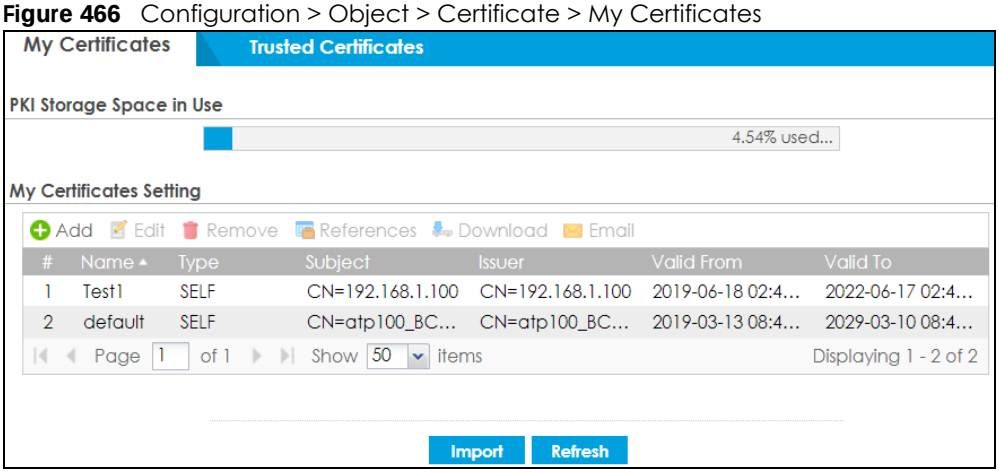


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

35.11.3 The My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the Zyxel Device's summary list of certificates and certification requests.

Figure 466 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 294 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the Zyxel Device generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
References	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **References** to open a screen that shows which settings use the entry.

Table 294 Configuration > Object > Certificate > My Certificates (continued)

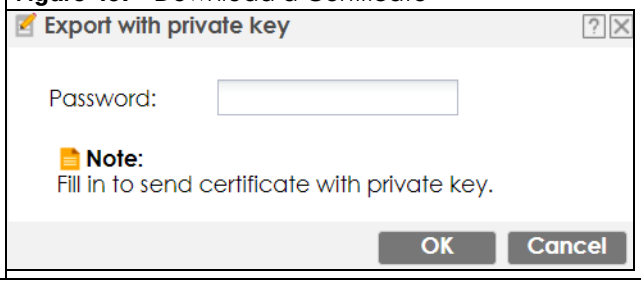
LABEL	DESCRIPTION
Download	Click this and the following screen will appear. Type the selected certificate's password and save the selected certificate to your computer. **Figure 467** Download a Certificate 

Table 294 Configuration > Object > Certificate > My Certificates (continued)

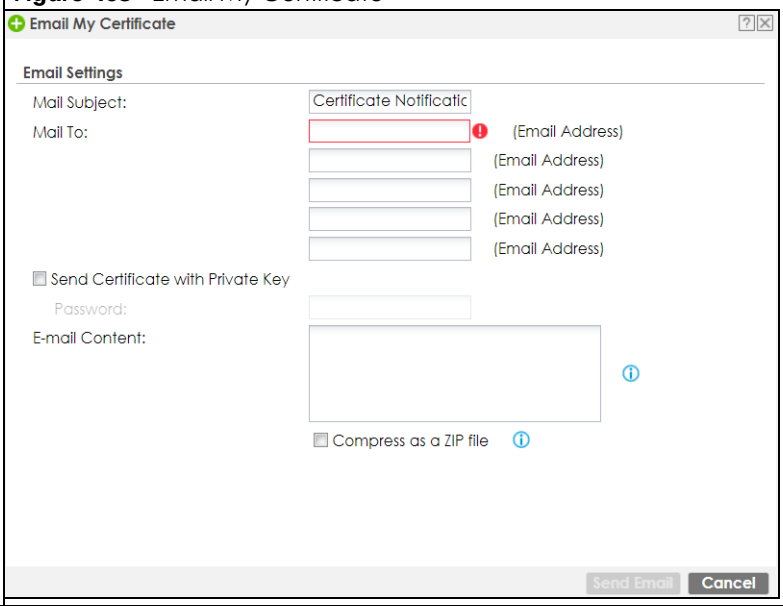
LABEL	DESCRIPTION
Email	Click this to email the selected certificate to the configured email address(es) for SSL connection establishment. This enables you to establish an SSL connection on your laptops, tablets, or smartphones. Click this and the following screen will appear. Here are the field descriptions: • **Mail Subject**: Type the subject line for outgoing email from the Zyxel Device. • **Mail To**: Type the email address (or addresses) to which the outgoing email is delivered. • **Send Certificate with Private Key**: Select the check box to send the selected certificate with a private key. • **Password**: Enter a private key of up to 31 keyboard characters for the certificate. The special characters listed in the brackets [;\ | `~!@#$%^&*()_+\\{}':,./<>=-"] are allowed. • **E-mail Content**: Create the email content in English, and use up to 250 keyboard characters. The special characters listed in the brackets [;\ \| `~!@#$%^&*()_+\\{}':,./<>=-"] are allowed. • **Compress as a ZIP File**: Select the check box to compress the selected certificate. Make sure the endpoint devices can decompress ZIP files before sending the compressed certificate. It's recommended to compress the certificate with a private key. Some email servers block PKCS #12 files. • **Send Email**: Click this to send the selected certificate. • **Cancel**: Click this to return to the previous screen without saving your changes. **Figure 468** Email My Certificate 
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

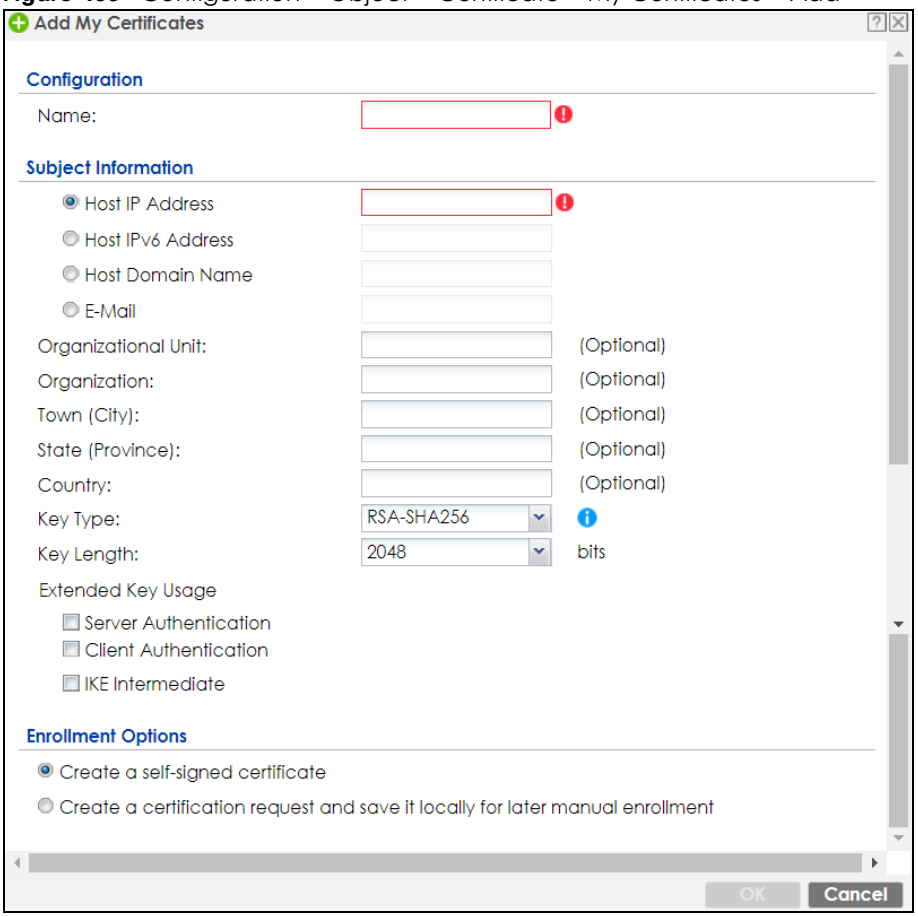
Table 294 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click **Refresh** to display the current validity status of the certificates.

35.11.3.1 The My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the Zyxel Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 469 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 295 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host IPv6 Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or email address. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An email address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 295 Configuration > Object > Certificate > My Certificates > Add (continued)

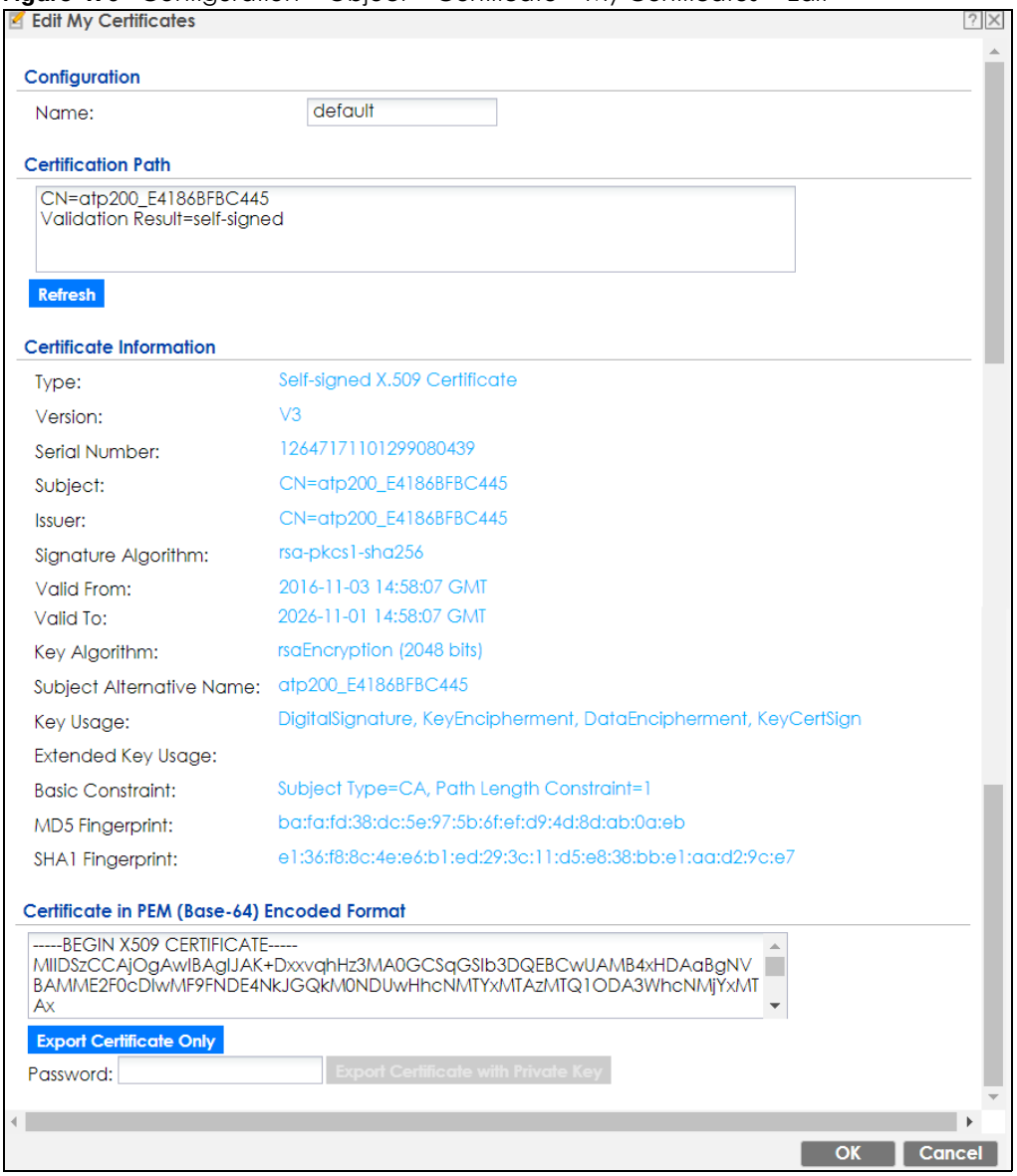
LABEL	DESCRIPTION
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm. Select **DSA** to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	
Server Authentication	Select this to have Zyxel Device generate and store a request for server authentication certificate.
Client Authentication	Select this to have Zyxel Device generate and store a request for client authentication certificate.
IKE Intermediate	Select this to have Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
Create a self-signed certificate	Select this to have the Zyxel Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the Zyxel Device generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 35.11.3.2 on page 701) and then send it to the certification authority.
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Zyxel Device to enroll a certificate online.

35.11.3.2 The My Certificates Edit Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 470 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 296 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Zyxel Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.

Table 296 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Zyxel Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The Zyxel Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some 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. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
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 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 how 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. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm.

Table 296 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	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 a certification request into a certification authority's web page, an email that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an email to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. 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**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **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 **My Certificates** screen.

35.11.3.3 The My Certificates Import Screen

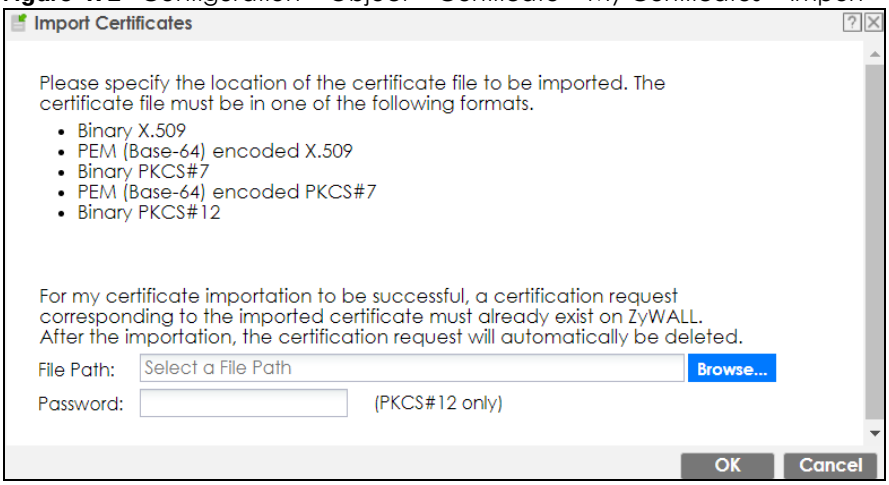
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

Note: 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.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

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

Figure 471 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

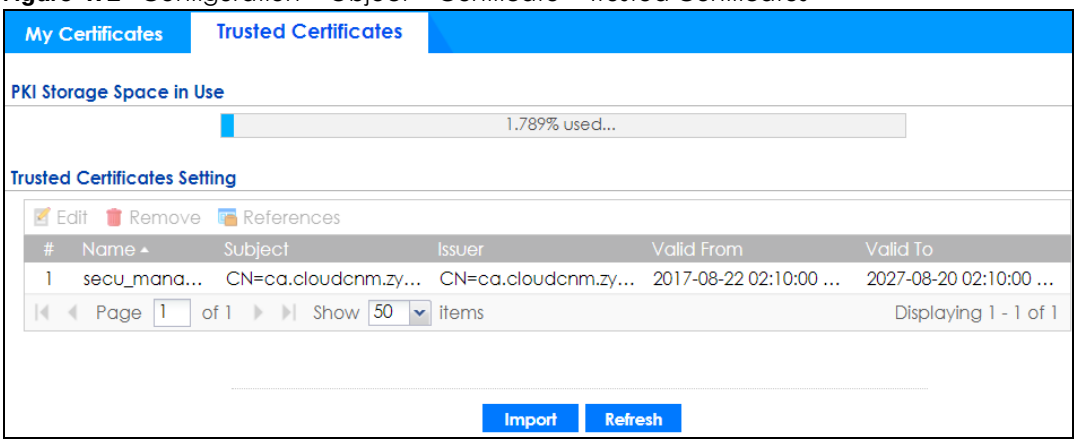
Table 297 Configuration > Object > Certificate > My Certificates > Import

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.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the Zyxel Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

35.11.4 The Trusted Certificates Screen

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

Figure 472 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 298 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
References	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.

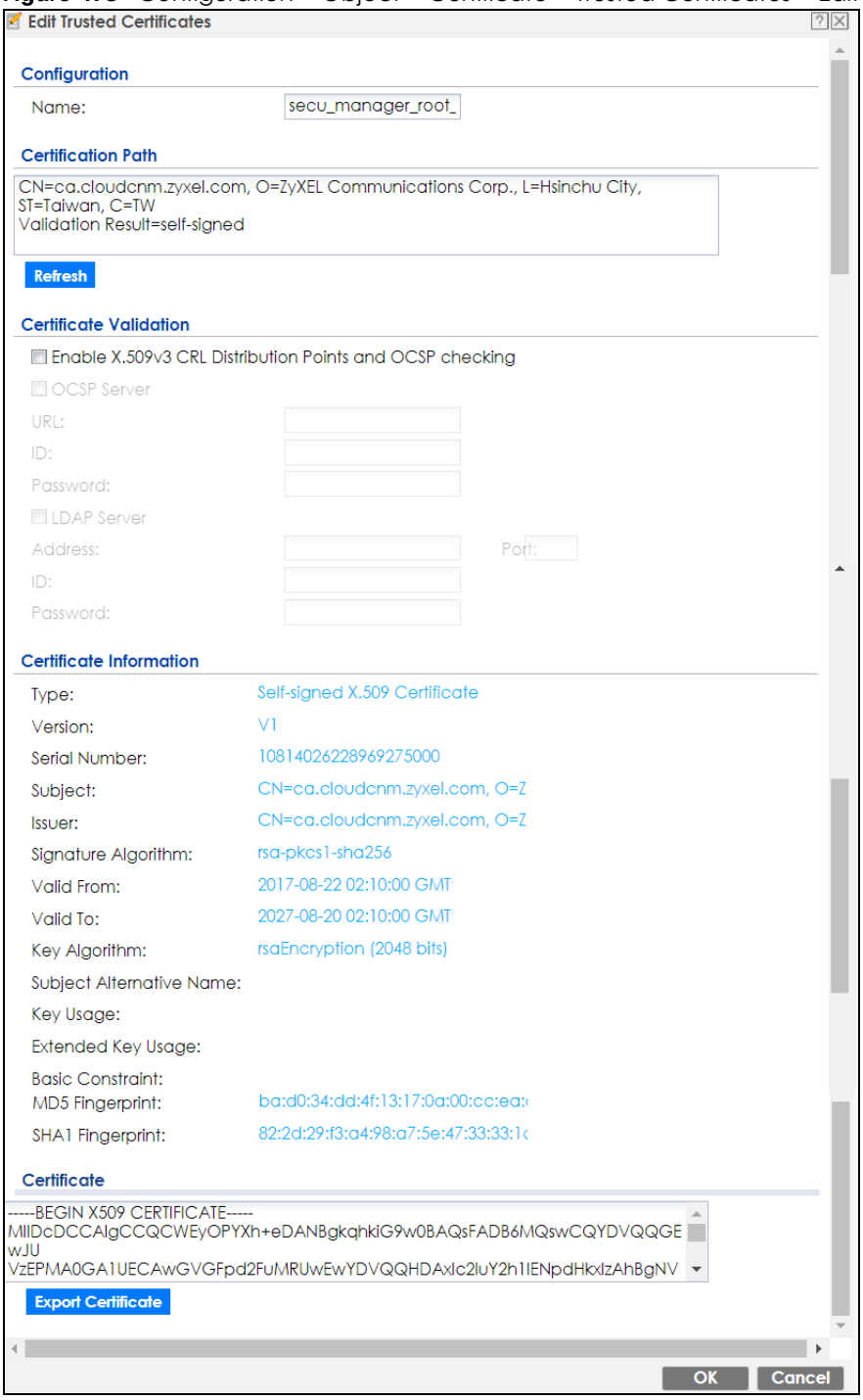
Table 298 Configuration > Object > Certificate > Trusted Certificates (continued)

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Zyxel Device.
Refresh	Click this button to display the current validity status of the certificates.

35.11.4.1 The Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the Zyxel Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 473 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 299 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The Zyxel Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to turn on/off certificate revocation. When it is turned on, the Zyxel Device validates a certificate by getting Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after selecting the **LDAP Server** check box) and online responder (can be configured after selecting the **OCSP Server** check box).
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and path name of the OCSP server.
ID	The Zyxel Device may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The Zyxel Device may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.