ZYXEL NETWORKS

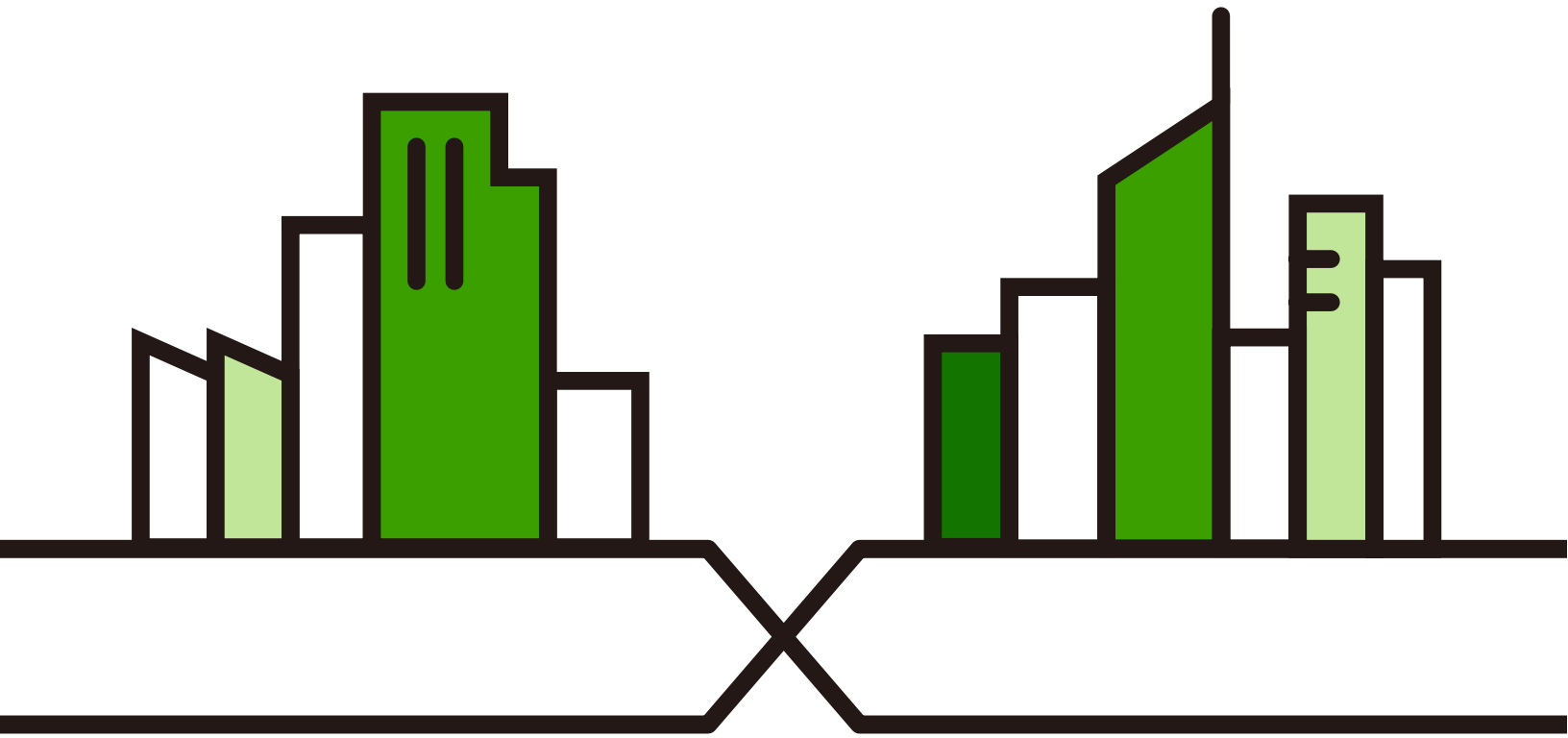
CLI Reference Guide

USG FLEX H Series

Default Login Details

IP Address	192.168.168.1
User Name	admin
Password	See Zyxel Device label or 1234
WAN	P1 or P2
LAN	P3 or P4

Version 1.38 Edition 2, 4/2026



IMPORTANT!
READ CAREFULLY BEFORE USE.
KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a Reference Guide for a series of products intended for people who want to configure the Zyxel Device using the Command Line Interface (CLI).

Note: The version number on the cover page refers to the latest firmware version supported by the Zyxel Device at the time of writing.

How To Use This Guide

Read Chapter 1 on page 19 for how to access and use the CLI (Command Line Interface).

Some commands or command options in this guide may not be available in your product. See your product's User's Guide for a list of supported features.
Do not use commands not documented in this guide. Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.
Some commands may be renamed in a firmware upgrade. In cases where a command has multiple names, the Reference Guide lists each variation.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device and access the Web Configurator.

- User's Guide

  Go to the Download Library to get the USG FLEX H Series User Guides that explains how to use the Web Configurator to configure the Zyxel Device. It also shows the product feature matrix for each device. General feature differences are written in the Introduction chapter while a more detailed table is in the Product Feature appendix.

- Online Help

  Click the help icon in the Web Configurator to access the latest Online Help with machine translation available.

- Nebula Control Center (NCC) Online Help

  Log into *nebula.zyxel.com* and click the Help icon to see how to configure the Zyxel Device using Nebula.

- More Information

  Go to *support.zyxel.com* to find other information on Zyxel Device.

Contents Overview

Table of Contents

Part I
Introduction

CHAPTER 1
Command Line Interface

This chapter describes how to access and use the CLI (Command Line Interface).

1.1 Overview

Zyxel Device refers to these models.

- USG FLEX 50H
- USG FLEX 50HP
- USG FLEX 100H
- USG FLEX 100HP
- USG FLEX 200H
- USG FLEX 200HP
- USG FLEX 500H
- USG FLEX 700H

If you have problems with your Zyxel Device, customer support may request that you issue some of these commands to assist them in troubleshooting.

Use of undocumented commands or misconfiguration can damage the Zyxel Device and possibly render it unusable.

1.1.1 The Configuration File

When you configure the Zyxel Device using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the Zyxel Device. You can store more than one configuration file on the Zyxel Device. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up the Zyxel Device configuration once the Zyxel Device is set up to work in your network.
- Restore the Zyxel Device configuration.
- Save and edit a configuration file and upload it to multiple Zyxel Devices (of the same model and firmware version) in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port or access the Zyxel Device using or SSH (Secure SHell).

See the cover page for default login credentials.

Note: The Zyxel Device might force you to log out of your session if re-authentication time, lease time, or idle timeout is reached. See Chapter 28 on page 234 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the Zyxel Device: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

When you turn on your Zyxel Device, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the Zyxel Device's.
- No text displays if the speed is set higher than the Zyxel Device's.
- If changing your terminal emulation program's speed does not get anything to display, restart the Zyxel Device.
- If restarting the Zyxel Device does not get anything to display, contact your local customer support.

Figure 1 Console Port Power-on Display

```
U-Boot 2018.03-7.1.0-svn568 (Dec 30 2023 - 10:23:14 +0800)



BootModule Version: V1.03 Dec 30 2020 10:23:14
DRAM: Size = 4096 Mbytes

Press any key to enter debug mode within 3 seconds.
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to USG FLEX 200HP

usgflex200hp login:
```

Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is on the Zyxel Device label or is **1234**. The username and password are case-sensitive.

1.2.2 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Before connecting, do the following in the Web Configurator:

- Enable **SSH** in **System > Settings**.
- To allow the SSH protocol from your remote computer to the Zyxel Device, add **SSH** to the service group **Default_Allow_WAN_To_ZyWALL** at **Object > Service > Service Group.** This group defines which services are allowed in the default **WAN_to_Device** security policy.

Note: The default login username is **admin** and password is on the Zyxel Device label or is **1234**. The username and password are case-sensitive.

Figure 3 SSH Login Example

```
C:\>ssh admin@192.168.168.1
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/
hostkeys/
ey_22_192.168.168.1.pub
host key for 192.168.168.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

1.3 How to Find Commands in this Guide

You can search for a command, look for the command in the feature chapter or find the command in the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

1.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

1.4.1 Background Information (Optional)

Note: See the User's Guide for more detailed background information about most features.

1.4.2 Command Input Values (Optional)

This section lists common input values for the commands for the feature in one or more tables

1.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

1.4.4 Command Examples (Optional)

This section contains any examples for the commands in this feature.

1.4.5 Command Syntax

The following conventions are used in this User's Guide.

- A command or keyword in `courier new` must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *`italics`*.
- Required fields that have multiple choices are enclosed in curly brackets `{}`.
- A range of numbers is enclosed in angle brackets `<>`.
- Optional fields are enclosed in square brackets `[]`.
- The `|` symbol means OR in a list of choices or can be used as a switch in a command, such as `show config running | no-pager`.

For example, look at the following command to create a TCP/UDP service object.

`object service-object service` ***`service-name`*** `type {tcp | udp} {<1..65535>-<1..65535>}`

1. Enter `object service-object service` exactly as it appears.
2. Enter the name of the object where you see *`service-name.`*
3. Enter `tcp` or `udp`, depending on the service object you want to create.
4. Enter two numbers between 1 and 65535.

1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the Zyxel Device. See Section 28.2 on page 234 for the appropriate commands.

1.4.7 Idle Timeout

See Section 28.3 on page 235 for commands on changing the default logout time when no activity is recorded.

1.5 CLI Modes

You run CLI commands is User Mode or Edit (Staging Configuration) Mode.

After you log into the Zyxel Device, you will see this prompt `usgflex200hp>` in User Mode.

Type `edit running` and you will see this prompt `usgflex200hp running config#` in Edit mode to configure settings that are currently running on the Zyxel Device.

In Edit mode, commands are not applied to the running configuration yet. You can configure several commands in this mode, then use the Diff command to see all the commands you edited at all levels. Review, revise or remove (`del /vrf main interface`) any wrong commands before using `commit` to save all the edited commands to the running configuration.

Note: You lose all edited commands if you exit Edit mode before using `commit`.

After you commit, the changed commands are saved in the running configuration, but not the startup configuration.

Note: You must copy the running configuration to the startup configuration to retain commands after the Zyxel Device restarts - use the command `copy running startup`.

This is a summary of the modes.

Table 2 CLI Modes

	USER MODE	EDIT (STAGING CONFIGURATION) MODE	EDIT SUB-COMMAND
What **Admin** users can do	• Look at system information (like the **Dashboard** screen) and settings. • Run basic diagnostics.	• Configure simple features such as an address object. • Create or remove general features such as an interface.	• Configure specific parts of a feature such as a particular interface on the Zyxel Device.
How you enter it	Type username and password to log into the Zyxel Device.	Type **edit running**	Type the command used to enter the specific part of the feature at the **Configuration** level.

What the prompt looks like	`usgflex200hp>`	`usgflex200hp running config#`	(varies by command)
			`usgflex500h running vrf main#`
			`usgflex200hp running allow-list ...`

How you exit it	N/A	Type **exit**.	Type **exit**.

See Section 2.1.4 on page 38 for examples of configuration error prompts.

1.6 CLI Levels

The CLI has various levels of commands such as:

- root
- vrf main
- interface
- ethernet ge1

Type '`/`' to go to the root level

Type `show config full path` to display the full path for each command.

Type `pwd` to print out current path

Type '`..`' to go back one level.

1.7 CLI Structure

- Type `cmd` to have the Zyxel Device execute actions, such as pinging the specified IP address or rebooting.

Figure 4 `cmd` Command Example

```
usgflex200hp> cmd ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=7.41 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=9.90 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=10.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=8.64 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=8.43 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=7.58 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=114 time=7.26 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=114 time=8.20 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 7.255/9.531/17.651/3.068 ms
```

- Type `show state` to displays the status of the settings you configured that will effect the Zyxel Device and your network.

Figure 5 `show state` Command Example

```
usgflex200hp> show state two-factor-auth admin-access enabled
enabled true
```

- Type `show config` to displays the settings currently running on the Zyxel Device.

Figure 6 `show config` Command Example

```
usgflex200hp> show config object user-object admin
admin admin
    role admin
    enabled true
    logon-lease-time default
    logon-reauth-time default
    password $8$xdvd0Uhn$xVzlMpHy$LCoIrGtNtuQ8bdaw/3Mvq/
WXW1KwWiHTA+3HWjHV8xgmP7NLCjGwKkgyQaALJnDsg7trI9FVfHKJYcr9fDSCOZDnWM2bPHVjK
4XKbf+uNDoE/
l3vYcnQiOJATc2af7T89oLX+xEv5+vjBZMhWU8wP8f1056wg7ChqrpjHyhNN615WhLBxvck9x3b
ZrtuEFVjofJuazB+GgLxdqJiaF1YtKJTkEeXESKkZ5C0aEonzZF3SRinfKIXvWvHd8ketnn9Xpf
raYS6lSpqvM4Duqy+KeTmQCKth9zXURh4DV7f9Ixz7/PD97ZS3ZFo/
kNbLRX7vMMTf8bRTzm7Z2cJ2r+IT0oEIcg7Emu7NKJh/BBsOh8$
```

- Type `vrf main` to configure the Zyxel Device Internet and Internet related settings, such as the anti-malware settings or the interface settings.

Figure 7 `vrf main` Command Example

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware
default-profile    statistics         eicar-detection    cloud-query
allow-list
block-list         default-port       enabled            scan-mode
usgflex200hp running config# vrf main anti-malware enabled true
```

- Use the `commit` command to apply changes to the configuration file that is currently running on the Zyxel Device.

Note: Always apply (commit) the changes you made to the running configuration file before you exit the configuration mode. All changes that are not applied will be lost after you log out of the configuration mode.

Note: Always save the changes you made in the running configuration file to the start up configuration file (startup-config.conf) before you reboot the Zyxel Device. Changes that are not saved to the start up configuration file will be lost after you reboot the Zyxel Device.

Figure 8 `commit` Command Example

```
usgflex200hp running config# object user-object admin admin role admin
usgflex200hp running config# commit
Configuration committed.
```

- Enter the `exit` command in the configuration or sub-command mode to go to the admin mode.

  Enter the `exit` command in the admin mode to log out of the CLI.

Figure 9 `exit` Command Example

```
usgflex200hp running config# exit
usgflex200hp> exit

Welcome to USG FLEX 200HP

usgflex200hp login:
```

1.8 Shortcuts and Help

See the following sections for the shortcuts and help you can use the CLI.

1.8.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter <command> ? or <command> [TAB].

Figure 10 Help: Available Commands Example 1

```
usgflex200hp>?
  cliconfig            Enable/disable pager for this session.
  cmd                  Send a command.
  copy                 Copy a configuration into another one.
  diff                 Diff configurations.
  echo                 Echo arguments.
  edit                 Edit configuration.
  exec                 Execute a cli script file.
  exit                 Quit the cli.
  export               Export a configuration file.
  flush                Flush objects.
  help                 Show the help.
  import               Import a configuration file.
  netconf             NETCONF related commands: connect, disconnect, status.
  remove               Remove a configuration file.
  resize               Resize terminal.
  show                 Show configuration or system state.
  validate             Validate a configuration.
```

Figure 11 Help: Available Command Example 2

```
usgflex200hp>show ?
  absolute             Select display path mode (default: relative).
  all                  Select display mode (default: all).
  config               Show the configuration.
  dry-run              Display NETCONF RPC instead of sending it.
  fullpath             Select display path mode (default: relative).
  json                 Select display format (default: text).
  nodefault            Select display mode (default: all).
  relative             Select display path mode (default: relative).
  state                Show the system state.
  text                 Select display format (default: text).
  with-deprecated      Show deprecated nodes, which are by default hidden in
                       show text state.
  xml                  Select display format (default: text).

  alg ftp              Show configuration or system state.
  app-patrol-applications
                       Show app patrol applications
  app-patrol-categories
                       Show app patrol categories
  app-patrol-signature-version
                       Show app patrol signature version
  bfd                  Show BFD information.
  bgp                  Show BGP information.
```

1.8.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter `<command> <sub command> ?`.

Figure 12 Help: Required User Input Example

```
usgflex200hp running config# switch 0 port ?
  port                 Set value of configuration leaves.
  port-grouping        Set value of configuration leaves.
```

Figure 13 Help: Sub-command Information Example

```
usgflex200hp running vrf main# anti-malware allow-list logging ?
  log                  Default: no.
                       allow list log setting
  no                   Default: no.
                       allow list log setting
```

1.8.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the Zyxel Device automatically display the full command.

For example, if you enter `edi` and press [TAB] , the full command of `edit` automatically displays.

If you enter a partial command that is not unique and press [TAB], the Zyxel Device displays a list of commands that start with the partial command.

Figure 14 Non-Unique Partial Command Example

```
usgflex200hp> e [TAB]
echo      exec      exit      edit      export
usgflex200hp> ex [TAB]
exec      exit      export
```

1.8.4 Entering a ? in a Command

Typing a `?` (question mark) usually displays help information. However, some commands allow you to input a `?`, for example as part of a string. Press [CTRL+V] on your keyboard to enter a `?` without the Zyxel Device treating it as a help query.

1.8.5 Command History

The Zyxel Device keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

1.8.6 Navigation

Press [CTRL+A] to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

1.8.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

1.9 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may not be displayed in the screen. For example, in the following example, the next input value is a string called <description>.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object admin admin description
  <description>        Description string.
```

The following table provides more information about input values like <description>.

Table 3 Input-Value Formats for Strings in CLI Commands

TAG	# VALUES	LEGAL VALUES
***	1	*
all	--	ALL
authentication key	Used in IPSec SA	
	32-40 16-20	"0x" or "0X" + 32-40 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
	Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP	
	0-16	alphanumeric or _-
	Used in text authentication keys for OSPF	
	0-8	alphanumeric or _-
certificate name	1-31	alphanumeric or ;`~!@#$%^&()_+[\]{}',.=-
community string	0-63	alphanumeric or .- first character: alphanumeric or -
connection_id	1+	alphanumeric or -_:
contact	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
country code	0 or 2	alphanumeric
custom signature file name	0-30	alphanumeric or _-. first character: letter
description	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
	Used in other commands	
	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
distinguished name	1-511	alphanumeric, spaces, or .@=,_-

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
domain name	Used in content filtering	
	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	0-247	alphanumeric or - first character: alphanumeric or -
	Used in domain name, ip dhcp and ip domain	
	0-254	alphanumeric or _- first character: alphanumeric or -
email	1-63	alphanumeric or @_-
e-mail	1-64	alphanumeric or @_-
encryption key	16-64 8-32	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-
fqdn	Used in ip dns server	
	0-252	alphanumeric or .- first character: alphanumeric or -
	Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+".conf"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".conf" at the end
import shell script	1-26+".zysh"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".zysh" at the end
initial string	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
isp account password	0-63	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
isp account username	0-30	alphanumeric or -_@$./

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
ipv6_addr		An IPv6 address. The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000. IPv6 addresses can be abbreviated in two ways: Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0. Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.
key length	--	512, 768, 1024, 1536, 2048, 4096
license key	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
mac address	--	aa:bb:cc:dd:ee:ff (hexadecimal)
mail server fqdn		lower-case letters, numbers, or -.
name	1-31	alphanumeric or _-
notification message	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
password: less than 15 chars	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
password	Used in user and ip ddns	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:,.
	Used in registration	
	6-20	alphanumeric or .@_-
phone number	1-20	numbers or ,+
preshared key	16-64	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	0-30	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	0-30	alphanumeric or _- first character: letters or _-
quoted string less than 127 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (") must put a backslash (\) before double quotation marks that are part of input value itself
service name	0-63	alphanumeric or -_@$./
spi	2-8	hexadecimal
string less than 15 chars	1-15	alphanumeric or -_
string: less than 63 chars	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
string	1+	alphanumeric or -_@
subject	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@$_%-
system type	0-2	hexadecimal
timezone [-+]*hh*	--	-12 through +12 (with or without "+")
url	1-511	alphanumeric or '()+,/:.=?;!*#@$_%-
url	Used in content filtering redirect	
	"http://"+ "https://"+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with "http://" or "https://" may contain one pound sign (#)
	Used in other content filtering commands	
	"http://"+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with "http://" may contain one pound sign (#)
user name	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.10 Ethernet Interfaces

At the time of writing, Zyxel Devices use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface on your Zyxel Device, as the name for the Ethernet interface.

1.11 Resetting the Zyxel Device

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

1.12 Fast-Path Acceleration

Fast-path Acceleration is a way to speed up certain traffic such as NAT, IPSec VPN, Security policies through the Zyxel Device by bypassing the kernel. SSL VPN traffic does not use fast-path acceleration.

1.12.1 Load Balancing

Enable Load Balancing to improve the processing of large volumes of encrypted traffic, such as VPN traffic.

Note: This is NOT the same as traffic load balancing using weighted round robin, least load first or the spillover algorithms.

Encrypted traffic processing is done by distributing incoming Encapsulating Security Payload (ESP) packets across different CPUs for decoding. Use these commands to enable Load Balancing and see the status.

Table 4 Encrypted Traffic Balancing Commands

COMMAND	DESCRIPTION
`system fast-path-esp-rx-loading-balance enabled {true | false}`	Enables (`true`) load balancing for incoming encrypted traffic.
`show system fast-path esp-rx-loading-balance status`	Displays load balancing for incoming encrypted traffic.

Figure 15 Enable Encrypted Traffic Balancing Example

```
usgflex500h> edit running
usgflex500h running config# system fast-path-esp-rx-loading-balance enabled true
usgflex500h running config# commit
Configuration committed.
usgflex500h running config# show system fast-path esp-rx-loading-balance status
show-system-fast-path-esp-rx-loading-balance-status
    status Enabled
```

You may disable Load Balancing if your network does not have a lot of VPN traffic, or if certain data must be processed on the same CPU core or if you want to simplify the network architecture for troubleshooting.

Figure 16 Disable Encrypted Traffic Balancing Example

```
usgflex500h> edit running
usgflex500h running config# system fast-path-esp-rx-loading-balance enabled false
usgflex500h running config# commit
Configuration committed.
usgflex500h running config# show system fast-path esp-rx-loading-balance status
show-system-fast-path-esp-rx-loading-balance-status
    status Disabled
```

1.12.2 Fast-Path Recovery

If the fp-rte daemon crashes, then fast-path is lost and the Zyxel Device will be unable to function properly.

Fast-path recovery is enabled by default, and the Zyxel Device will recover if the fp-rte daemon crashes. Recovery will take 1~2 minutes.

If fast-path recovery is disabled, the Zyxel Device will reboot using fast-path watchdog if the fp-rte daemon crashes. Reboot will take 3~5 minutes.

If the fp-rte daemon crashes, the Zyxel Device will not reboot if fast-path watchdog is disabled.

Table 5 Fast-Path Recovery Commands

COMMAND	DESCRIPTION
`system fastpath-recovery enabled {true | false}`	Enables (`true`) fast-path recovery.
`show fast-path mem status details`	Displays fast-path recovery details

Figure 17 Fast-Path Recovery

```
usgflex500h> edit running
system fastpath-recovery enabled true
usgflex500h running config# commit
usgflex500h running config# show fast-path mem status details
Heap id:0
        Heap name:socket_0
        Heap_size:2720006144,
        Free_size:1445140736,
        Alloc_size:1274865408,
        Greatest_free_size:1439621376,
        Alloc_count:12752,
        Free_count:3,
Heap id:1
        Heap name:mbuf_pool_socket_0
        Heap_size:224395264,
        Free_size:134770176,
        Alloc_size:89625088,
        Greatest_free_size:134770176,
        Alloc_count:3,
        Free_count:1,
Heap id:2
        Heap name:fp_ips_app_ring_mem_zone-0_0
        Heap_size:39845888,
        Free_size:39845888,
        Alloc_size:0,
        Greatest_free_size:39845888,
        Alloc_count:0,
```

1.13 Packet Reordering

In the fast-path architecture, traffic is processed in parallel (multi-core, offload, acceleration), so this can cause out-of-order packets.

Enable pkt-reorder to temporarily buffer, then re-sequence packets back into order before passing them up the networking stack. (Reordering may not be perfect with VPN or load-balancing.)

Disable pkt-reorder to leave them in whatever order they were received for maximum forwarding performance.

Out-of-order packets may cause duplicate ACKs or gaps in TCP sequence numbers, so enable fast-retransmit-enabled to retransmit a packet immediately instead of waiting for a TCP timeout. This improves throughput, recovery time and latency on reordered paths.

Note: If you disable `pkt-reorder`, you cannot use `fast-retransmit-enabled`.

This table lists the packet reordering commands.

Table 6 Packet Reordering Commands

COMMAND	DESCRIPTION
`vrf main pkt-reorder enabled {true | false}`	Re-sequences (`true`) packets back into order before passing them up the networking stack.
`vrf main pkt-reorder fast-retransmit-enabled {true | false}`	Retransmits (`true`) a packet immediately instead of waiting for a TCP timeout.

CHAPTER 2
Getting Started

This chapter shows you how to use some of the more common commands to help you get started using the Zyxel Device using the CLI.

Wireless Management on page 52	See the Managed APs' Status on page 52
	See the WiFi Clients' Status on page 53
	Block a WiFi Client from the WiFi Network on page 53
Troubleshooting on page 54	Restart the Zyxel Device on page 54
	Restart the NCC Connection on page 54
	Reset the Configuration to the Factory Defaults on page 54
	Display Management Logs on page 55
	Display Kernel Console Level on page 56
	Activate a Remote Support Account on page 56

2.1 CLI Tips

These are some general tips on using the CLI.

2.1.1 Resize the Terminal Emulation Software Screen

Use the `resize` command to change the width of your terminal emulation software screen (such as Tera Term) to view complete commands in a single row.

2.1.2 Display All The Results Of a Command At Once

Use `no-pager` to display all the results of a command at once. The default is to display one page a time ending with `':'`. You then press any key to continue the display.

- To disable paging for a specific command, use the no-pager switch in the command. For example, `show config running | no-pager`.
- To disable paging for all commands in a CLI session, use the following command: `cliconfig pager enabled false`
- Type `Q` or CTRL-C to exit the pager display.

2.1.3 Difference Between Show Config and Show State

`show config` displays the configuration settings, while `show state` displays the run time state of the configuration. As a result, `show state` generally includes the items in `show config`, plus additional runtime information. This is an example.

Figure 18 `show config` Vs `show state`

```
usgflex200hp> show config nebula
nebula
    enabled true
usgflex200hp> show state nebula
nebula
    enabled true
    callhome-status Connected
 operating-status CLOUD
        ..
    port-status
        epoch 1760432927
        port 1
            link-up-type copper
            high-speed 1000
            duplex-mode full
            ..
        port 2
            link-up-type down
            ..
        port 3
            link-up-type down
            ..
        port 4
            link-up-type down
            ..
        port 5
:
```

2.1.4 Remove a Configuration Error Prompt

If you see a prompt with an exclamation mark (!) at the end, it means that there is an error in the configuration.

Figure 19 Configuration Error Prompt

```
usgflex500h running config# vrf main interface vlan vlan100 vlan-id 100
usgflex500h running config#!
```

However, you will not see what the error is until you commit the configuration. In the following example, the VLAN was not linked with a port first.

Figure 20 Committed Configuration with Error

```
usgflex500h running config# vrf main interface vlan vlan100 vlan-id 100
usgflex500h running config#! commit
ERROR: [LY] / vrf main interface vlan vlan100:
  Too few "link-port" elements.
ERROR: Invalid configuration, cannot commit.
usgflex500h running config#!
```

In the following example, a role was not set for the user.

Figure 21 Committed Configuration with Error

```
usgflex200hp> edit running
usgflex200hp running config# object user-object user test
usgflex200hp running user test#! show config
user test
    logon-lease-time default
    logon-reauth-time default
    ..
usgflex200hp running user test#! commit
ERROR: [LY] / object user-object user test:
  Missing required element "role" in "user".
ERROR: Invalid configuration, cannot commit.
usgflex200hp running user test#!
```

In the following example, the interface type was not set to external.

Figure 22 Committed Configuration with Error

```
usgflex200hp> edit running
usgflex200hp running config# vrf main interface pppoe pppoe01
usgflex200hp running pppoe pppoe01#! link-interface ge1
usgflex200hp running pppoe pppoe01# type internal
usgflex200hp running pppoe pppoe01#! commit
ERROR: [LY] / vrf main interface pppoe pppoe01 type internal:
  Must condition ". = 'external'" not satisfied.
ERROR: Invalid configuration, cannot commit.
       usgflex200hp running pppoe pppoe01#!
```

2.2 Admin

Use these commands to change the name of the Zyxel Device in your network and manage administrators of the Zyxel Device.

2.2.1 Change the Default Host Name

Use these commands to display the name of the Zyxel Device in your network. You may want to change the default host name to distinguish it from other Zyxel Devices in your network.

Figure 23 Show Hostname

```
usgflex500h> show state system hostname
hostname usgflex500h
usgflex500h> edit running
usgflex500h running config# system hostname 2Foffice
usgflex500h running config# commit
Configuration committed.
usgflex500h running config#
```

2.2.2 Edit / Admin Administrator or User Account

Use the below commands to create a new user account **Max** with unique password and a 60 minute idle timeout.

Figure 24 Create a New Account

```
usgflex200hp> edit running
usgflex200hp running config# object user-object user Max role user
usgflex200hp running config# object user-object user Max
usgflex200hp running user Max# password
Enter value for password>
Confirm value for password>
usgflex200hp running user Max# logon-lease-time 60
usgflex200hp running user Max# logon-reauth-time 0
```

2.3 Interfaces and Ports

Use these commands to manage interfaces and ports on the Zyxel Device.

2.3.1 Show Interface Information

Use this command to display an overview of the interfaces.

Figure 25 Show Interface Information

```
usgflex500h> show interface
No.Name          Status    Ip Address                                IP Assignment  Interface
Type
=============================================================================================
1  ge2           DOWN      0.0.0.0/0                                  Dynamic        ethernet
2  ge1           UP        172.21.x.x/22                             DHCP client    ethernet
                           fe80::daec:e5ff:fe60:94fe/64                  Link Local
3  ge3           DOWN      192.168.168.1/24                           Static         ethernet
                           fe80::daec:e5ff:fe60:9500/64                  Link Local
4  ge4           DOWN      192.168.169.1/24                           Static         ethernet
                           fe80::daec:e5ff:fe60:9504/64                  Link Local
5  cat           DOWN      fe80::daec:e5ff:fe60:9509/64               Link Local     ethernet
6  DMZ           DOWN      fe80::daec:e5ff:fe60:9505/64               Link Local     ethernet
7  vti_custom_1009UP       169.254.148.254/32                            Static
legacy_vti
                           fe80::5efe:a9fe:94fe/64                       Link Local
=============================================================================================
usgflex500h>
```

2.3.2 Assign a Dynamic IP Address to an Interface

Use this command to allow a specific Zyxel Device interface to receive a dynamic IP address. Then use the show command to verify the change.

Figure 26 Assign a Dynamic IP to an Interface

```
usgflex500h running config# vrf main interface ethernet ge1 ipv4 dhcp enabled true

usgflex500h running config# show interface name ge1
No.Name          Status    Ip Address                                IP Assignment  Interface
Type
=============================================================================================
1  ge1            UP        172.21.x.x/22                              DHCP client    ethernet
                             fe80::daec:e5ff:fe60:94fe/64                  Link Local
=============================================================================================
usgflex500h running config#
```

2.3.3 Assign a Static IP Address to an Interface

Use this command to specify a fixed IP address of 172.16.100.100 to Zyxel Device interface ge2.

Figure 27 Assign a Static IP to an Interface

```
usgflex500h running config# vrf main interface ethernet ge2 ipv4 address 172.16
.100.100
```

2.3.4 Display Interface Statistics

Use this command to display interface statistics.

Figure 28 Display Interface Statistics

```
usgflex500h running config# show fast-path statistics interface all
show-fast-path-statistics
    interface lo-vr0
        accelerated false
        input-bytes 0
        input-errors 0
        input-last-error 0
        input-multicasts 0
        input-packets 0
        output-bytes 0
        output-errors 0
        output-packets 0
        ..
    interface ifb1-vr0
        accelerated false
        input-bytes 0
        input-errors 0
        input-last-error 0
        input-multicasts 0
        input-packets 0
        output-bytes 0
        output-errors 0
        output-packets 0
        ..........................
usgflex500h running config#
```

2.3.5 Show Port Information

Use these commands to display Zyxel Device port status, details and statistics.

2.3.6 Show Port Status

Use this command to display Zyxel Device port status.

Figure 29 Show Port Status

```
usgflex500h> show port status
show-port-status-cli
    ok
        port-list 1
            name p1
            status 100M/Full
            ..
        port-list 2
            name p2
            status Down
..........
```

2.3.7 Show Port Throughput

Use this command to display port throughput.

Figure 30 Show Port Throughput

```
usgflex500h> show port throughput
show-port-statistics
    ok
        port-list 1
            name P1
            rx_bps 18089.6
            tx_bps 3462.4
            ..
        port-list 2
            name P2
            rx_bps 0.0
            tx_bps 0.0
.......................
```

2.3.8 Show Port Statistics

Use this command to display port statistics.

Figure 31 Show Port Statistics

```
usgflex500h> show-port-statistics-detail
    ok
        port-list 1
            name p1
            rx_bytes 0
            rx_pkts 0
            rx_errs 0
            tx_bytes 4751291
            tx_pkts 8236
            tx_errs 0
            tx_colls 0
            uptime 115
            ..
        port-list 2
            name p2
            rx_bytes 281474561465440
            rx_pkts 4204252
            rx_errs 3879722144
            tx_bytes 0
            tx_pkts 281474561465504
            tx_errs 2512205668
            tx_colls 0
            uptime 0
-------------------------
```

2.4 Security

Use these commands to manage security settings on the Zyxel Device.

2.4.1 Show Signature Update Status

These commands show the last system protection signature update and the version number.

```
Router# show system protection signature update status
show-system-protection-signature-update-status
    ok
        status "System protection signature is updated to the latest version
2.1.99.20250801.8. (success) at Thu Oct 23 07:54:01 2025
         last update time: 2025-10-23 07:54:01"
         ..
    ..
Router# show ip-reputation-signature-version
ip-reputation-signature-version
    ok
         current-version 1.0.0.20250921.0
         signature-number 439742
         released-date "2025-09-22 02:31:23"
         ..
    ..
```

2.4.2 Show LED Alert if the License Has Expired

Use this command to have the **USER** LED blink green to alert you if your license has expired. You cannot use the security features on the Zyxel Device if your license has expired. Your network will be unprotected and security statistics will not update.

Figure 32 Show LED Alert if the License Has Expired

```
usgflex500h running config# system user-defined-led type
license_expired(green_blinking)
usgflex500h running config#
```

2.4.3 Enable / Disable Web Configurator Security Best Practice Wizard

The Security Best Practice wizard appears after each login to remind you of the recommended security settings. Use this command to disable the Security Best Practice wizard on every login to the web configurator.

Figure 33 Enable Security Best Practice Wizard

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# gui system security-best-practice-wizard-display
false
MyUSGFLEX500H running config# commit
Configuration committed.
```

2.4.4 Enable / Disable Security

Use this command to enable security on the Zyxel Device.

Type `vrf main secure-policy enabled false` to disable all security policies.

Note: This is only recommended for temporary remote access or debugging of the Zyxel Device.

Figure 34 Enable Security

```
usgflex500h running config# vrf main secure-policy enabled true
```

2.4.5 Display Security Policy Settings

Use this command to display security policy settings on the Zyxel Device.

Figure 35 Display Security Policy Settings

```
usgflex500h running config# show config vrf main secure-policy
secure-policy
    enabled true
    asymmetrical-route enabled false
    rule LAN_Outgoing
        user any
        schedule any
        from LAN
        source-ip any
        to any
        destination-ip any
        service any
        action allow
        logging no
        content-filter-profile profile none log by-profile enabled true
        ssl-inspection-profile profile none log by-profile enabled true
        app-patrol-profile profile none log by-profile enabled true
        enabled true
        ..
secure-policy
    enabled true
    asymmetrical-route enabled false
    rule LAN_Outgoing
        user any
        schedule any
        from LAN
        source-ip any
        to any
        destination-ip any
        service any
        action allow
        logging no
        content-filter-profile profile none log by-profile enabled true
        ssl-inspection-profile profile none log by-profile enabled true
        app-patrol-profile profile none log by-profile enabled true
        enabled true
        ..
    rule DMZ_to_WAN
        user any
        schedule any
        from DMZ
        source-ip any
:.............................
```

2.4.6 Display Security Settings and Matching Packets

Use this command to display security settings and matching packets (“hits”) on the Zyxel Device.

Figure 36 Display Security Settings and Matching Packets

```
usgflex500h running config# show state vrf main secure-policy
secure-policy
    enabled true
    asymmetrical-route enabled false
    rule LAN_Outgoing
        user any
        schedule any
        from LAN
        source-ip any
        to any
        destination-ip any
        service any
        action allow
        logging no
        content-filter-profile profile none log by-profile enabled true
        ssl-inspection-profile profile none log by-profile enabled true
        app-patrol-profile profile none log by-profile enabled true
        enabled true
        hits 1838
        ..
    rule DMZ_to_WAN
        user any
        schedule any
        from DMZ
        source-ip any
        to WAN
        destination-ip any
        service any
        action allow
        logging no
        content-filter-profile profile none log by-profile enabled true
        ssl-inspection-profile profile none log by-profile enabled true
        app-patrol-profile profile none log by-profile enabled true
        enabled true
        hits 0
        ..
    rule IPSec_VPN_Outgoing
        user any
        schedule any
        from IPSec_VPN
        source-ip any
        to any
        destination-ip any
        service any
        action allow
        logging no
        content-filter-profile profile none log by-profile enabled true
        ssl-inspection-profile profile none log by-profile enabled true
        app-patrol-profile profile none log by-profile enabled true
        enabled true
        hits 0
        ..
    ::.............................
```

2.4.7 Collect and Display Application and Security Statistics

Use these commands to:

- Enable collection of the specified security statistics
- Display a summary of the specified security statistics collected.

App Patrol

Figure 37 Enable and Display App Patrol Statistics

```
usgflex500h running config# vrf main app-patrol statistics enabled true
usgflex500h running config# show state vrf main app-patrol statistics top-entry
usage entry
```

Anti Malware

Figure 38 Enable and Display Anti-Malware Statistics

```
usgflex500h running config# vrf main anti-malware statistics enabled true
usgflex200hp running config# show state vrf main anti-malware statistics summary
```

IP Reputation

Figure 39 Enable and Display IP Reputation Statistics

```
usgflex500h running config# vrf main ip-reputation statistics enabled true
usgflex500h running config# show state vrf main ip-reputation summary
```

IPS

Figure 40 Enable and Display IPS Statistics

```
usgflex500h running config# vrf main ips statistics enabled true
usgflex500h running config# show state vrf main ips statistics summary
```

Content Filtering

Figure 41 Enable and Display Content Filtering Statistics

```
usgflex500h running config# vrf main content-filter statistics enabled true
usgflex500h running config# vrf main content-filter statistics summary
```

Sandboxing

Figure 42 Enable and Display Sandboxing Statistics

```
usgflex500h running config# vrf main sandbox statistics enabled true
usgflex500h running config# show state vrf main sandbox statistics summary
```

SSL Inspection

Figure 43 Enable and Display SSL Inspection Statistics

```
usgflex500h running config# vrf main ssl-inspection statistics enabled true
usgflex500h running config# show state vrf main ssl-inspection statistics summary
```

2.5 Firmware Management

Use these commands to manage firmware on the Zyxel Device.

2.5.1 Show the Firmware Version

This command shows if you're using the latest firmware. Both firmware partitions are shown below, but the default display is one partition in the web configurator.

Use `gui system standby-firmware-display true` to display both partitions in the web configurator.

Figure 44 Show the Firmware Version

```
usgflex500h running config# show version
show-version
    firmware 1
        model-id "USG FLEX 500H"
        firmware-version V1.21(ABZH.0)b6
        build-date "2024-06-28 14:17:42"
        boot-status Standby
        ..
    firmware 2
        model-id "USG FLEX 500H"
        firmware-version V1.21(ABZH.0)
        build-date "2024-07-11 06:36:27"
        boot-status Running
        ..
    ..
usgflex500h running config#
```

2.5.2 Display LED Alert if There is New Firmware

Use this command to have the **USER** LED blink green to alert you if there is new firmware available on Cloud Helper.

Figure 45 Display LED Alert if There is New Firmware

```
usgflex500h running config# system user-defined-led type
new_firmware_available(green_blinking)
usgflex500h running config#
```

2.5.3 Download the Latest Firmware From Cloud Helper

Use the command to download the latest firmware on the Cloud Helper server to the specified partition on the Zyxel Device, 1 in this example. Then use the second command to automatically reboot the Zyxel Device after the firmware is downloaded.

Figure 46 Download the Latest Firmware From Cloud Helper and Reboot

```
usgflex500h running config# cmd cloud-helper get firmware 1
OK
usgflex500h running config# cloud-helper firmware auto-reboot true
usgflex500h running config#
```

2.5.4 Upload Firmware Using the CLI

This command uploads the specified firmware (“latestFW”) to firmware partition 1 on the Zyxel Device.

Note: Do not turn off the Zyxel Device while the firmware is uploading.

Figure 47 Upload Firmware Using the CLI

```
usgflex500h running config# cmd firmware upgrade-1 image latestFW
command successful
usgflex500h running config#
```

2.5.5 Upload Firmware From Your Computer Using FTP

You may also use FTP to upload the firmware to the Zyxel Device if the FTP server is enabled on the Zyxel Device. You must first download the firmware from the website to a specific path on your computer. Then open the command prompt on your computer and run the following commands.

Note: Do not turn off the Zyxel Device while the firmware is uploading.

Figure 48 Upload Firmware From Your Computer Using FTP I

```
C:\Users\User.xxxx>ftp 172.21.x.x (IP address of the Zyxel Device)
Connected to 172.21.x.x.
220 FTP Server (FTP Server) [::ffff:172.21.x.x]
500 OPTS UTF8 not understood
User (172.21.x.x:(none)): admin
331 Password required for admin
Password:
230 User admin logged in
ftp> bin
200 Type set to I
ftp> put <firmware path on computer> <firmware name>
```

2.5.6 Specify Firmware Boot Partition

This command specifies which firmware boot partition, 1 in this example, to use when the Zyxel Device reboots.

Figure 49 Specify Firmware Boot Partition

```
usgflex500h running config# boot-number 1
command successful
usgflex500h running config#
```

2.6 Configuration File Management

Use these commands to view, back up or restore a configuration file.

2.6.1 See the Current Configuration

Type `show config text` or `json` or `xml` to see the current configuration in text, JSON or XML format.

Use the below command to see the current running configuration of a specific item in text format.

Figure 50 See Current Running Configuration

```
usgflex500h running config# show config text running
all                 nodefault           with-deprecated     absolute
relative            fullpath            dry-run             /
system              configuration       aaa                 object
notification        diagnostics         geoip               cloud-helper
logging             gui                 two-factor-auth     poe
nebula              vrf                 switch              running
startup             staging             origin              file
```

2.6.2 See the Startup Configuration

Type `show config startup text` or `json` or `xml` to see the startup configuration in text, JSON or XML format.

Use the below command to see the startup configuration on screen.

Figure 51 See Startup Configuration

```
usgflex500h running config# show config startup
vrf main
    system
        default-interface-group
            algorithm wrr
            ..
        ..
    dos-prevention
        enabled true
        profile DOS_PREVENTION_PROFILE
            scan-detection
                sensitivity medium
                block-period 5
                ip-protocol-scan
                    action block
                    enabled true
                    logging log
                    ..
                tcp-portscan
                    action block
                    enabled true
                    logging log
                    ..
                udp-portscan
```

2.6.3 See the Staging Configuration

The staging configuration displays configurations made but not yet committed. For example, I create an address object, and then use the show staging command with match to see the change.

Figure 52 See Staging Configuration

```
usgflex500h running config# object address-object address H1.1.1.1 type host
1.1.1.1
usgflex500h running config# show config staging | match "H1.1.1.1"
        address H1.1.1.1 type host 1.1.1.1
```

You can also use the `Diff` command to see what configurations you made, but have not yet saved (`commit`).

Figure 53 Diff

```
usgflex500h running config# diff
=== / object address-object
+ address H1.1.1.1 type host 1.1.1.1
usgflex500h running config#
```

2.6.4 Back Up a Configuration

You should regularly back up configurations so that you may use a previously saved good configuration if there are errors in the current configuration.

First copy an existing (good) configuration as shown in the next example where “lastgood.conf” is copied to “currentgood_2024-7-30.conf” on the Zyxel Device. If you want to download this configuration file to your computer, you must use the **Maintenance > Firmware/File Manager > Configuration File** menu in the web configurator or FTP.

Figure 54 Copy a Good Configuration

```
usgflex500h running config# cmd config-copy from lastgood.conf to
currentgood_2024-7-30.conf
configuration-copy
    ok
        message OK
        ..
    ..
usgflex500h running config#
```

Alternatively, you could email the specified configuration to previously configured email addresses using this command.

Figure 55 Email a Good Configuration

```
usgflex500h running config# cmd config-mail send-now currentgood_2024-7-30.conf
usgflex500h running config#
```

2.6.5 Restore a Configuration

Use this command to replace the current configuration with a previously saved configuration on the Zyxel Device. You may want to do this if recent configuration changes have caused unknown errors.

Figure 56 Apply a Previously Saved Configuration

```
usgflex500h running config# cmd config-apply startup-config_2024-7-30.conf
configuration-apply
    ok
        message OK
        ..
    ..
usgflex500h running config#
```

See the next section for how to copy the current configuration to the system default current configuration, that is, reset the Zyxel Device to the factory defaults.

2.7 Wireless Management

Use these commands to view and configure the managed APs and the WiFi stations.

2.7.1 See the Managed APs’ Status

Use the following commands to view the specified status of the managed APs.

Figure 57 Current Managed APs' Status

```
MyUSGFLEX500H running config# show state apc ap
ethernet            smart-mesh-status       custom-port-setting    hw-capability
sw-capability       custom-radio-setting    slot                   ap-mac
index               online                  status                 error-message
config-status       ap-ip                   description            model
usage               cpu-usage               station                radio-num
ac-vlan-id          wtp-vlan-id             wtp-vlan-tag           fw-version
primary-ac-ip       secondary-ac-ip         recent-online          last-offline
loop-status         ed-status               suppress-mode-status   power-mode
locator-led-status  locator-led-time        locator-led-lease      roaming-group
load-balancing-group                        selectable-antenna-status
fw-available         compatible              port-num               conflict
non-support          ethernet-storming       ethernet-uplink        ble-status
nebula-flex-status   serial-number           group                  location
sysname              override-tag
```

2.7.2 See the WiFi Clients' Status

Use the following command to view the status and traffic usage of connected WiFi clients.

Figure 58 See the WiFi Clients' Status

```
MyUSGFLEX500H running config# show state apc station
station
    sta-mac 02:AA:BB:CC:DD:EE
    index 1
    hostname ""
    associated-ap AP-2
    group-of-ap -APGroup_test2
    ssid SSID_TW
    security WPA3-Personal
    channel 40
    band 5GHz
    signal-strength "-57 dbm"
    ipv4-address 192.168.167.41
    tx-rate 306M
    rx-rate 324M
    upload "268.45 KB"
    download "22.00 KB"
    usage "290.45 KB"
    association-time "2026/01/23 14:42:55"
    capability 802.11be
    dot11-features N/A
    vlan 1
    ..
```

2.7.3 Block a WiFi Client from the WiFi Network

Use the following commands to prevent the WiFi client from connecting to the specified WiFi network. In the following example, you want to block the WiFi client with MAC address 02:11:22:33:44:66 from the WiFi network ssid-1-1.

Figure 59 Block a WiFi Client from the WiFi Network

```
MyUSGFLEX500H running config# wlan-setting macfilter-profile macfilter-1-1 mac
02:11:22:33:44:66 ff:ff:ff:ff:ff:ff filter-type block
MyUSGFLEX500H running config# wlan-setting ssid-profile ssid-1-1 macfilter-action
block
MyUSGFLEX500H running config# commit
Configuration committed.
```

2.8 Troubleshooting

Use these commands if you are having problems with your Zyxel Device.

2.8.1 Restart the Zyxel Device

If the Zyxel Device is unstable or you want to use firmware from another partition, then use this command to restart the Zyxel Device.

Figure 60 Restart Zyxel Device

```
usgflex500h> edit running
usgflex500h running config# cmd reboot
System will reboot on Wed 2024-07-31 10:40:10
```

2.8.2 Restart the NCC Connection

Nebula Cloud Center (NCC) is a cloud-based management tool. Use this command if your Zyxel Device is managed by NCC and is having connection problems with NCC. This command will restart the connection to NCC.

Figure 61 Restart NCC Connection

```
usgflex500h> edit running
usgflex500h running config# cmd debug nebula callhome restart
debug-nebula-callhome-restart
    ok
```

2.8.3 Reset the Configuration to the Factory Defaults

If you forgot your user name or password, use this command to return the Zyxel Device to the default configuration using the system-default.conf file.

Note: All configuration files including those you saved on the Zyxel Device will be deleted. The **Login** password returns to the password on the back label or 1234, and the LAN IP address returns to 192.168.168.1.

License registration bindings, IPSec certificates, remote access VPN certificates, trusted certificates and two-factor authentication (2FA) information are retained.

Figure 62 Apply the System Default Configuration

```
usgflex500h running config# cmd config-apply system-default.conf
    ok
        message OK
        ..
    ..
usgflex500h running config#
```

2.8.4 Display Management Logs

Use this command to display a certain number of the latest management logs. The logs include:

- Booting time and from which partition
- When and how firmware was upgraded

Figure 63 Display Management Logs

```
usgflex500h> edit running
usgflex500h running config# cmd debug show sys-mgnt-log max-lines <number>
```

This is an example.

Figure 64 Display Management Logs Example

```
usgflex500h running config# cmd debug show sys-mgnt-log max-lines 10
[2024-04-01 17:14:04][2][1.20(ABZH.0)b5s1][CGI][file_upload] Firmware upgrading,
partition:1
[2024-04-01 17:17:51][1][1.20(ABZH.0)b6] Booting time: 146 seconds (70 services
loaded)
[2024-04-11 10:36:57][1][1.20(ABZH.0)b6][FTP] Firmware upgrading, file: /db/etc/
zyxel/ftp/firmware1/120ABZH0b6s1.bin
[2024-04-11 10:40:31][1][1.20(ABZH.0)b6s1] Booting time: 143 seconds (71 services
loaded)
[2024-04-15 15:27:44][1][1.20(ABZH.0)b6s1][CGI][file_upload] Firmware upgrading,
partition:2
[2024-04-15 15:31:24][2][1.20(ABZH.0)b7] Booting time: 148 seconds (70 services
loaded)
[2024-04-16 10:23:27][2][1.20(ABZH.0)b7][CGI][file_upload] Firmware upgrading,
partition:1
[2024-04-16 10:27:06][1][1.20(ABZH.0)] Booting time: 148 seconds (70 services
loaded)
[2024-04-23 10:22:00][1][1.20(ABZH.0)][CGI][file_upload] Firmware upgrading,
partition:2
[2024-04-23 10:25:43][2][1.20(ABZH.0)] Booting time: 149 seconds (70 services
loaded)
usgflex500h running config#
```

2.8.5 Display Kernel Console Level

Customer support may require you to use this command to display the kernel console log level for troubleshooting. All kernel messages with a log level smaller than the console log level will be printed to the console command line interface. The log levels are defined as follows:

Table 7 Kernel Log Console

0 (KERN_EMERG)	System is unusable
1 (KERN_ALERT)	Action must be taken immediately
2 (KERN_CRIT)	Critical conditions
3 (KERN_ERR)	Error conditions
4 (KERN_WARNING)	Warning conditions
5 (KERN_NOTICE)	Normal but significant condition
6 (KERN_INFO)	Informational
7 (KERN_DEBUG)	Debug-level messages

The default log level is 1, so only KERN_EMERG and KERN_ALERT log types are printed to the console command line interface.

Figure 65 Show Kernel Log Console Level

```
usgflex500h> edit running
usgflex500h running config# cmd debug kernel console-level show
kernel console-level: 1
usgflex500h running config#
```

2.8.6 Activate a Remote Support Account

If you need outside help with your Zyxel Device configuration, then enable the following command to allow an external administrator to log in and diagnose the problem. You must also set the allowed time for external access to one day, two days or one week. Make sure the Zyxel Device has Internet access.

Figure 66 Allow External Access

```
usgflex500h running config# cmd users remote-support-account enabled true expire-
time two-days
set-remote-support-account
    ok
        msg ok
        ..
    ..
usgflex500h running config#
```

Use the `false` option to turn off external access to your Zyxel Device.

Figure 67 Disallow External Access

```
usgflex500h running config# cmd users remote-support-account enabled false
set-remote-support-account
    ok
        msg ok
        ..
usgflex500h running config#
```

Part II
Reference

CHAPTER 3
Object Reference

This chapter describes how to use object reference commands.

3.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specific object. You can use this table when you want to delete an object because you have to remove references to the object first.

Table 8 `show reference` Commands

COMMAND	DESCRIPTION
`show reference object address [object_name]`	Displays which configuration settings reference the specified address object.
`show reference object address-group [object_name]`	Displays which configuration settings reference the specified address group object.
`show reference object service [object_name]`	Displays which configuration settings reference the specified service object.
`show reference object service-group [object_name]`	Displays which configuration settings reference the specified service group object.
`show reference object schedule [object_name]`	Displays which configuration settings reference the specified schedule object.
`show reference object schedule-group [object_name]`	Displays which configuration settings reference the specified schedule group object.
`show reference object zone [object_name]`	Displays which configuration settings reference the specified zone object.
`show reference object user [username]`	Displays which configuration settings reference the specified user object.
`show reference object user-group [username]`	Displays which configuration settings reference the specified user group object.
`show reference object {aaa-radius| aaa-ldap| aaa-ad} [object_name]`	Displays which configuration settings reference the specified AAA RADIUS, AAA LDAP or AAA AD group object.
`show reference profile {app-patrol| content-filter| dos-prevention| ssl-inspection| certManager}`	Displays which configuration settings reference the specified: • App patrol profile. • Content filter profile. • DoS prevention profile. • SSL inspection profile. • Certificate profile.

3.1.1 Object Reference Command Example

This example shows how to check which configuration is using the HTTP service.

```
usgflex200hp> show reference object service HTTP
show-reference-object
    ok
        reference 1
            category "Service Group"
            sub_category ""
            priority ""
            rule_name Default_Allow_WAN_To_ZyWALL
            description ""
```

CHAPTER 4
Status

This chapter explains some commands you can use to display information about the Zyxel Device's current operational state.

4.1 Show Commands

These commands display the status of certain features.

Table 9 Status Show Commands

COMMAND	DESCRIPTION
`show config`	Displays the settings you configured.
`show state`	Displays the status of the specified settings.
`show all`	Displays all settings in the specified category.
`show fullpath`	Displays all settings in the specified category.
`show bgp`	Displays border gateway protocol (BGP) information.
`show object`	Displays the Zyxel Device zones.
`show geo-ip`	Displays the Geo IP database and country list.
`show cloud-helper`	Displays cloud helper firmware information and download status.
`show debug myzyxel-server status`	Displays myzyxel server status.
`show fast-path`	Displays fast-path memory, cpu-usage, table-usage and service statistics.
`show interface`	Displays the Zyxel Device interfaces information.
`show certificate`	Displays the Zyxel Device certificates information.
`show filter`	Displays the protocols list.
`show ntp`	Displays network time protocol (NTP) information.
`show port status`	Displays the Zyxel Device ports status.
`show conn filter`	Displays all established sessions that pass through the Zyxel Device.
`show firmware`	Displays the Zyxel Device firmware and reboot options.
`show gui dashboard resource local-usage`	Displays the used space (in MB or GB), available space (in MB or GB), and the percentage of used space on the Zyxel Device. Local storage refers to the permanent (flash) memory, where data is retained after rebooting. It stores database files, including actual data, logs, backups, packet capture files, and configuration files. New logs and files are not saved when storage is full.
`show gui dashboard boot-status`	Displays when the Zyxel Device was last updated with new firmware. For example, 'status OK. detail "Firmware update at 2024-02-02 09:31"'
`show certManager`	Displays the Zyxel Device SSL certificate.

Table 9 Status Show Commands (continued)

COMMAND	DESCRIPTION
show reference	Displays which configuration settings reference a specific object.
show logging	Displays the logs.
show summary	Displays a summary of the Zyxel Device system status.
show conntracks	Displays connection tracking records.
show product	Displays the Zyxel Device model name and firmware version.
show date	Displays the current date of your Zyxel Device.
show neighbors	Displays neighbors information.
show ipv4-routes	Displays the IPv4 routing table.
show ospf	Displays OSPFv2 information.
show dhcp-server	Displays the DHCP unique identifier (DUID).
show dns-server	Displays DNS server information.
show ike	Displays security association (SA) status.
show log	Displays log information.
show rip	Displays RIP information.
show version	Displays the Zyxel Device firmware information.
show users	Displays the Zyxel Device user accounts login information.
show lockout-users	Displays the user accounts that are locked out of the Zyxel Device.
show service-inspect	Displays the services available on the Zyxel Device.
show mac	Displays the Zyxel Device MAC address.
show serial-number	Displays the serial number of this Zyxel Device.
show system traffic-statistics-chart summary host_ip filter application <application name>	Displays traffic statistics in a chart by application.
show system traffic-statistics-chart summary application range begin <1 - 1000> end <1 - 1000>	Displays traffic statistics in a chart by range of traffic size.
show system traffic-statistics summary host_ip filter application <application name>	Displays traffic statistics summary of host IP addresses by application.
show system traffic-statistics summary host_ip range begin <1 - 1000> end <1 - 1000>	Displays traffic statistics summary of host IP addresses by range of IP addresses.
show system database status	Displays the number of traffic sessions that went through the Zyxel Device and the file size in the database. for example, “session_count 10000, db_usage "7673 kB”.
show service-register status	Displays if services are active and when they expire.

Table 9 Status Show Commands (continued)

COMMAND	DESCRIPTION
`show lldp config`	Displays LLDP configuration status. LLDP (Link Layer Discovery Protocol) is a non-proprietary link layer protocol for LAN devices to transmit device information such as chassis identification, port ID, port description, system name, device role (such as router, switch, hub), IP/MAC address, and so on, to directly connected neighbors. This information is also stored in local Management Information Databases (MIBs), and can be queried with the Simple Network Management Protocol (SNMP).
`show lldp status`	Displays LLDP statistics
`show lldp local`	Displays Zyxel Device LLDP information.
`show lldp remote`	Displays LLDP information of the device connected to the Zyxel Device.
`show apc license count`	Displays the number of APs managed by this Zyxel Device (the AP Controller).

4.2 Command Examples

User Account Information on page 63

MAC Address, Serial Number, and Firmware Version on page 64

Interface Information on page 64

Port Information on page 65

System Uptime on page 65

LLDP Commands on page 66

Status of Services on page 68

Session Monitor on page 68

4.2.1 User Account Information

Use `show users` to display user accounts that have logged into the Zyxel Device. The unique value only displays for logged in user running this command.

```
usgflex500h> show users
show-users
    admin-list Boss
        role admin
        from console
        tunnel-ip 0.0.0.0
        service console
        login-time 6:19:14
        lease-timeout 17:40:52
        reauth-timeout 17:40:46
        user-info admin(Boss)
        unique ttyS1
        ..
    admin-list Boss
        role admin
        from 172.21.x.x
        tunnel-ip 0.0.0.0
        service http/https
        login-time 6:17:28
        lease-timeout 23:31:07
        reauth-timeout 17:42:32
        user-info admin(Boss)
        unique FLNxNgteL2aFy9MtLgrHTtz0pgtWHBAgJqlObG1OO6Fqsg5GmlFtqPLYcu2zoD+-
        ..
    admin-list Boss
        role admin
        from 172.21.x.y
        tunnel-ip 0.0.0.0
        service ssh
        login-time 3:31:23
        lease-timeout 23:59:55
        reauth-timeout 20:28:37
        user-info admin(Boss)
        unique /dev/pts/0
        ..
```

4.2.2 MAC Address, Serial Number, and Firmware Version

Here are examples of the commands that display the MAC address, serial number, and firmware version.

```
usgflex200hp> show mac
MAC address: D8:EC:E5:5C:0D:04-D8:EC:E5:5C:0D:0C
usgflex200hp> show serial-number
serial number: S212L16295036
usgflex200hp> show version
show-version
    firmware 1
        model-id "USG FLEX 200HP"
        firmware-version 7.00(ABXE.0)b2
        build-date "2022-08-30 14:58:48"
        boot-status Standby
        ..
    firmware 2
        model-id "USG FLEX 200HP"
        firmware-version 1.00(ABXE.0)b2s1
        build-date "2022-09-21 11:55:41"
        boot-status Running
```

4.2.3 Interface Information

Here is an example of the command that displays the Zyxel Device interfaces information.

```
usgflex200hp> show interface
No.Name           Status    Ip Address              IP Assignment  Interface  Type
================================================================================
====================
0  ge1            DOWN      fe80::daec:e5ff:fe5c:d04/64   Link Local   ethernet
1  ge2            DOWN      fe80::daec:e5ff:fe5c:d05/64   Link Local   ethernet
2  ge3            DOWN      192.168.168.1/24              Static       ethernet
                            fe80::daec:e5ff:fe5c:d06/64   Link Local
3  ge4            DOWN      192.168.169.1/24              Static       ethernet
                            fe80::daec:e5ff:fe5c:d0a/64   Link Local
================================================================================
```

4.2.4 Port Information

Here is an example of the command that displays the ports information.

```
usgflex200hp> show port statistic
show-port-statistics
    ok
        port-list 1
            name p1
            rx_bypes 0
            rx_pkts 0
            rx_errs 0
            rx_drops -2007148728
            rx_bps 0
            tx_bytes 0
            tx_pkts 0
            tx_errs 0
            tx_colls 0
            tx_bps 0
            uptime 0
        port-list 2
            name p2
            rx_bypes 0
            rx_pkts 0
            rx_errs 0
            rx_drops -1237797048
            rx_bps 0
            tx_bytes 0
            tx_pkts 0
            tx_errs 0
            tx_colls 0
            tx_bps 0
            uptime 0
        port-list 3
            name p3
            rx_bypes 194620
            rx_pkts 1995
            rx_errs 0
            rx_drops -1183496376
            rx_bps 204
            tx_bytes 1461644
            tx_pkts 1783
            tx_errs 0
            tx_colls 0
            tx_bps 162
            uptime 69
```

4.2.5 System Uptime

Here are examples of the commands that display the system uptime.

```
usgflex200hp> show system uptime
show-uptime
    ok
        uptime 0:12:09
```

4.2.6 LLDP Commands

Here are examples of using the LLDP commands to display device information.

This command shows the LLDP configuration status.

```
usgflex500h> show lldp config
show-lldp-config
    lldpMessageTxInterval 30
    lldpMessageTxHoldMultiplier 0
    lldpReinitDelay 1
    lldpTxDelay 1
    lldpNotificationInterval 5
    ..
```

This command shows LLDP statistics.

```
usgflex500h> show lldp status
show-lldp-status
    epoch 1727160381968
    lldpStatsRemTablesLastChangeTime 172714197200
    lldpStatsRemTablesInserts 4
    lldpStatsRemTablesDeletes 2
    lldpStatsRemTablesDrops 0
    lldpStatsRemTablesAgeouts 0
    lldpStatsTxPortEntry
        lldpStatsTxPortNum 1
        lldpStatsTxPortFramesTotal 0
        ..
    lldpStatsTxPortEntry
        lldpStatsTxPortNum 2
        lldpStatsTxPortFramesTotal 0
        ..
    lldpStatsTxPortEntry
        lldpStatsTxPortNum 3
        lldpStatsTxPortFramesTotal 0
        ..
    lldpStatsTxPortEntry
        lldpStatsTxPortNum 4
        lldpStatsTxPortFramesTotal 0
        ..
```

This command shows Zyxel Device LLDP information.

```
usgflex500h>  show lldp local
show-lldp-local
    epoch 1727160410932
    lldpLocChassisIdSubtype 4
    lldpLocChassisId BA:05:FB:90:EF:EA
    lldpLocSysName usgflex500h
    lldpLocSysDesc "Buildroot 2020.02.5 Linux 4.14.207-10.3.7.0-2 #5 SMP
PREEMPT Fri Sep 20 19:21:09 UTC 2024 aarch64"
    lldpLocSysCapSupported 156
    lldpLocSysCapEnabled 20
    lldpLocPortEntry
        lldpLocPortNum 1
        lldpLocPortIdSubtype 3
        lldpLocPortDesc ifb0
        ..
    lldpLocPortEntry
        lldpLocPortNum 2
        lldpLocPortIdSubtype 3
        lldpLocPortDesc ifb1
        ..
    lldpLocPortEntry
        lldpLocPortNum 3
        lldpLocPortIdSubtype 3
        lldpLocPortDesc gretap0
```

This command shows LLDP information of the device connected to the Zyxel Device.

```
usgflex500h>  show lldp remote
OK.
usgflex500h>
```

4.2.7 Status of Services

Here is an example of the command that displays the Zyxel Device services information.

```
usgflex500h running config# show service-register status
================================================================================
========
|            service             |                  status                  |
expiration |
================================================================================
========
| Security_Profile_Sync          | Activated                                | 2025/
09/13 |
| SecuReporter                   | Activated                                | 2025/
09/13 |
| Device_Insight                 | Activated                                | 2025/
09/13 |
| Sandboxing                     | Activated                                | 2025/
09/13 |
| Nebula_Professional_Pack       | Activated                                | 2025/
09/13 |
| Reputation_Filter              | Activated                                | 2025/
09/13 |
| Web_Filtering                  | Activated                                | 2025/
09/13 |
| Application_Patrol             | Activated                                | 2025/
09/13 |
| Anti-Malware                   | Activated                                | 2025/
09/13 |
| IPS                            | Activated                                | 2025/
09/13 |
================================================================================
========
License Agent Version: 1.0.0
```

4.2.8 Session Monitor

Here is an example of the command that displays all established sessions that pass through the Zyxel Device for debugging or statistical analysis. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source IP address and country
- Destination IP address and country
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

- BWM rule applied

```
MyUSGFLEX500H> show conn filter
show-conn-filter-cli
    ok
        count 68
        conn 1
            user ctc-users
            service HTTPS
            source 192.168.167.51:65104
            source_country Private_IP
            destination 17.253.117.201:443
            destination_country TW
            rx_bytes 3096
            tx_bytes 1944
            duration 16
            proto 6
            bwm_rule_name BWM2
            ..
        conn 2
            user ctc-users
            service HTTPS
            source 192.168.167.51:65115
            source_country Private_IP
            destination 17.8.131.124:443
            destination_country US
            rx_bytes 3104
            tx_bytes 1981
            duration 14
            proto 6
            bwm_rule_name BWM2
            ..
            .
            .
```

CHAPTER 5
USER LED

5.1 User LED

The **USER** LED is located at the front panel of the Zyxel Device. Use this LED to check one of the following:

- Admin account login status.
- User IP address locked out status.
- License status.
- New firmware available for update.

Use the command to configure one of the following **USER** LED settings. You must use the `edit running` command before you can use the command.

Table 10 USER LED Command

COMMAND	DESCRIPTION
`system user-defined-led type {Admin_login(green_on)| user_lockout(amber_on)| license_expired(green_blinking)| new_firmware_available(green_blinking) | Off}`	Select how you want the **USER** LED to behave. • Select **Admin login (green on)** if you want the **USER** LED to be steady green when there are admin accounts logged into the Zyxel Device. • Select **User Lockout (amber on)** if you want the **USER** LED to be steady amber when a user IP address is locked out of the Zyxel Device. A user IP address will be locked out when the user has logged into the Zyxel Device unsuccessfully (for example, wrong password) for more than three times. • Select **License Expired (green blinking)** if you want the **USER** LED to be steady amber when a Zyxel Device service license has expired. • Select **New Firmware Available (green blinking)** if you want the **USER** LED to blink green when there is new firmware available for upload. • Select **Off** to turn off the **USER** LED.

CHAPTER 6
Interfaces

6.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interfaces can belong to the same zone.

Some characteristics do not apply to some types of interfaces.

6.1.1 Types of Interfaces

You can create several types of interfaces in each Zyxel Device model. The types supported vary by Zyxel Device model.

- **Ethernet interfaces** are the foundation for defining other interfaces and network policies.
- **VLAN interfaces** receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the Zyxel Device. You can also assign an IP address and subnet mask to the bridge.
- **Trunk interfaces** manage load balancing between interfaces.
- **PPPoE interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE interfaces.
- **VPN Tunnel Interface (VTI**) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

Port groups, and trunks have a lot of characteristics that are specific to each type of interface. These characteristics are listed in the following tables and discussed in more detail farther on.

Table 11 Interface Characteristics

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE
Name*	gex	vlanx	brx	pppx
IP Address Assignment				
Static IP Address	Yes	Yes	Yes	Yes
DHCP Client	Yes	Yes	Yes	Yes (Auto)
Interface Parameters				
Packet Size (MTU)	Yes	Yes	Yes	Yes

Table 11 Interface Characteristics (continued)

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE
Data Size (MSS)	Yes	Yes	Yes	Yes
Traffic Prioritization	Yes	Yes	Yes	Yes
DHCP				
DHCP Server	Yes	Yes	Yes	No
DHCP Relay	Yes	Yes	Yes	No
Ping Check	Yes	Yes	Yes	Yes

Note: The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

6.1.2 Relationships Between Interfaces

In the Zyxel Device, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

Table 12 Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	VLAN	PPPOE	BRIDGE
Name*	wan1, wan2	lan1, lan2	vlan*x*	pppx	br*x*
Configurable Zone	No	No	Yes		Yes
IP Address Assignment				Yes	
Static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes
Interface Parameters				Yes	
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes
DHCP				Yes (Auto)	
DHCP server	No	Yes	Yes		Yes
DHCP relay	No	Yes	Yes	No	Yes
Connectivity Check	Yes	Yes	Yes	No	Yes

6.2 Interface Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 13 Interface Command Input Values

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE interfaces your Zyxel Device model supports.
profile_name	The name of the DHCP. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces.

Table 14 Overall Interface Commands

COMMAND	DESCRIPTION
`vrf main interface bridge <interface-name> {ipv4 | default-snat | ping-check | ethernet | ipv6 | network-stack | forward-802dot1x | stp | mtu | promiscuous | enabled | type | description | ageing-time | link-interface}`	Sets the criteria for a selected bridge interface on the Zyxel Device.
`vrf main interface ethernet <interface-name> {default-snat | ping-check | ipv4 | network-stack | ethernet | qos | mtu | promiscuous | enabled | type | description | ports}`	Sets the criteria for a selected Ethernet interface on the Zyxel Device.
`vrf main interface gre <interface-name> {default-snat | ping-check | ipv4 | ipv6 | network-stack | key | mtu | promiscuous | enabled | type | description | ttl | tos | link-interface | link-vrf | local | remote | checksum | sequence-number}`	Sets the criteria for a selected GRE (Generic Routing Encapsulation, for data transmission) interface on the Zyxel Device.

Table 14 Overall Interface Commands (continued)

COMMAND	DESCRIPTION
`vrf main interface lag <interface-name> {ipv4 | default-snat | ping-check | ethernet | ipv6 | network-stack | mtu | promiscuous | enabled | type | description | mode | xmit-hash-policy | lacp-rate | mii-link-monitoring | updelay | downdelay | primary | link-interface}`	Sets the criteria for a selected LAG (Link Aggregation Group, a combined set of physical ports) interface on the Zyxel Device.
`vrf main interface vti <interface-name> {default-snat | ping-check | ethernet | ipv4 | ipv6 | network-stack | mtu | promiscuous | enabled | type | description | vti-mark | local | remote | link-vrf}`	Sets the criteria for a selected VTI (Virtual Tunnel Interface) on the Zyxel Device.
`vrf main interface pppoe <interface-name> {auth | ipcp | ipv6cp | periodical-reconnection | lcp-setting | logging | ping-check | enabled | description | link-interface | type | service-name | ac-name | remote-mac-address | mtu | mru | compression | idle | lcp | request}`	Sets the criteria for a selected PPPoE (Point-to-Point Protocol over Ethernet, PPP frames inside Ethernet frames) on the Zyxel Device.
`vrf main interface vlan <interface-name> {default-snat | ping-check | ethernet | ipv4 | ipv6 | network-stack | mtu | promiscuous | enabled | type | description | vlan-id | protocol | link-vrf | vlan-priority-code | link-interface | link-port}`	Sets the criteria for a selected VLAN (virtual logical network segment} on the Zyxel Device.
`qos policer <profile-name> bandwidth <rate-limit>`	Sets the maximum traffic rate for bandwidth in the QoS policer profile. This profile can be applied to interfaces to control network traffic. `profile-name`: The name of QoS policer profile you want to configure. `rate-limit`: The transfer or receive rate limit. You can enter a number without a unit, which is interpreted as bps (bits per second), or a number followed by a unit, for example, 10G. **Supported units:** • K = Kbps (Kilobits per second) • M = Mbps (Megabits per second) • G = Gbps (Gigabits per second) • T = Tbps (Terabits per Second)

Table 14 Overall Interface Commands (continued)

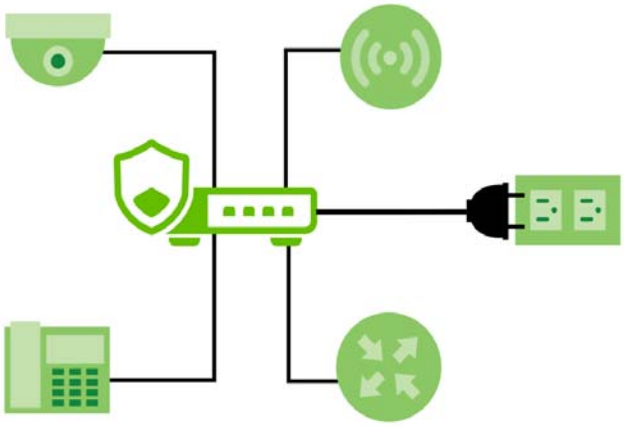
COMMAND	DESCRIPTION
`qos policer <profile-name> burst <burst-size>`	Sets the size of traffic that can pass through when traffic exceeds the bandwidth limit in the QoS policer profile. This prevents packet drops during short-term traffic increases. This profile can be applied to interfaces to control network traffic. `profile-name`: The name of QoS policer profile you want to configure. `burst-size`: The number of bytes for the burst size. The allowed range is 1 to 4,294,967,295 bytes.
`vrf main interface {ethernet | VLAN | bridge | pppoe | lag | legacy-vti} <interface-name> qos [ingress | egress] rate-limit policer <profile-name>`	Applies the ingress and egress rate limit of the QoS policer profile to the specified interface. Refer to the commands above for QoS policer profile rate limit configuration. If you also set a limit using Bandwidth Management Commands, the Zyxel Device will apply the lower value as the limit.

6.3 PoE Overview

The Zyxel Device is a Power Sourcing Equipment (PSE) because it provides a source of power through its Ethernet ports. Each device that receives power through an Ethernet port is a Powered Device (PD). A Powered Device (PD) is a device that receives power through PoE, such as an IP camera, a wireless router, an IP telephone or a general outdoor router.

The following example figure shows a Zyxel Device supplying PoE (Power over Ethernet) to PDs that are not within reach of a power outlet.

Figure 68 PoE Application



6.4 PoE Port Commands

This table lists the PoE port commands.

Table 15 PoE Port Commands

COMMAND	DESCRIPTION
`cmd poe reset-power port <port-number>`	Powers off the PD (powered device) connected to the port, by temporarily disabling then re-enabling PoE.
`show state poe port <port-number>`	Shows the status of the port, including if power is sent to the PD, the current, and the temperature of the port.

6.4.1 PoE Port Command Example

The following command shows you the details for the ports.

```
usgflex500h> edit running
usgflex500h running config# show state poe port
port p3
    pd-enable PORT_ENABLE
    state R_OPEN
    mode AF
    class 5
    power "0.0 W"
    current "0.0 mA"
    temperature 45.875
    ..
port p4
    pd-enable PORT_ENABLE
    state R_GOOD
    mode AF
    class 0
    power "3.703 W"
    current "64.500 mA"
    temperature 44.375
    ..
```

6.5 Ethernet Interface Commands

This table lists the Ethernet interface commands.

Table 16 Ethernet Interface Commands

COMMAND	DESCRIPTION
`vrf main interface ethernet <interface-name> default-snat enabled {true | false}`	Enables default SNAT settings for the specified interface.
`vrf main interface ethernet <interface-name> ipv4 dhcp enabled {true | false}`	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway.

Table 16 Ethernet Interface Commands (continued)

COMMAND	DESCRIPTION
`vrf main interface ethernet <interface-name> ipv4 dhcp dhcp-lease-time <0...4294967295>`	Sets how long the specified interface can use the information (especially the IP address) received from the DHCP server before it has to request the information again. The default value is 7200.
`cmd dhcp-client renew-lease <interface-name>`	Has DHCP clients on the specified interface request their DHCP information again even if the lease time is not up.
`vrf main interface ethernet <interface-name> ipv4 primary-address <ipv4-address>`	This is available only when the interface is not a DHCP client. Sets the primary IP address for this interface to identify the WAN address used for sending traffic with other network devices.
`[del] vrf main interface ethernet <interface-name> ipv4 address <ipv4-address>`	This is available only when the interface is not a DHCP client. Sets up to three secondary public IP addresses to be bound to this interface. You can assign these IP addresses to different servers on the same interface, enabling the servers to receive traffic using different IP addresses and ports. Enter `del` to remove an IP address from the specified interface.
`vrf main interface ethernet <interface-name> ipv4 gateway <ipv4-address>`	Enters the IP address of the router through which this connection will send traffic.
`vrf main interface ethernet <interface-name> enabled {true| false}`	Enables or disables the specified interface.
`vrf main interface ethernet <interface-name> type {internal| external}`	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
`vrf main interface ethernet <interface-name> description <description>`	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/ :=?;!*#@$_%-"
`vrf main interface ethernet <interface-name> mtu <0...4294967295>`	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
`show state vrf main interface`	Displays parameter status, counters and neighbor information for all interfaces.
`show state vrf main interface {bridge | ethernet | gre | lag | legacy-vti} <interface_name>`	Displays parameter status, counters and neighbor information for the specified interface.
`show config vrf main interface`	Displays configuration details for all interfaces.
`show config vrf main interface {bridge | ethernet | gre | lag | legacy-vti} <interface_name>`	Displays configuration details for the specified interface.

6.5.1 Ethernet Interface Command Examples

The following command shows you parameter status, counters and neighbor information for interface ge1, including the type.

```
usgflex500h running config# show state vrf main interface ethernet ge1
ethernet ge1
    mtu 1500
    promiscuous false
    enabled true
    type external
    oper-status UP
    counters
        in-octets 161320368
        in-unicast-pkts 1358427
        in-discards 265334
        in-errors 0
        out-octets 78887215
        out-unicast-pkts 248652
        out-discards 0
        out-errors 0
        ..
    ipv4
        address 172.21.a.b/22
        neighbor 172.21.b.c link-layer-address 00:00:5e:00:01:04 state reachable
        neighbor 172.21.a.d link-layer-address c0:3f:d5:ba:9e:b7 state stale
        neighbor 172.21.a.f link-layer-address 84:a9:3e:76:4e:b4 state reachable
        neighbor 172.21.a.g link-layer-address 50:eb:f6:d6:16:19 state stale
        neighbor 192.168.168.33 link-layer-address c0:3f:d5:ba:9e:b7 state stale
ethernet ge1
    mtu 1500
    promiscuous false
    enabled true
    type external
    oper-status UP
    counters
        in-octets 161320368
        in-unicast-pkts 1358427
        in-discards 265334
        in-errors 0
        out-octets 78887215
        out-unicast-pkts 248652
        out-discards 0
        out-errors 0
 :
```

The following command shows you configuration details for interface ge1.

```
 usgflex500h> show config vrf main interface ethernet ge1
ethernet ge1
    enabled true
    type external
    default-snat
        enabled true
        ..
    ping-check
        enabled false
        method icmp
        port 1
        period 30
        timeout 5
        fail-tolerance 5
        probe-condition any
        ..
    ipv4
        enabled true
        dhcp
            enabled true
            timeout 60
            retry 300
            select-timeout 0
            reboot 10
            initial-interval 10
            dhcp-lease-time 7200
            request subnet-mask
            request broadcast-address
            request time-offset
            request routers
            request domain-name
            request domain-search
            request domain-name-servers
            request host-name
            request nis-domain
            request nis-servers
            request ntp-servers
            request interface-mtu
            ..
        ..
    ipv6
        enabled true
        ..
    ports p1
    ethernet
        mac-address auto1
        ..
```

6.6 DHCP Server Commands

This section covers the DHCP Server commands.

This table lists the DHCP Server commands.

Table 17 DHCP Server Commands

COMMAND	DESCRIPTION
`vrf main dhcp server enabled {true | false}`	Enables or disables DHCP server.
`vrf main dhcp server default-lease-time <180..31536000>`	Sets the network address lease time assigned to DHCP clients (in seconds). The default is 172800 seconds (2 days).
`vrf main dhcp server max-lease-time <180..31536000>`	Sets the maximum network address lease time assigned to DHCP clients (in seconds). The default is 31536000 seconds (365 days, 1 non-leap year).
`vrf main dhcp server subnet <a.b.c.d/m> {dhcp-options | default-lease-time | max-lease-time | authoritative | interface | default-gateway | range | host}`	Sets the criteria for the specified subnet which is the network prefix of the subnet on which the DHCP server listens.

Table 17 DHCP Server Commands (continued)

COMMAND	DESCRIPTION
`vrf main dhcp server subnet <a.b.c.d/m> dhcp-options <option>`	Sets the extra configuration values the DHCP server sends to clients along with the IP address. These are the DHCP options supported at the time of writing. • `bootfile`: DHCP server option 67 - bootfile name • `capwap-ac`: Max count: 3. DHCP server option - 138 OPTION_CAPWAP_AC_V4 • `dhcp-server-identifier`: Identifies which DHCP server issued the lease by IPv4 address. This is used in DHCP messages to allow the client to distinguish between lease offers. • `domain-name`: Supplies the DNS suffix appended to unqualified hostnames. • `domain-name-server`: Sets up to 3 DNS server IP v4 addresses one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. • `interface-mtu`: Range: 0..65535. Tells the client what MTU size to use on the interface. • `netbios-name-server`: Specifies up to 2 WINS server(s) one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. • `netbios-node-type`: Controls how NetBIOS names are resolved. • `netbios-scope`: Defines a NetBIOS scope ID (logical group). NETBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002. • `ntp-server`: Sets up to 2 NTP servers for time synchronization one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. • `pxe-server`: DHCP server option - PXE Server Ip • `pxe-server-file-name`: DHCP server option - PXE Boot Loader File Name • `sip-server`: Sets up to 2 SIP server IP v4 addresses one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. DHCP server option - 120 SIP Server • `tftp-server`: Sets up to 3 TFTP server IP v4 addresses one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. DHCP server option - 150 TFTP Server Ip • `tftp-server-name`: DHCP server option 66 - TFTP Server Name • `time-offset`: Sets the time zone offset from UTC (in seconds). • `time-server`: Sets up to 2 time server IP v4 addresses one-by-one in order of server preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order. DHCP server option 4 - Time Server Ip • `user-defined`: Max count: 15. User defined DHCP option, usage: user-defined [option code] [type] [value] • `vivc`: Max count: 2. DHCP server option 124 - Vendor-Identifying Vendor Class (VIVC) • `vivs`: Max count: 2. DHCP server option 125 - Vendor Identifying Vendor Specific (VIVS)
`vrf main dhcp server subnet <a.b.c.d/m> default-lease-time <180..31536000>`	Sets the default network address lease time assigned to DHCP clients in this subnet, in seconds.
`vrf main dhcp server subnet <a.b.c.d/m> max-lease-time <180..31536000>`	Sets the maximum network address lease time assigned to DHCP clients in this subnet, in seconds.
`vrf main dhcp server subnet <a.b.c.d/m> authoritative {true | false}`	`true` requires the client to be in the same subnet as the DHCP server. If a client is not in the same subnet as the DHCP server, the DHCP server sends a DHCPNAK (Negative Acknowledgment) which invalidates the client's current IP address configuration. This causes the DHCP server to assign a new IP address to the client, which should be in the same subnet as the DHCP server.

Table 17 DHCP Server Commands (continued)

COMMAND	DESCRIPTION
`vrf main dhcp server subnet <a.b.c.d/m> interface <interface>`	Sets the interface of the Zyxel Device on which the DHCP server should listen. If you use an external DHCP server, by default the DHCP server must have an IP address in the same subnet as the IP address of the Interface on the Zyxel Device. Use this command if you want to change the IP address of the DHCP server to be in a different subnet to that of the Zyxel Device interface. For example, if you have a DHCP server with IP address 192.168.170.200 on the ge3 interface, then you can bind that DHCP server to the g4 interface with IP subnet 192.168.168.1/24 using this command.
`vrf main dhcp server subnet <a.b.c.d/m> default-gateway <ipv4-address>`	Sets up to 2 IPv4 addresses of a default gateway one-by-one in order of gateway preference. To re-order preference, delete these IPv4 addresses, then set them one-by-one again in the new order.
`vrf main dhcp server subnet <a.b.c.d/m> range <ipv4-address>`	Sets the starting IPv4 Address of a range.
`vrf main dhcp server subnet <a.b.c.d/m> host <a.b.c.d/m> mac-address <mac-address> host-name <name>`	Sets the IPv4 address, MAC address and hostname of a host in this subnet.
`vrf main dhcp server subnet <a.b.c.d/m> host <ipv4-address> mac-address <mac-address> host-name <name> description <string>`	Sets the IPv4 address, MAC address, hostname and description of a host in this subnet.

6.7 VLAN Interface Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 6.2 on page 73.

This table lists the VLAN interface commands.

Table 18 VLAN Interface Commands

COMMAND	DESCRIPTION
`vrf main interface vlan <interface-name> default-snat enabled {true| false}`	Enables default SNAT settings for the specified interface.
`vrf main interface vlan <interface-name> ipv4 dhcp enabled {true| false}`	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway.
`vrf main interface vlan <interface-name> ipv4 dhcp dhcp-lease-time <0...4294967295>`	Sets how long each computer can use the information (especially the IP address) before it has to request the information again. The default value is 7200.
`vrf main interface vlan <interface-name> ipv4 address <ipv4-address>`	Enters the IP address for this interface.

Table 18 VLAN Interface Commands (continued)

COMMAND	DESCRIPTION
`vrf main interface vlan <interface-name> ipv4 gateway <ipv4-address>`	Enters the IP address of the router through which this connection will send traffic.
`vrf main interface vlan <interface-name> enabled {true| false}`	Enables or disables the specified interface.
`vrf main interface vlan <interface-name> type {internal| external}`	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
`vrf main interface vlan <interface-name> description <description>`	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"
`vrf main interface vlan <interface-name> mtu <1280...1500>`	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
`vrf main interface vlan <interface-name> vlan-id <1...4094>`	Sets the VLAN ID used to identify the VLAN.
`vrf main interface vlan <interface-name> vlan-priority-code <0...7>`	Sets the 802.1p priority for VLAN outgoing traffic from 0 to 7 where 0 is the lowest priority (background traffic) and 7 the highest (network control traffic).
`vrf main interface vlan <interface-name> qos [ingress | egress] rate-limit policer <profile-name>`	Applies the ingress and egress rate limit of the QoS policer profile to the interface. Refer to Overall Interface Commands for QoS policer profile rate limit configuration. If you also set a limit using Bandwidth Management Commands, the Zyxel Device will apply the lower value as the limit.

6.7.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN vlan100 with the following parameters: VLAN ID 100, interface port p1, IP 1.2.3.4, MTU 598, gateway 2.2.2.2.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main interface vlan vlan100 vlan-id 100
usgflex200hp running config# vrf main interface vlan vlan100 ipv4 address 1.2.3.4
usgflex200hp running config# vrf main interface vlan vlan100 ipv4 gateway 2.2.2.2
usgflex200hp running config# vrf main interface vlan vlan100 mtu 598
usgflex200hp running config# vrf main interface vlan vlan100 link-port p1
usgflex200hp running config# commit
Configuration committed.
```

6.8 Bridge Interface Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 6.2 on page 73.

A bridge interface creates a software bridge between the members of the bridge interface, and becomes the Zyxel Device's interface for the resulting network. To use the whole Zyxel Device as a transparent bridge, add all of the Zyxel Device's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the Zyxel Device removes the members' entries from the routing table and adds the bridge interface's entries to the routing table.

Table 19 Bridge Interface Commands

COMMAND	DESCRIPTION
`vrf main interface bridge <interface-name> default-snat enabled {true| false}`	Enables default SNAT settings for the specified interface.
`vrf main interface bridge <interface-name> enabled {true| false}`	Enables or disables the interface.
`vrf main interface bridge <interface-name> type {internal| external}`	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
`vrf main interface bridge <interface-name> mtu <1280...1500>`	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
`vrf main interface bridge <interface-name> description <description>`	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"
`show config / vrf main interface bridge <interface-name>`	Displays configuration settings for the named bridge.

6.8.1 Bridge Command Examples

The following command shows you configuration details for the named interface.

```
usgflex500h> show config / vrf main interface bridge CathyBridge
bridge CathyBridge
    ipv4
        enabled true
        dhcp
            enabled false
            timeout 60
            retry 300
            select-timeout 0
            reboot 10
            initial-interval 10
            dhcp-lease-time 7200
            request subnet-mask
bridge CathyBridge
    ipv4
        enabled true
        dhcp
            enabled false
            timeout 60
            retry 300
            select-timeout 0
            reboot 10
            initial-interval 10
            dhcp-lease-time 7200
            request subnet-mask
            request broadcast-address
            request time-offset
            request routers
            request domain-name
            request domain-search
            request domain-name-servers
            request host-name
            request nis-domain
            request nis-servers
            request ntp-servers
            request interface-mtu
            ..
        ..
    mtu 1500
    enabled true
    type general
    default-snat
        enabled true
        ..
```

These commands enter a specific bridge interface and displays the forwarding database (FDB) table.

```
usgflex500h running config# vrf main interface bridge CathyBridge
usgflex500h running bridge CathyBridge# show bridge fdb
interface link-layer-address link-interface state
========= ================== ============== =====
usgflex500h running bridge CathyBridge#
```

6.9 VTI Interface Commands

IPsec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

VTI allows static routes to send traffic over the VPN. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPsec tunnel as soon as the tunnel is active.

Create a trunk using VPN tunnel interfaces for load balancing.

6.9.1 Restrictions for IPsec Virtual Tunnel Interface

- IPSec tunnel mode only. A shared keyword must not be configured when using tunnel mode.
- With a VTI VPN you do not add local or remote LANs to your VPN configuration.
- For a VTI VPN you should only have one local and one remote WAN.
- A dynamic peer is not supported.
- The IPsec VTI is limited to IP unicast and multicast traffic only.

This table lists the VTI-specific interface commands. See Table 16 on page 76 for common `interface` commands.

Table 20 VTI Interfaces Commands

COMMAND	DESCRIPTION
`vrf main interface legacy-vti <interface-name>`	Sets the name of the interface.
`enabled {true| false}`	Enables the specified interface.
`ipv4 address <ipv4-address>`	Sets the IP address for the specified interface.
`ipv4 gateway <ipv4-address>`	Sets the gateway IP address to which the Zyxel Device routes to.
`ping-check enabled {true| false}`	Enables the connection check. The interface can regularly check the connection to the gateway you specified to make sure it is still available. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
`ping-check method {icmp| tcp}`	Sets the connection check method to `icmp` to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Sets the connection check method to `tcp` to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it si still available.
`ping-check period <5...600>`	Sets the number of seconds between connection check attempts. The default value is 30.
`ping-check timeout <1...10>`	Sets the number of seconds to wait for a response before the attempt is a failure. The default value is 5.
`ping-check fail-tolerance <1...10>`	Sets the number of consecutive failures before the Zyxel Device stops routing through the gateway. The default value is 5.

Table 20 VTI Interfaces Commands (continued)

COMMAND	DESCRIPTION
ping-check probe-condition {any| all}	Sets the probe condition to `any` if you want the check to pass if at least one of the domain names or IP addresses responds. Sets the probe condition to `all` if you wan the check to pass only if both domain names or IP addresses respond.
ping-check target <*ipv4-address*| *domain-name*>	Specifies one or two domain names or IP addresses to receive test packets for the connectivity check.
ping-check source <*ipv4-address*>	Specifies the IP address to use for sending test packets for the connectivity check.

6.10 Network Debug Commands

If you're having problems with the Zyxel Device, customer support may request the output from certain debug commands such as these.

Table 21 Network Debug Commands

COMMAND	DESCRIPTION
cmd debug network brctl show	Displays members in all bridge interfaces.
cmd debug network brctl showmacs <bridge interface>	Displays the MAC addresses of members in a specific bridge interface.
cmd debug network brctl showstp <bridge interface>	Displays spanning tree details of a bridge interface.
cmd debug network zone info	Displays zone IDs, interfaces and zone names.
cmd debug network ipset list	Displays IP set details. An IP set is a framework for storing IP addresses, port numbers, IP and MAC address pairs, or IP address and port number pairs.
cmd debug network socket	Displays network socket details. A socket is one endpoint of a two-way communication link between two programs running on the network. An endpoint is a combination of an IP address and a port number.
cmd debug network interface	Displays network interface details such as number of bytes, packets, errors, packets dropped, overrun, multicast packets received or transmitted on an interface.
cmd debug network statistics	Displays network statistics details on IP, ICMP, ICMP messages, TCP, UDP, UdpLite, TcpExt, IpExt, and SCTP (Stream Control Transmission Protocol) similar to the 'netstat –s' command in Linux.

6.10.1 Network Debug Command Examples

The following are some example network debug commands.

Figure 69 Debug Zones

```
usgflex500h running config# cmd debug network zone info
zone id, interface: ready?
==============================
2 ge1:1
2 ge2:1
3 ge3:1
3 ge4:1
3 cat:1
4 DMZ:1

zone id, zone name
==============================
2 WAN
3 LAN
4 DMZ
5 IPSec_VPN
6 SSL_VPN
usgflex500h running config#
```

Figure 70 Debug IP Sets

```
usgflex500h running config#cmd debug network ipset list
Name: zyset-address4-0
Type: zyip
Revision: 0
Header: family inet count 1
Size in memory: 40
References: 4294967295
Members:
192.88.99.1
 count 1

Name: zyset-service-0
Type: zyport
Revision: 0
Header: family inet count 1
Size in memory: 12
References: 4294967295
Members:
AH
.
.
```

Figure 71 Debug Network Sockets

```
usgflex500h running config# cmd debug network socket
Netid State  Recv-Q Send-Q      Local Address:Port    Peer Address:Port Process
raw   UNCONN 0      0                0.0.0.0:255          0.0.0.0:*
raw   UNCONN 0      0                0.0.0.0:255          0.0.0.0:*
raw   UNCONN 229376 0                     *:58                 *:*
raw   UNCONN 0      0                     *:255                *:*
raw   UNCONN 0      0                     *:255                *:*
udp   UNCONN 0      0                0.0.0.0:3799         0.0.0.0:*
udp   UNCONN 0      0             172.21.56.19:53         0.0.0.0:*
udp   UNCONN 0      0            192.168.169.1:53         0.0.0.0:*
udp   UNCONN 0      0         169.254.148.254:53          0.0.0.0:*
udp   UNCONN 0      0            192.168.168.1:53         0.0.0.0:*
udp   UNCONN 0      0                127.0.0.1:53         0.0.0.0:*
udp   UNCONN 0      0                  0.0.0.0:68         0.0.0.0:*
udp   UNCONN 0      0                  0.0.0.0:161        0.0.0.0:*
udp   UNCONN 0      0                  0.0.0.0:4500       0.0.0.0:*
.......
```

Figure 72 Debug Network Interfaces

```
usgflex500h running config# cmd debug network interface
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX: bytes  packets  errors  dropped overrun mcast
    237666657  447661   0       0       0       0
    RX errors: length   crc     frame   fifo    missed
               0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    237666657  447661   0       0       0       0
    TX errors: aborted  fifo   window heartbeat transns
               0        0       0       0       0
2: ifb0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN mode DEFAULT group
default qlen 32
    link/ether ea:fa:e7:1c:57:a7 brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    0          0        0       0       0       0
    RX errors: length   crc     frame   fifo    missed
               0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    0          0        0       0       0       0
    TX errors: aborted  fifo   window heartbeat transns
               0        0       0       0       0
```

Figure 73 Debug Network Statistics

```
usgflex500h running config# cmd debug network statistics
Ip:
    Forwarding: 1
    4741765 total packets received
    53 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1298780 incoming packets delivered
    954581 requests sent out
    323 dropped because of missing route
    28 reassemblies required
    14 packets reassembled ok
Icmp:
    280 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 11
        echo requests: 16
        echo replies: 253
    613 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 57
        echo requests: 540
        echo replies: 16
IcmpMsg:
        InType0: 253
        InType3: 11
        InType8: 16
....
```

CHAPTER 7
Trunks

7.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface’s connection goes down, the Zyxel Device sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The Zyxel Device can balance the load between multiple connections. If one interface's connection goes down, the Zyxel Device can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface’s connection goes down, the Zyxel Device can still send its traffic through another interface.

7.2 Trunk Scenario Examples

Suppose one of the Zyxel Device's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface’s connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

7.3 Load Balancing Algorithms

The following sections describe the load balancing algorithms the Zyxel Device can use to decide which interface the traffic (from the LAN) should use for a session. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic. The available bandwidth you configure on the Zyxel Device refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

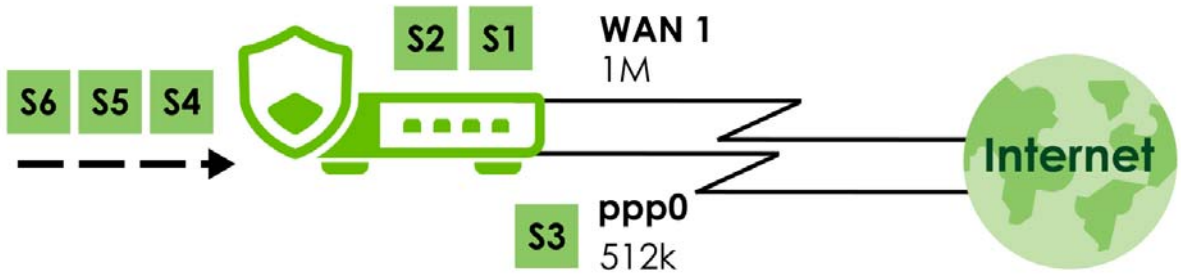
7.3.1 Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the Zyxel Device to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the Zyxel Device to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The Zyxel Device assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 74 Weighted Round Robin Algorithm Example



7.3.2 Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The Zyxel Device calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the Zyxel Device will send the subsequent new session traffic through WAN 2.

Table 22 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

7.3.3 Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

7.4 Trunk Commands Input Values

The following table explains the values you can input with the trunk commands.

Table 23 Trunk Command Input Values

LABEL	DESCRIPTION
group-name	A descriptive name for the trunk. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
interface-name	The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use are as follows. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports.
num	The interface's position in the trunk's list of members `<1..8>`.

7.5 Trunk Commands

The following table lists the trunk commands. Use trunks for WAN traffic load balancing to divide traffic loads between multiple interfaces to increase overall network throughput and reliability.

- The least load first (`llf`) algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about which interface a new session is to be distributed.
- The Weighted Round Robin (`wrr`) algorithm sets the Zyxel Device to send traffic through each WAN interface in turn, and according to the assigned weight of the WAN interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

- The spillover (`spill-over`) load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached. It then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

If one WAN interface's connection goes down, the Zyxel Device sends traffic through another member of the trunk.

You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

There is a system default trunk and you can also define your own trunk adding specific interfaces.

You must use the `edit running` command to enter the configuration mode before you can use these commands. See Table 23 on page 93 for details about the values you can input with these commands.

Table 24 Trunk Commands

COMMAND	DESCRIPTION
`vrf main interface-group <group-name> algorithm <wrr| spill-over|llf>.`	Sets the trunk's load balancing algorithm.
`vrf main interface-group <group-name> interface <interface-name> passive {true| false} weight <1...10>`	Sets the interface's weight or sets it to be passive to have the Zyxel Device only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
`vrf main interface-group <group-name> loadbalancing-index <outbound | inbound| total>`	Sets the load balancing index interface for spill-over or llf algorithms. The load balancing index sets the interface for which a new session is to be distributed.
`vrf main interface-group <group-name> limit <1.. 2097152 >`	Sets the upper throughput threshold in bytes for spill-over or llf algorithms. Throughput is the moving average of traffic passing through the Zyxel Device in the last 10 seconds updated every 1 second.
`vrf main system default-interface-group name <group-name>`	Sets the system default trunk.
`vrf main system default-interface-group algorithm [llf | spill-over | wrr]`	Sets the system default trunk's load balancing algorithm.
`vrf main system fallback-session-disconnect enabled [true | false]`	Sets the Zyxel Device to end all connections on the passive interface if the active interface comes back up again, and the trunk goes back to using the active interface.
`vrf main system link-sticking enabled [true | false]`	Has the Zyxel Device ignore load balancing and continue to use the same WAN interface for certain source-destination links when you have multiple active WAN interfaces. This is useful when a server requires authentication for a link coming from a specific IP address. If the IP address changes due to load balancing changing the WAN interface, then the server may reject the request. Link Sticking has a default 300 second timeout (5 minutes), so the WAN interface record for the source-destination pair is refreshed 5 minutes after the last time a connection of this source-destination pair was established.
`show config vrf main interface-group <group-name>`	Displays the interface group settings you configured.
`show state vrf main interface-group <group-name>`	Displays the default interface group settings and the interface group settings you configured.

7.6 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge3 and ge4. The Zyxel Device sends twice as much traffic as it does through ge4.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main interface-group Example1 interface ethernet
ge3 weight 2
usgflex200hp running config# vrf main interface-group Example1 interface ethernet
ge4 weight 1
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 8
Route

8.1 Policy Route

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

8.1.1 Source Network Address Translation (SNAT)

SNAT allows the Zyxel Device to rewrite the source IP address of packets in a policy route. This means you can make packets coming from an IP address appear to originate from a different IP address.

8.1.1.1 SNAT with the ZyWALL Interface

You can apply SNAT to packets sent from the ZyWALL interface. This can be used to separate internally generated Zyxel Device traffic from other traffic.

For example: The Zyxel Device has two IP addresses, 6.6.6.6 and 6.6.6.7, on a WAN interface. There is a firewall in front of the Zyxel Device with the following security rules:

- IP address 6.6.6.6 is client traffic. There are no restrictions.
- IP address 6.6.6.7 is Zyxel Device traffic, Packets can only go to *.myzyxel.com and *.cloud.zyxel.com.

If clients are connected to ge3 on the Zyxel Device, then you need to create two policy routes with SNAT enabled:

- Client_Route - Incoming interface: ge3, SNAT: 6.6.6.6.
- Device_Route - Incoming interface: ZyWALL, SNAT: 6.6.6.7.

8.2 Policy Route and Static Route Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 25 Policy Route and Static Route Command Input Values

LABEL	DESCRIPTION
address-object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE interfaces your Zyxel Device model supports.
schedule-object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

8.3 Policy Route Commands

The following table describes the commands available for policy route. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 26 Policy Route Commands

COMMAND	DESCRIPTION
`vrf main routing policy-route rule <profile-name> enabled {true | false}`	Activates the profile.
`vrf main routing policy-route rule <profile-name> description <description>`	Enter a description for this profile, You can use 1 to 60 single-byte characters.
`vrf main routing policy-route rule <profile-name> match user {admin-object <admin-object> | user-object <user-object> | group <group> | any}`	Sets a user name or user group from which the packets are sent.
`vrf main routing policy-route rule <profile-name> match schedule {object <schedule-profile> | group <schedule-object> | none}`	Sets a schedule to control when the policy route is active. `none` means the route is active at all times if enabled.
`vrf main routing policy-route rule <profile-name> match from <interface>`	Sets where the packets are coming from.

Table 26 Policy Route Commands (continued)

COMMAND	DESCRIPTION
`vrf main routing policy-route rule <profile-name> match source {object <object> | group <group> | any}`	Sets a source IP address object, including geographic address and FQDN (group) objects, from which the packets are sent.
`vrf main routing policy-route rule <profile-name> match destination {object <object> | group <group> | any}`	Sets a destination IP address object, including geographic address and FQDN (group) objects, to which the traffic is being sent. Note: If the next hop is a dynamic VPN tunnel, the Zyxel Device uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.
`vrf main routing policy-route rule <profile-name> match service-type service service {<object> | any}`	Sets a service or service group to identify the type of traffic to which this policy route applies.
`vrf main routing policy-route rule <profile-name> match service-type application-sid application-sid <sid>`	Specifies an application to identify the traffic to which this policy route applies. You can use the command *`show routing policy-route applications`* to find the corresponding signature ID (sid) of the applications.
`vrf main routing policy-route rule <profile-name> match srcport {object <object> | group <group> | any}`	Sets a service or service group to identify the source port of packets to which the policy route applies.
`vrf main routing policy-route rule <profile-name> match dscp <dscp-code>`	Sets a DSCP code point value of incoming packets to which this policy route applies. The lower the number the higher the priority with exception of 0 which is usually given only best-effort treatment. `any` means all DSCP value or no DSCP marker. `default` means traffic with a DSCP value of 0. This is usually best effort traffic. The **af** choices stand for Assured Forwarding. The number following the **af** identifies one of four classes and one of three drop preferences. See Section 8.3.1 on page 99 for more information.
`vrf main routing policy-route rule <profile-name> action next-hop {gateway <address-object> | gateway-ip <ipv4-address> | interface <interface> | trunk <trunk> | auto | ipsec-vpn <name>}`	Sets the next-hop to which the matched packets are routed. `auto` means to have the Zyxel Device use the routing table to find a next-hop and forward the matched packets automatically. `ipsec-vpn` routes the matched packets through the specified policy-based VPN Tunnel to a remote gateway.

Table 26 Policy Route Commands (continued)

COMMAND	DESCRIPTION
`vrf main routing policy-route rule <profile-name> action snat {pool <address-group> | outgoing-interface <address-object> | none}`	Use `none` to not use SNAT for this profile. Use `outgoing-interface` to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnet. Use `pool` to set a pre-defined address or address group to use as the source IP addresses of the packets that match this route. Note: If the address object is a group or range of IP addresses, then the Zyxel Device picks one IP address randomly from the group or range, and then assigns the address permanently to the policy.
`vrf main routing policy-route rule <profile-name> action dscp-marking <dscp-code>`	Sets how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Set this to `default` to have the Zyxel Device set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Section 8.3.1 on page 99 for more information.
`vrf main routing policy-route override-direct-route {true | false}`	Forwards packets that match a policy route according to the policy route instead of sending the packets directly to a connected network (`true`). The default `false` sends packets directly to a connected network.
`vrf main routing policy-route rule <profile-name> ping-check source <ipv4-address>`	Sets a source IPv4 address of a gateway that ping test packets will be sent from. The source IP address can be any IP address that can be routed back to the Zyxel Device. If you don't set a specific IP address, the Zyxel Device may send test packets from the primary or secondary IP address of the Next Hop interface.
`cmd rename rule policy-route from <original-profile-name> to <new-profile-name>`	Renames a policy route rule. Make sure the original policy route rule exists.
`show routing policy-route application`	Displays a list of available applications for policy route configuration and their signature IDs.
`show state vrf main routing`	Displays the Zyxel Device routing status, such as the number of connected routes and each routing function settings.
`show config vrf main routing`	Displays if the override direct route feature is enabled.
`show state vrf main routing policy-route`	Displays details of a Zyxel Device policy routing, such as the match rule, action and number of matching packets.

8.3.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If

congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 27 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

8.3.2 Policy Route Command Example

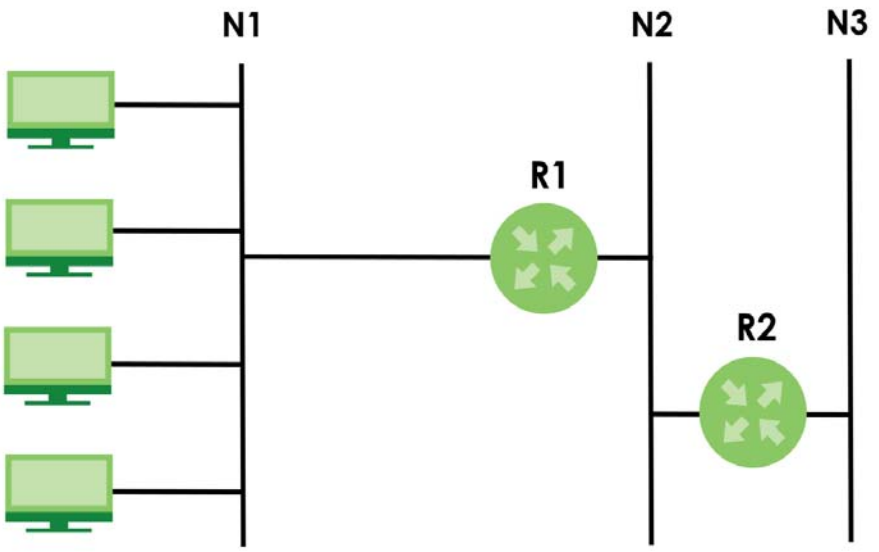
The following commands create two address objects (TW_SUBNET and GW_1) and create a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) to the next-hop router GW_1.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address TW_SUBNET type host
192.168.2.0
usgflex200hp running config# object address-object address TW_SUBNET type host
255.255.255.0
usgflex200hp running config# object address-object address GW_1 type host
192.168.2.250
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# vrf main routing policy-route rule Rule1 description
example
usgflex200hp running config# vrf main routing policy-route rule Rule1 match
destination any
usgflex200hp running config# vrf main routing policy-route rule Rule1 match source
object TW_SUBNET
usgflex200hp running config# vrf main routing policy-route rule Rule1 action snat
outgoing-interface
usgflex200hp running config# vrf main routing policy-route rule Rule1 action next-
hop gateway GW_1
usgflex200hp running config# vrf main routing policy-route rule Rule1 match user
admin-object admin
usgflex200hp running config# vrf main routing policy-route rule Rule1 match
schedule none
usgflex200hp running config# vrf main routing policy-route rule Rule1 match from
any
usgflex200hp running config# vrf main routing policy-route rule Rule1 match service
any
usgflex200hp running config# vrf main routing policy-route rule Rule1 match srcport
any
usgflex200hp running config# vrf main routing policy-route rule Rule1 match dscp
default
usgflex200hp running config# commit
Configuration committed.
```

8.4 Static Route

The Zyxel Device has no knowledge of the networks beyond the network that is directly connected to the Zyxel Device. For instance, the Zyxel Device knows about network **N2** in the following figure through gateway **R1**. Use a static route to define a route when there is a single route or a preferred route for traffic to reach a destination.

Figure 75 Example of Static Routing Topology



8.5 Static Route Commands

The following table describes the commands available for static route. You must use the `edit running` command to enter the configuration mode before you can use these commands. See Section Table 25 on page 97 for information on input values.

Table 28 Static Route Commands

COMMAND	DESCRIPTION
`vrf main routing static-route rule <profile-name> description <description>`	Enter a description for this profile.
`vrf main routing static-route rule <profile-name> metric <1...127>`	Sets a number that approximates the cost for this link. Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for direct connected networks.

Table 28 Static Route Commands

COMMAND	DESCRIPTION
`vrf main routing static-route rule <profile-name> destination {cidr cidr| object address-object}`	Specifies the IP network address of the final destination.
`vrf main routing static-route rule <profile-name> via {gateway-object address-object| gateway ipv4-address| interface interface}`	`gateway-object/ gateway`: Enters the IP address or selects the address object of the next-hop gateway. `interface`: Sets a pre-defined interface through which the traffic is sent.

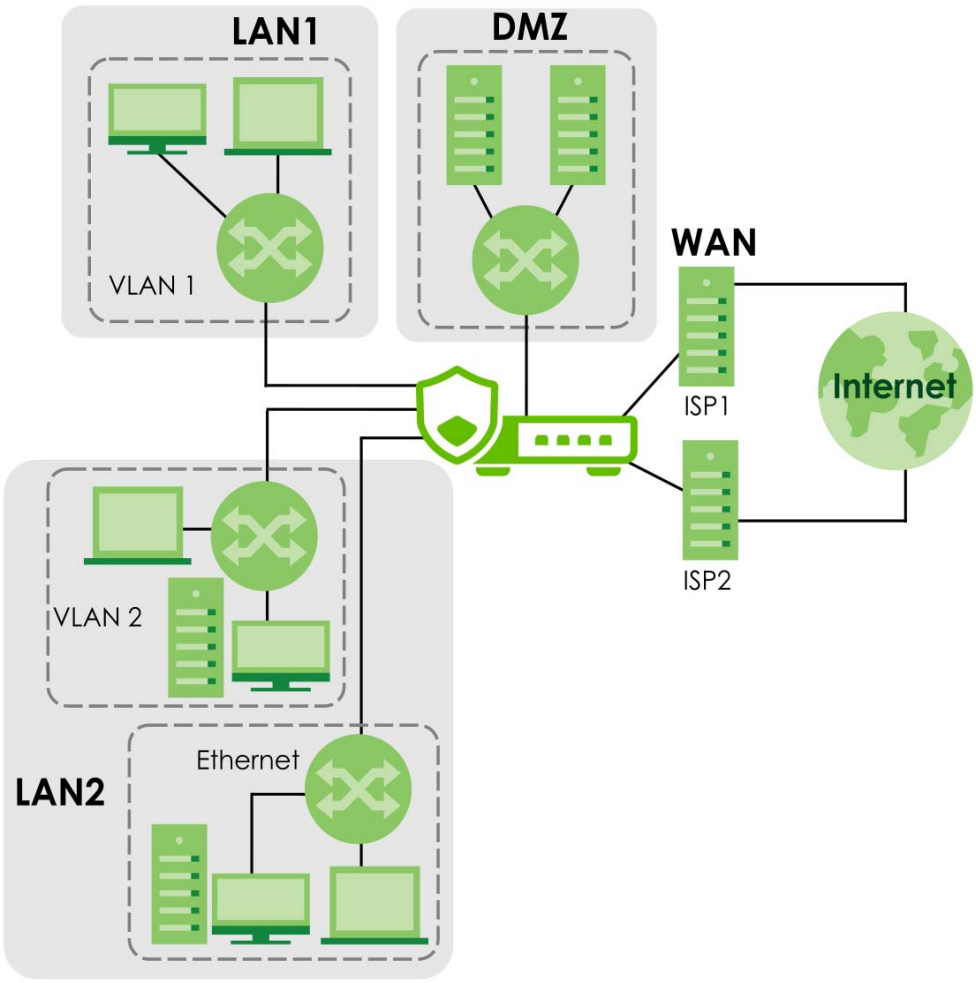
CHAPTER 9
Zones

9.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. Set up zones to configure network security and network policies in the Zyxel Device. The Zyxel Device uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE 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 76 Example: Zones



9.2 Zone Command Input Values

The following table describes the values required for many zone commands. Other values are discussed with the corresponding commands.

Table 29 Zone Command Input Values

LABEL	DESCRIPTION
profile-name	The name of a zone, or the name of a VPN tunnel. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

9.3 Zone Commands

This table lists the zone commands.

Table 30 Zone Commands

COMMAND	DESCRIPTION
`object zone-object zone <profile-name> interface-list <interface>`	Adds the specified interface to the specified zone.
`object zone-object zone <profile-name> description <description>`	Enters a description associated with the specified zone.
`show object zone none-binding`	Displays the interfaces, tunnels and IPSec VPNs that are not associated with a zone yet.
`show object zone system-default`	Displays the pre-configured default zones that you cannot delete from the Zyxel Device.
`show object zone user-define`	Displays all customized zones.
`show object zone default-binding`	Displays the pre-configured interface and zone mappings that come with the Zyxel Device.
`show object zone binding-iface`	Displays each interface and zone mappings.

9.3.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to the WAN zone.

```
usgflex200hp> edit running
usgflex200hp running config# object zone-object zone
WAN          LAN          DMZ          IPSec_VPN
usgflex200hp running config# object zone-object zone WAN
interface-list    description
usgflex200hp running config# object zone-object zone WAN interface-list ethernet
ge1 ethernet ge2
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 10
DDNS

10.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, and so on) or to access your FTP server or Web site, regardless of the current IP address.

Note: The Zyxel Device WAN interface must have a public WAN IP address to use Dynamic DNS.

Set up a dynamic DNS account with a supported DNS service provider to be able to use Dynamic DNS services with the Zyxel Device. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the Zyxel Device supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 31 Network > DDNS

DDNS SERVICE PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com)
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Selfhost	Selfhost	selfhoost.de

Note: Record your DDNS account's user name, password, and domain name to use to configure the Zyxel Device.

After, you configure the Zyxel Device, it automatically sends updated IP addresses to the DDNS service provider, which updates domain name mapping accordingly.

10.2 DDNS Command Input Values

The following table describes the values required for many DDNS commands. Other values are discussed with the corresponding commands.

Table 32 DDNS Command Input Value

LABEL	DESCRIPTION
profile-name	The name of the DDNS profile. You may use 1-31 single-byte characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

10.3 DDNS Commands

The following table lists the DDNS commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 33 DDNS Commands

COMMAND	DESCRIPTION
`vrf main ddns rule <profile-name>`	Creates or edits the specified DDNS profile and enters the sub-command mode.
`enabled {true| false}`	Enables the specified DDNS profile.
`ddns-type {user-custom| dyndns| dyndns-static| dyndns-custom| no-ip| selfhost| dynu-basic| dynu-premium}`	Sets the service type in the specified DDNS profile.
`account username username password password`	Sets the username and password in the specified DDNS profile. *username*: You can use up to 31 single-byte characters and :_.-@ *password*: You can use up to 64 single-byte characters and the underscore (_).
`setting primary-binding interface <interface-name| any>`	Sets the primary interface to use for updating the IP address mapped to the domain name. `any` allows the domain name to be used with any interface.
`setting primary-binding ip-address <interface | custom ip ipv4-address| object object-name| auto| public ip>`	Configures the primary interface to use for updating the IP address mapped to the domain name. `interface`: The Zyxel Device sends the IP address of the specified interface to the DDNS server. `custom ip`: Select this if you're using a static IPv4 address for the domain name. The Zyxel Device sends your configured static IP address or the specified address object to the DDNS server. `auto`: Use this if the DDNS server supports it, there are one or more NAT routers between the Zyxel Device and the DDNS server, and the Zyxel Device interface has a dynamic IP address. The DDNS server checks the source IP address of packets from the Zyxel Device and uses that for the domain name. The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. `public ip`: The DDNS server uses this public IP address for the domain name. If you choose this, you must configure the `check-public-ip` commands, so that the Zyxel Device may know the public IP address (of the NAT router in front of the Zyxel Device, for example) and inform the DDNS server.
`settings check-public-ip URL`	If the DDNS server uses a public IP address for the domain name, this command has the Zyxel Device check the public IP address given to the URL it is using as its domain name.

Table 33 DDNS Commands (continued)

COMMAND	DESCRIPTION
`settings check-public-ip period`	If the The DDNS server uses a public IP address for the domain name, this command sets how often (5 to 1,440 minutes) the Zyxel Device should check the public IP address given to its URL.
`setting backup-binding interface <`*`interface-name`*`| any| none>`	Sets an alternate interface to map the domain name to when the interface specified in the `primary-binding` command is not available. `none` means to not use a backup address.
`setting backup-binding ip-address <interface | custom ip `*`ipv4-address`*`| object `*`object-name`*`| auto| public ip>`	Configures an alternate interface to map the domain name to when the interface specified in the `primary-binding` command is not available. `interface`: The Zyxel Device sends the IP address of the specified interface to the DDNS server. `custom ip`: Select this if you're using a static IPv4 address for the domain name. The Zyxel Device sends your configured static IP address or the specified address object to the DDNS server. `auto`: Use this if the DDNS server supports it, there are one or more NAT routers between the Zyxel Device and the DDNS server, and the Zyxel Device interface has a dynamic IP address. The DDNS server checks the source IP address of packets from the Zyxel Device and uses that for the domain name. The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. `public ip`: The DDNS server uses this public IP address for the domain name. If you choose this, you must configure the `check-public-ip` commands, so that the Zyxel Device may know the public IP address (of the NAT router in front of the Zyxel Device, for example), and inform the DDNS server.
`setting domain-name <`*`domain-name`*`>`	Enter the domain name you registered. You can use up to 255 characters.
`setting wildcard {true| false}`	Enables to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. Please note that you can only use this command with DDNS type set to DnyDNS.
`setting mail-exchanger <`*`email-address`*`>`	Enter the host record of your mail server. DynDNS can route email for your domain name to a mail server. For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. Please note that you can only use this command with DDNS type set to DnyDNS.
`setting backup-mail-exchanger {true| false}`	Lets DynDNS store your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. Please note that you can only use this command with DDNS type set to DnyDNS.

Table 33 DDNS Commands (continued)

COMMAND	DESCRIPTION
`https {true| false}`	Encrypts traffic using SSL, including traffic with username and password, to the DDNS server.
`show config vrf main ddns rule`	Displays DDNS rules settings.
`cmd ddns update rule <profile-name>`	Has the Zyxel Device update the specified rule.
`show ddns status`	Displays DDNS rules status, last update time and the IP address of the domain name.

CHAPTER 11
Virtual Servers

11.1 Virtual Server Overview

NAT is also known as virtual server, port forwarding or port translation.

Virtual servers are computers on a private network behind the Zyxel Device that you want to make available outside the private network. If the Zyxel Device has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

11.1.1 1:1 NAT and Many 1:1 NAT

1:1 NAT - If the private network server will initiate sessions to the outside clients, use 1:1 NAT to have the Zyxel Device translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.

Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, use many 1:1 NAT to have the Zyxel Device translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.

One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases the configuration effort since you only create one rule.

11.2 Virtual Server Command Input Values

The following table describes the values required for many virtual server commands. Other values are discussed with the corresponding commands.

Table 34 Virtual Server Command Input Values

LABEL	DESCRIPTION
service-object	The name of a service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
profile-name	The name of the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

11.3 Virtual Server Commands

Please note that if you create a NAT rule using the IP address of the Web Configurator and set the external port to 80 (HTTP) or 443 (HTTPS), the rule will conflict with the Zyxel Device's default HTTP server port. You will not be able to access the Web Configurator through this interface.

Table 35 Virtual Server Commands

COMMAND	DESCRIPTION
`vrf main virtual-server rule <profile-name> nat-1-1-map {true| false}`	Enables 1:1 NAT type.
`vrf main virtual-server rule <profile-name> nat-loopback {true| false}`	Allows local users to use a domain name to access the virtual server.
`vrf main virtual-server rule <profile-name> enabled {true| false}`	Enables the virtual server profile.
`vrf main virtual-server rule <profile-name> interface <interface-name>`	Sets the interface on which packets for the virtual server profile must be received.
`vrf main virtual-server rule <profile-name> source-ip {object service-object| address ipv4-address| cidr cidr| any| range from ipv4-address to ipv4-address}`	Specifies the source IP address of the packets received by the virtual server profile's specified incoming interface. `any` means to use all of the incoming interface's IP addresses including dynamic address.
`vrf main virtual-server rule <profile-name> original-ip {object service-object| address ipv4-address| cidr cidr| any| range from ipv4-address to ipv4-address}`	Specifies the destination IP address of the packets received by the virtual server profile's specified incoming interface. The specified IP address will be translated to the internal IP address. `any` means to user all of the incoming interface's IP addresses including dynamic address or those of any virtual interfaces built upon the selected incoming interface.
`vrf main virtual-server rule <profile-name> map-to {object service-object| address ipv4-address| cidr cidr| any| range from ipv4-address to ipv4-address}`	Maps the specified destination IP address to the specified destination address object or IP address.
`vrf main virtual-server rule <profile-name> map-type {any| port| ports| service| service-group}`	Sets how many original destination ports the virtual server profile supports for the original IP you set. `any`: The virtual server profile supports all the destination ports. `port`: The virtual server profile supports one destination port. `ports`: The virtual server profile supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. `service`: The virtual server profile supports a service such as FTP. `service-group`: The virtual server profile supports a group of services such as all service objects related to DNS.

Table 35 Virtual Server Commands (continued)

COMMAND	DESCRIPTION
`vrf main virtual-server rule <profile-name> garp-interval <5-86400>`	Sets how frequently the Zyxel Device sends Gratuitous ARP (GARP) packets using the virtual server's external IP address. This refreshes ARP tables in the network ensuring correct IP-to-MAC address mapping, preventing network segment traffic loss.
`show config vrf main virtual-server rule`	Displays the virtual server profiles settings.

11.3.1 Virtual Server Command Examples

The following command creates virtual server profile Profile1 on the ge1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also enables NAP loopback.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main virtual-server rule Profile1 interface ge1
enabled true
usgflex200hp running config# vrf main virtual-server rule Profile1 original-ip
address 10.0.0.8
usgflex200hp running config# vrf main virtual-server rule Profile1 source-ip
address 192.168.1.56
usgflex200hp running config# vrf main virtual-server rule Profile1 map-type port
protocol tcp original-port 1720 mapped-port 1720
usgflex200hp running config# vrf main virtual-server rule Profile1 nat-loopback
true
usgflex200hp running config# vrf main virtual-server rule Profile1 map-to address
192.168.1.56
usgflex200hp running config# commit
Configuration committed.
```

The following command shows information about all the virtual servers in the Zyxel Device.

```
usgflex200hp running config# show config vrf main virtual-server rule
virtual-server Profile
    enabled true
    interface LAN1_SUBNET
    source-ip address 2.2.2.2
    original-ip address 3.3.3.3
    map-to address 1.1.1.1
    nat-1-1-map
        false
        ..
    nat-loopback
        false
        ..
    map-type any
    ..
virtual-server Profile1
    enabled true
    interface ge1
    source-ip address 192.168.1.56
    original-ip address 10.0.0.8
    map-to address 192.168.1.56
    nat-1-1-map
        false
        ..
    nat-loopback
        true
        ..
    map-type port protocol tcp original-port 1720 mapped-port 1720
    ..
```

CHAPTER 12
ALG

12.1 ALG Introduction

The Zyxel Device can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as FTP) to operate properly through the Zyxel Device's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The Zyxel Device examines and uses IP address and port number information embedded in the FTP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has FTP passed through enabled, the Zyxel Device translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The Zyxel Device only needs to use the ALG feature for traffic that goes through the Zyxel Device's NAT. The firewall allows related sessions for FTP applications that register with a server. The firewall allows or blocks peer to peer FTP traffic based on the firewall rules.

12.2 ALG FTP Commands

The following table lists the ALG FTP commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 36 ALG FTP Commands

COMMAND	DESCRIPTION
`vrf main alg ftp enabled {true| false}`	Enables the ALG for FTP.
`vrf main alg ftp signal-port <1025...65535>`	Sets a listening port number if you are using FTP on a TCP port other than 21.
`vrf main alg ftp signal-extra-port <1025...65535>`	Sets a listening port number if you are using FTP on an additional TCP port.
`show config vrf main alg ftp`	Displays the ALG for FTP settings.

12.3 ALG Commands Example

The following example uses ALG to allow FTP through the Zyxel Device NAT.

```
usgflex200hp running config# vrf main alg ftp enabled true
usgflex200hp running config# commit
Configuration committed.
```

12.4 ALG SIP Commands

The following table lists the ALG SIP commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 37 ALG SIP Commands

COMMAND	DESCRIPTION
`vrf main alg sip enabled {true| false}`	Enables the ALG for SIP.
`vrf main alg sip port` *`<1..65535>`*	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
`vrf main alg sip direct-signaling {true| false}`	Sets the Zyxel Device to allow SIP signaling sessions.
`vrf main alg sip direct-media {true| false}`	Sets the Zyxel Device to allow SIP audio session.
`vrf main alg sip inactivity-timeout enabled {true| false}`	Sets the number of seconds (1-86400) for how long to allow a SIP signaling session to remain idle (without SIP packets) before dropping it.
`vrf main alg sip inactivity-timeout signal-timeout` *`<1..86400>`*	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Zyxel Device. If the SIP client does not have this mechanism and makes no calls during the Zyxel Device SIP timeout, the Zyxel Device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1-86400).
`vrf main alg sip inactivity-timeout media-timeout` *`<1..86400>`*	Sets how many seconds (1-86400) the Zyxel Device will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the Zyxel Device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

CHAPTER 13
Multicast

13.1 Multicast Introduction

This chapter explains how to use commands to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways – Unicast (one sender to one recipient) or Broadcast (one sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP Proxy

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group – it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

Internet Group Management Protocol (IGMP) proxy is used for multicast routing. IGMP proxy enables the Zyxel Device to issue IGMP host messages on behalf of hosts that the Zyxel Device discovered on its IGMP-enabled interfaces. The Zyxel Device acts as a proxy for its hosts.

mDNS Proxy

Multicast DNS (mDNS) is a protocol that sends discovery packets to resolve hostnames to IP addresses on a local network without using a DNS server. It is commonly used by zero-configuration services that require no manual IP or DNS setup, such as printers, TVs, AirPlay, Chromecast, and IoT devices.

mDNS uses a query and response exchange to allow devices to find each other and then establish a communication session.

mDNS discovery is only sent to a local network multicast address (224.0.0.251:5353). The Zyxel Device supports mDNS Proxy that allows the Zyxel Device to act as a the mDNS reflector to transmit the multicast discovery packets across subnets.

13.2 IGMP Commands

The following table lists the IGMP commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 38 IGMP Commands

COMMAND	DESCRIPTION
`vrf main multicast igmp-proxy enabled {true| false}`	Enables the IGMP Proxy to route multicast traffic.
`vrf main multicast igmp-proxy upstream interface <interface-name>`	Specifies an interface that connects to a router (host) running IGMP and closer to the multicast server. Note: You can specify Ethernet, VLAN, Bridge, or LAG interfaces as the IGMP Proxy upstream interface.
`vrf main multicast igmp-proxy downstream interface <interface-name>`	Specifies an interface that connects to the multicast hosts. Note: You can specify Ethernet, VLAN, Bridge, or LAG interfaces as the IGMP Proxy downstream interface.
`vrf main multicast reception-policy type {allow-all | allow-object}`	Specifies whether multicast traffic is sent to all IGMP hosts or only to specified IGMP hosts. `allow-all`: Sends all multicast traffic to all the IGMP host. `allow-object`: Sends multicast traffic only to the specified IGMP hosts. This is recommended when too much multicast traffic congests your network.
`vrf main multicast reception-policy allow-object-list <object-name>`	Specifies an existing IP address object to receive the multicast traffic.
`vrf main multicast mdns-proxy enabled {true| false}`	Enables the mDNS proxy to forward mDNS multicast traffic across subnets.
`vrf main multicast mdns-proxy allow-interface <interface-name>`	Specifies an internal interface that mDNS multicast packets are allowed to pass. Devices on the specified interfaces can receive and forward mDNS multicast packets. Note: You can specify two to four Ethernet, VLAN, Bridge, or LAG interfaces to enable communication between devices connected to these interfaces.
`show multicast route`	Displays the currently active multicast groups and the multicast traffic passing through the Zyxel Device.

13.3 Commands Example

The following example enables IGMP on the Zyxel Device and configures how the Zyxel Device routes multicast traffic.

```
MyUSGFLEX500H running config# vrf main multicast igmp-proxy enabled true
MyUSGFLEX500H running config# vrf main multicast igmp-proxy upstream interface
InterfaceA
MyUSGFLEX500H running config# vrf main multicast igmp-proxy downstream interface
InterfaceB
MyUSGFLEX500H running config# vrf main multicast reception-policy type allow-all
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# exit
```

The following example enables mDNS on the Zyxel Device and configures how the Zyxel Device routes multicast traffic.

```
MyUSGFLEX500H running config# vrf main multicast mDNS-proxy enabled true
MyUSGFLEX500H running config# vrf main multicast mDNS-proxy allow-interface ge3
MyUSGFLEX500H running config# vrf main multicast mDNS-proxy allow-interface ge4
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# exit
```

The following example displays the IP addresses of the currently active multicast groups and how the multicast traffic passes through.

```
MyUSGFLEX500H> show multicast route
show-multicast-route
    ok
        multicast-route
            group-address 224.10.10.10
            source-address 192.168.100.35
            incoming-interface ge1
            outgoing-interface ge4
            packet-count 48613
            ..
        multicast-route
            group-address 224.10.10.11
            source-address 192.168.169.33
            incoming-interface InterfaceA
            outgoing-interface InterfaceB
            packet-count 57923
            ..
        multicast-route-count 2
```

CHAPTER 14
Secure Policy

14.1 Secure Policy Overview

A secure 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

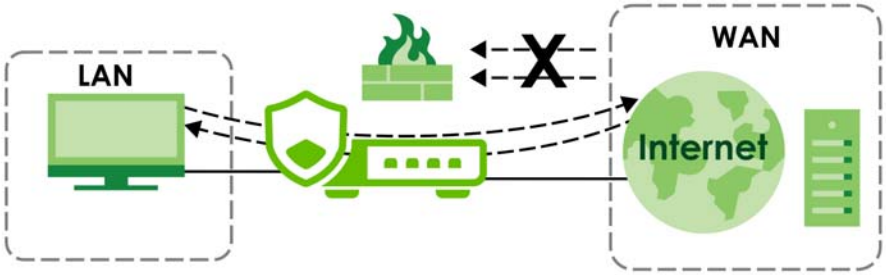
The policy can be configured:

- 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 security service profiles (such as application patrol, content filter, SSL inspection) to traffic that matches the criteria above

The secure 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 77 Default Directional Policy Example



14.1.1 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.

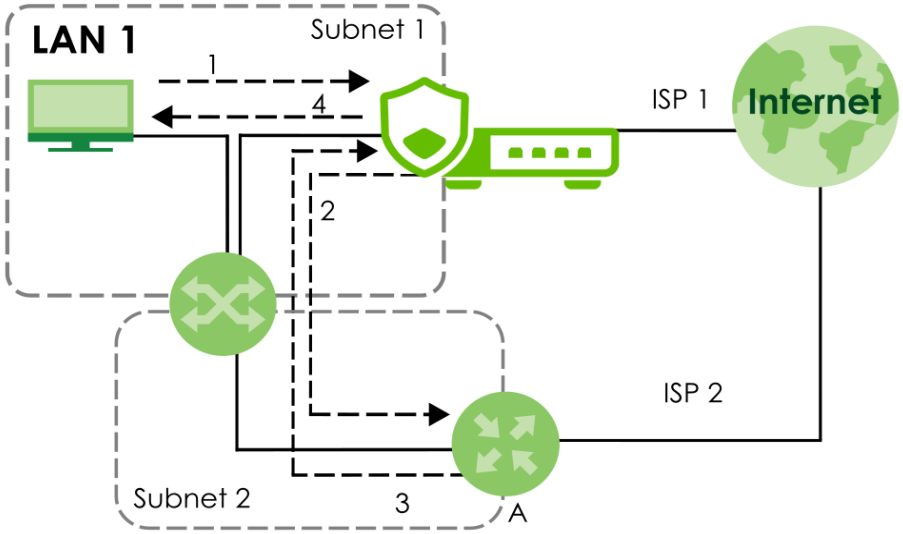
1 A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.

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 78 Using Virtual Interfaces to Avoid Asymmetrical Routes



14.2 Secure Policy Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 39 Secure Policy Command Input Values

LABEL	DESCRIPTION
address-object	The name of the IP address object. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user-object	The name of the user. You may use 1-30 single-byte characters, including 0-9a-zA-Z._-. This value is case-sensitive.

Table 39 Secure Policy Command Input Values (continued)

LABEL	DESCRIPTION
zone-object	The name of the zone. For some Zyxel Device models, use up to 30 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Devicemodels, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
schedule-object	The name of the schedule. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service-object	The name of the service. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

14.3 Secure Policy Commands

The following table describes the commands available for the secure policy. You must use the `edit running` command to enter the configuration mode before you can use the configuration commands.

Table 40 Secure Policy Commands

COMMAND	DESCRIPTION
`vrf main secure-policy enabled {true| false}`	Enables secure policy on the Zyxel Device.
`vrf main secure-policy default-rule action {allow| deny| reject} logging {no| log| log-alert}`	Sets how the secure policy handles packets that do not match any other secure policy rule.
`vrf main secure-policy asymmetrical-route enabled {true| false}`	Allows or disallows asymmetrical route topology.
`vrf main secure-policy rule <profile-name> action {allow| deny| reject}`	Sets the action the Zyxel Device takes when packets match this rule.
`vrf main secure-policy rule <profile-name> logging {no| log| log-alert}`	Sets the Zyxel Device to create a log or a log and an alert when packets match this rule. The `no` command sets the Zyxel Device not to create a log or alert when packets match this rule.
`vrf main secure-policy rule <profile-name> description <description>`	Sets a descriptive name (up to 60 printable ASCII characters) for a secure policy rule.
`vrf main secure-policy rule <profile-name> enabled {true| false}`	Activates the specified secure policy.
`vrf main secure-policy rule <profile-name> user {admin| user-object user-object| user-group user-group| any}`	Sets a user name or user group to which to apply the policy. The secure policy is activated only when the specified user logs into the system. The policy will be disabled when the user logs out. Sets this value to `any` to apply the policy to all users or user groups.
`vrf main secure-policy rule <profile-name> schedule {schedule-object schedule-object| schedule-group schedule-group| any}`	Sets the schedule that the policy uses.

Table 40 Secure Policy Commands (continued)

COMMAND	DESCRIPTION
vrf main secure-policy rule <*profile-name*> from {zone-object *zone-object*| any}	Sets the zone on which the packets are received.
vrf main secure-policy rule <*profile-name*> to {zone-object *zone-object*| any| ZyWALL}	Sets the zone from which the packets are sent.
vrf main secure-policy rule <*profile-name*> source-ip {address-object *address-object*| address-group *address-group*| any}	Sets an IPv4 address or address group object to apply the policy to traffic coming from it. Set this value to `any` to apply the policy to all traffic coming from IPv4 addresses.
vrf main secure-policy rule <*profile-name*> destination-ip {address-object *address-object*| address-group *address-group*| any}	Sets an IPv4 address or address group object to apply the policy to traffic going to it. Set this value to `any` to apply the policy to all traffic going to IPv4 addresses.
vrf main secure-policy rule <*profile-name*> service {service-object *service-object*| service-group *service-group*| any}	Sets a service or service group for the secure policy profile.
vrf main secure-policy rule <*profile-name*> content-filter-profile none	Uses this command if no content filter profiles have been created.
vrf main secure-policy rule <*profile-name*> content-filter-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) content filter profile to traffic that matches the secure-policy rule. `log by-profile`: Generates a log for all traffic that matches criteria in the content filter profile.
vrf main secure-policy rule <*profile-name*> ssl-inspection-profile none	Use this command if no SSL inspection profiles have been created.
vrf main secure-policy rule <*profile-name*> ssl-inspection-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) SSL inspection profile to traffic that matches the secure-policy rule. `log by-profile`: Generates a log for all traffic that matches criteria in the SSL inspection profile.
vrf main secure-policy rule <*profile-name*> app-patrol-profile none	Use this command if no app patrol profiles have been created.
vrf main secure-policy rule <*profile-name*> app-patrol-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) app patrol profile to traffic that matches the secure-policy rule. `log by-profile`: Generates a log for all traffic that matches criteria in the app patrol profile.
vrf main secure-policy block-quic enabled {true| false}	Blocks QUIC (Quick UDP Internet Connections, transport protocol that encrypts traffic) to stop browsers using QUIC so that the Zyxel Device can use SSL inspection to inspect encrypted traffic for AI requests and replies. If QUIC is not blocked, the Zyxel Device may not be able to inspect AI requests and replies in order to apply content filtering correctly.

Table 40 Secure Policy Commands (continued)

COMMAND	DESCRIPTION
`show config vrf main secure-policy`	Displays the secure policy settings.
`show state vrf main secure-policy`	Displays the secure policy settings including matching packets.

14.3.1 Secure Policy Command Examples

These are IPv4 secure policy configuration examples.

The following example shows you how to add an IPv4 secure policy rule to allow a MyService connection from the WAN zone to the IP addresses Dest_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Create a secure policy rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.
- Set the action the Zyxel Device is to take on packets which match this rule.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address Dest_1 type range
10.0.0.10-10.0.0.15
t service MyService type tcp 1234
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# vrf main secure-policy rule Rule1 from zone-object WAN
usgflex200hp running config# vrf main secure-policy rule Rule1 to zone-object LAN
usgflex200hp running config# vrf main secure-policy rule Rule1 destination-ip
address-object Dest_1
usgflex200hp running config# vrf main secure-policy rule Rule1 service service-
object MyService
usgflex200hp running config# vrf main secure-policy rule Rule1 action allow
usgflex200hp running config# vrf main secure-policy rule Rule1 user any
usgflex200hp running config# vrf main secure-policy rule Rule1 schedule any
usgflex200hp running config# vrf main secure-policy rule Rule1 source-ip any
usgflex200hp running config# vrf main secure-policy rule Rule1 content-filter-
profile none
usgflex200hp running config# vrf main secure-policy rule Rule1 ssl-inspection-
profile none
usgflex200hp running config# vrf main secure-policy rule Rule1 app-patrol-profile
none
usgflex200hp running config# commit
Configuration committed.
```

14.4 DoS Prevention Overview

DoS attacks can flood your Internet connection with invalid packets and connection request, 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.

DoS prevention protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces DoS prevention profiles and applying a DoS prevention 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.

14.5 DoS Prevention Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 41 DoS Prevention Command Input Values

LABEL	DESCRIPTION
zone	The name of a zone. Use up to 30 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case- sensitive.
profile-name	The name of a DoS prevention profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

14.6 DoS Prevention Commands

The following table describes the DoS prevention commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 42 DoS Prevention Commands

LABEL	DESCRIPTION
`vrf main dos-prevention enabled {true| false}`	Enables DoS prevention.
`vrf main dos-prevention profile <profile-name> description <description>`	Enter a description for the profile. You can use up to 60 printable ASCII characters .

Table 42 DoS Prevention Commands (continued)

LABEL	DESCRIPTION
`vrf main dos-prevention profile <profile-name> scan-detection {ip-protocol-scan| tcp-portscan| udp-portscan| icmp-sweep| ip-protocol-sweep| tcp-port-sweep| udp-port-sweep} action {none| block} enabled {true| false} logging {no| log| log-alert}`	Sets the scan detection options and actions. Generates a log (`log`) or a log and an alert (`log-alert`) when traffic matches the scan detection options you set.
`vrf main dos-prevention profile <profile-name> scan-detection sensitivity {low| medium| high}`	Sets scan detection sensitivity.
`vrf main dos-prevention profile <profile-name> scan-detection block-period <1...3600>`	Sets the time in seconds that the Zyxel Device blocks the source IP address from which the packets are coming if the Zyxel Device detects possible scan attack packets, such as port scanning.
`vrf main dos-prevention profile <profile-name> flood-detection {icmp-flood| ip-flood| tcp-flood| udp-flood} action {none| block} enabled {true| false} logging {no| log| log-alert} threshold <1...65535>`	Sets the flood detection options and actions. Generates a log (`log`) or a log and an alert (`log-alert`) when traffic matches the flood detection options you set. Sets a suitable threshold level (the number of packets per second that match the flood detection criteria) for your network. If you set a low threshold, most flood attacks will be detected, but you may have more logs and false positives. If you set a high threshold, some flood attacks may not be detected, but you will have fewer logs and false positives.
`vrf main dos-prevention profile <profile-name> flood-detection block-period <1...3600>`	Sets the time in seconds that the Zyxel Device blocks the source IP address from which the packets are coming if the Zyxel Device detects a large number of packets that are possibly attempting to flood your network.

Table 42 DoS Prevention Commands (continued)

LABEL	DESCRIPTION
vrf main dos-prevention profile <*profile-name*> protocol-anomaly-detection {icmp-smurf-attack | udp-smurf-attack | ip-fragment | ip-land-attack} enabled {true | false}	Sets and enables or disables a protocol anomaly detection option. • icmp-smurf-attack: ICMP Smurf Attack An ICMP Smurf attack is a distributed denial-of-service (DDoS) attack that floods a target (victim) with pings (ICMP echo request packets) where the source IP address is spoofed as the victim's IP address. The destination IP address of each packet is the broadcast address of the network, so all hosts on the network reply to the victim at once, overwhelming the victim. • udp-smurf-attack: UDP Smurf Attack A UDP Smurf attack is a distributed denial-of-service (DDoS) attack that floods a target (victim) with small UDP requests where the source IP address spoofed as the victim's IP address. Servers reply with responses to the victim, overwhelming the victim. The Zyxel Device detects the attack when it receives a UDP packet in which the destination IP address matches the broadcast address of the network and the destination port is 7 or 19. • ip-fragment: IP Fragment The Zyxel Device detects IP fragments when it receives packets with malformed, overlapping, or oversized fragments. • ip-land-attack: IP LAND Attack A LAND attack sends a spoofed packet where the source IP address is the same as destination IP address, so the victim replies to itself, causing DoS and making the victim unavailable.
vrf main dos-prevention profile <*profile-name*> protocol-anomaly-detection {icmp-smurf-attack | udp-smurf-attack | ip-fragment | ip-land-attack} logging {no | log | log-alert}	Sets the protocol anomaly detection options and actions. Generates a log (log), a log and an alert (log-alert), or neither (no) when traffic matches the specified protocol anomaly detection options.
vrf main dos-prevention profile <*profile-name*> protocol-anomaly-detection {icmp-smurf-attack | udp-smurf-attack | ip-fragment | ip-land-attack} action {none | drop}	Sets the action the Zyxel Device takes when traffic matches the specified protocol anomaly detection options. • none: No action when traffic matches the policy. • drop: Silently drops packets that match the policy. Neither the sender nor the receiver is notified.
vrf main dos-prevention policy <*policy-name*> enabled {true| false}	Enables or disables the DoS prevention policy.
vrf main dos-prevention policy <*policy-name*> from-zone zone-object {any| zone *zone*}	Specifies the zone the traffic is coming from.
vrf main dos-prevention policy <*policy-name*> bind-profile <*profile-name*> enabled {true| false}	Binds the DoS prevention profile to the entry's traffic direction.
show config vrf main dos-prevetion	Displays DoS prevention settings.

14.6.1 DoS Prevention Block List

DoS block lists contain IP addresses or domains that are identified as attackers launching DoS or Distributed DoS (DDoS) attacks. When the Zyxel Device sees traffic coming from an IP on the block list, it automatically blocks or drops those packets, preventing the attack traffic from reaching your network.

The following table describes the commands to display or remove IP addresses from a block list.

Table 43 Commands for URL / DNS Threat Filter External Block List

COMMAND	DESCRIPTION
`show dos-prevention-block-list`	Displays IP addresses in the DoS prevention block list.
`cmd dos-prevention-block-list clear all`	Removes all IP addresses from the DoS prevention block list to allow traffic from these IP addresses. You may do this if you changed the DoS profile and you want to have the updated profile scan for DoS attacks from scratch.
`cmd dos-prevention-block-list clear ip <ip address>`	Removes a specific IPv4 address from the DoS prevention block list to allow traffic from this IP address. You may do this if the IP address was wrongly classified as a source of DoS attacks by the DoS profile.

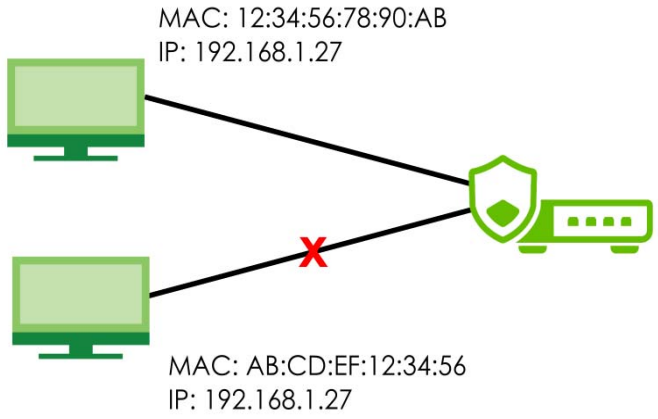
14.7 IP Spoofing Overview

Trusted IP address/MAC address Pair

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The Zyxel Device uses DHCP to assign IP addresses and records the MAC address it assigned to each IP address. The Zyxel Device then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the Zyxel Device.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 79 Trusted IP address/MAC address Pair



14.8 IP Spoofing Prevention Commands

The following table describes the IP spoofing prevention commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 44 IP Spoofing Prevention Commands

LABEL	DESCRIPTION
`vrf main spoofing-prevention enabled {true|false}`	Enables or disables IP spoofing prevention.
`vfr main spoofing-prevention rules <ip address> mac <MAC address> interface <interface> description <description>`	Sets a trusted IP address/MAC address pair to allow traffic from a device with that IP address/MAC address pair. • ip address: Enter the IP address that the Zyxel Device assigns to a device with the entry's MAC address. • mac: Enter the MAC address of the device to which the Zyxel Device assigns the entry's IP address. • interface: Enter the name of the interface on the Zyxel Device to trust the IP address/MAC address pair. • description: Enter a description to help identify the purpose of the rule. This is optional.
`vrf main spoofing-prevention trusted-ip <address-object>`	Specifies an address object to allow traffic from all devices with that IP address.
`show config vrf main spoofing-prevention`	Displays IP spoofing prevention settings.

14.8.1 IP Spoofing Command Example

This command shows how to set a trusted IP address/MAC address pair to allow traffic from a device with that IP address/MAC address pair.

```
usgflex500h> edit running
usgflex500h running config# vrf main spoofing-prevention enabled true
usgflex500h running config# vrf main spoofing-prevention rules 1.1.1.1
interface ge4 mac 11:33:66:99:ee:44
usgflex500h running config# show config vrf main spoofing-prevention
spoofing-prevention
    enabled true
    include-dhcp-lease true
    logging log
    rules 1.1.1.1
        interface ge4
        mac 11:33:66:99:ee:44
        ..
    trusted-ip CathyObject
        ..
```

14.9 System Protection Signature Commands

Use these commands to view the system protection signature information and update the signatures if necessary.

Table 45 System Protection Signature Commands

COMMAND	DESCRIPTION
`show system protection signature version`	Displays system protection signatures of the Zyxel Device. These signatures do not require a license. The Zyxel Device will synch with the Cloud Helper Server every day to update these signatures automatically. You can also update manually using the command below. Please note that in the web configurator, the system protection signature version displays in **Dashboard** > **About**. System protection signatures protect your Zyxel Device and local networks from web attacks, such as command injection, cross-site scripting and path traversal. Command injection: This is an attack in which an attacker uses the Zyxel Device vulnerabilities to execute commands to control your Zyxel Device. Cross-site scripting: This is an attack in which an attacker implants malicious scripts in a website. When you visit this website, the malicious scripts are sent and executed on your web browser. Path traversal: This is an attack that allows an attacker to access files you store in the web root folder.
`show system protection signature update status`	Displays if the system protection signatures are updated to the latest version.
`cmd system protection signatures update signature`	Use this command to update the system protection signatures to the latest version. Make sure the Zyxel Device can access the Cloud Helper Server when you want to update the signatures.

CHAPTER 15
Captive Portal

15.1 Overview

Use this screen to configure captive portal settings for each interface. A captive portal is a designated login web page for client authentication before network access.

The policy can be applied:

- to a specific interface or zone
- with the walled garden feature
- to a specific client or group of clients

The policy can be configured:

- to exempt specific source and destination address objects
- to exempt specific type of traffic
- to use with HTTP or HTTPS server

15.2 Captive Portal Commands

The following table describes general captive portal commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 46 Captive Portal Commands

COMMAND	DESCRIPTION
`vrf main captive-portal enabled {true | false}`	Activates captive portal on the Zyxel Device.
`vrf main captive-portal cp-server server enabled {true | false}`	Activates a captive portal authentication server with HTTP access.
`vrf main captive-portal cp-server server port <1..65535>`	Sets a HTTP port for the captive portal authentication server. The default port is 1080.
`vrf main captive-portal cp-server server-ip <ipv4-address>`	Sets an IPv4 address for the captive portal authentication server. The default IPv4 address is 6.6.6.6.
`vrf main captive-portal cp-server server-redirect-fqdn <fully-qualified-domain-name>`	Sets the FQDN (Fully Qualified Domain Name), such as www.example.com, for the captive portal authentication server.
`vrf main captive-portal cp-server secure-server enabled {true | false}`	Activates a secure captive portal authentication server with HTTPS access.
`vrf main captive-portal cp-server secure-server port <1..65535>`	Sets a HTTPS port for the secure captive portal authentication server. The default port is 1443.

Table 46 Captive Portal Commands (continued)

COMMAND	DESCRIPTION
`vrf main captive-portal cp-server secure-server force-https {true | false}`	Requires HTTPS for access to the secure captive portal authentication server. It is not recommended to enable this in order to avoid a certificate warning when users log into the captive portal.
`vrf main captive-portal cp-server secure-server auth-client {true | false}`	Requires client authentication for access to the secure captive portal authentication server.
`vrf main captive-portal cp-server secure-server certificate <cert-name>`	Requires the client to use a certificate as authentication for access to the secure captive portal authentication server. Note: Make sure the common name of certificate matches the server-redirect-fqdn setting.
`vrf main captive-portal cp-server max-concurrent-connection <256..65535>`	Sets the total allowed concurrent connections to the captive portal authentication server. The default is 256.
`vrf main captive-portal cp-server max-concurrent-connection-per-ip <16..65535>`	Sets the total allowed concurrent connections from the same IP address to the captive portal authentication server. The default is 16.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> enabled {true | false}`	Activates a specific captive portal policy on the Zyxel Device. `captive-portal-policy-uid`: The name of the captive portal policy you want to configure. The name can contain 1–31 single-byte characters, including [A–Z], [a–z], [0–9], and [\._-]. The name must start with [A–Z], [a–z], [0–9], [_], or [-]. If you create a profile using the Web Configurator, you cannot name it. You can see the automatically generated name in the CLI. It starts with “cp” followed by a sequential number in the order the profiles are created.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> description <string>`	Describes the specific captive portal policy on the Zyxel Device.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> incoming-type {interface-object | zone-object}`	This captive portal policy specifies network access for traffic that is coming in from the specified type of object (interface or zone) that has to authenticate with the captive portal server.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> incoming <interface | zone-name>`	This captive portal policy specifies network access for traffic that is coming in from the name of the object (interface or zone) that has to authenticate with the captive portal server.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> source-ip <object-name>`	Sets an object or group to enforce the policy on traffic from the specified object or group members.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> destination-ip <object-name>`	Sets an object or group to enforce the policy on traffic to the specified object or group members.

Table 46 Captive Portal Commands (continued)

COMMAND	DESCRIPTION
`vrf main captive-portal auth-policy <captive-portal-policy-uid> exempt-list <exempt-entry-uid> type {src-ip | service} object <object>`	Sets an exemption list of objects that do not need to authenticate with the captive portal server. `exempt-entry-uid`: The name of the entry you want to configure. If you create an entry using the Web Configurator, you cannot name it. You can see the automatically generated name in the CLI. It starts with "exempt" followed by a sequential number in the order the entries are created. `src-ip`: Exempts objects based on their source IP address. `service`: Exempts an object or a group of members based on the service. `object`: When using `service`: Sets an existing object or group by name. When using `src-ip`: Sets an existing object by name, a host IP address, a range of IP addresses using CIDR notation, or a range of IPv4 addresses by entering the start and end addresses separated by a hyphen (-).
`vrf main captive-portal auth-policy <captive-portal-policy-uid> redirect-tcp-443 {true | false}`	This captive portal policy redirect HTTPS traffic to the captive portal. It is not recommended to enable this in order to avoid the certificate warning that hotspot users will see when they log into the captive portal.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> idle-timeout-enabled {true | false}`	Enables or disables the specified idle timeout period that determines how long users can remain logged in without activity before being automatically logged out.
`vrf main captive-portal auth-policy <captive-portal-policy-id> idle-timeout <1...60>`	Specifies an idle timeout period (in minutes) that determines how long users can remain logged in without activity before being automatically logged out.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> sign-in-method {sign-on | click-to-continue}`	This captive portal policy specifies how clients are required to sign in for access to the captive portal server. `sign-on`: Blocks network access until the clients authenticate through the specified authentication policy. `click-to-continue`: Blocks network access until clients agree to the user agreement policy.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> portal-type {internal | external}`	This captive portal policy specifies the portal type that clients use to log on for network access. `internal`: Uses the default web page on the Zyxel Device. `external`: Uses the URL of an external portal. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> after-login-action {success-page | session-page | promotion-page}`	Specifies the page that clients will see when they successfully log into the captive portal. `success-page`: Keeps users on the success page after a successful login. `session-page`: Keeps users on the login page after a successful login. `promotion-page`: Redirects users to the specified URL after a successful login.

Table 46 Captive Portal Commands (continued)

COMMAND	DESCRIPTION
`vrf main captive-portal auth-policy <captive-portal-policy-uid> log {no | log | log-alert}`	This captive portal policy specifies if access attempts that are blocked before login should have a log (`log`) or alert (`log-alert`) or neither (`no`).
`vrf main captive-portal auth-policy <captive-portal-policy-uid> authentication-server type {local | ad server <ad-server-name> | ldap server <ldap-server-name> | radius server <radius-server-name> | oidc server <oidc-server-name> | cloud-auth}`	Specifies the captive portal authentication server: local on the Zyxel Device, AD (Active Directory), LDAP (Lightweight Directory Access Protocol RADIUS (Remote Authentication Dial-In User Service), OIDC (OpenID Connect), or NCAS (Nebula Cloud Authentication Server). You must first create the authentication server. See Section 32.2 on page 254 for more information on authentication servers.
`vrf main captive-portal auth-policy cp1 authentication-server cloud-disconnect-behavior {open | restricted}`	Allows or denies clients to access the network without authentication when NCAS (Nebula Cloud Authentication Server) is not reachable. `Open`: Clients can access the network with temporary credentials. They are logged out when the Zyxel Device reconnects to NCAS. After that, they can log in again with their credentials. `Restricted`: Clients cannot access until the connection between the Zyxel Device and NCAS (Nebula Cloud Authentication Server) is restored.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> authentication-server server <server-name>`	This captive portal policy specifies the name of the captive portal authentication server.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> external-portal-url <url>`	Specifies the URL of the external portal page to use when 'portal-type' is set to `external`. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`vrf main captive-portal auth-policy <captive-portal-policy-uid> external-promotion-url <url>`	Specifies the URL of the external promotion page to use when 'after-login-action' is set to `promotion-page`. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`vrf main captive-portal cp-server policy-match-cache-size <500..100000>`	Specifies the maximum number of entries in the captive-portal policy match cache. A captive-portal policy match cache stores recent session or client matches so the Zyxel Device doesn't have to repeatedly re-evaluate every packet against all captive-portal policies. The maximum entry limit prevents the cache from consuming excessive memory and enhances performance when tracking policy matches. These are the default values per model at the time of writing: • USG FLEX 50H/50HP: 500 • USG FLEX 100H/100HP: 1,000 • USG FLEX 200H/200HP: 2,000 • USG FLEX 500H: 5,000 • USG FLEX 700H: 10,000

Table 46 Captive Portal Commands (continued)

COMMAND	DESCRIPTION
`vrf main captive-portal cp-server policy-match-rate-limit <30..1000>`	Specifies the rate-limit threshold for HTTP/HTTPS requests per source IP, measured in requests per second. The default value is 100. A captive-portal policy-match-rate-limit prevents the Zyxel Device from being overwhelmed by too many new policy-match lookups per second, reducing CPU overload and increasing stability if there are DoS attacks.
`vrf main captive-portal settings redirect-parameter {ap-ip | ap-mac | client-ip | client-mac | ssid-name | vlan-id}`	Sets what the Zyxel Device appends to the redirect URL when an unauthenticated client is sent to the captive portal (or to an external authentication / landing page). After the Zyxel Device redirects the client to the portal URL, the redirect-parameters are appended to the URL. You may use from 0 (default value is used) to 31 uppercase English letters, lowercase English letters, underscores, and hyphens. The 'default value' means the parameter name used in the URL query string, not the value itself. Use the correct format for each type. • `ap-ip`: IP address of the Access Point that the client is connected to. • `ap-mac`: MAC address of the Access Point. • `client-ip`: IP address assigned to the client device. • `client-mac`: MAC address of the client device. • `ssid-name`: The WiFi network (SSID) the client is connected to - useful if multiple SSIDs share a portal. • `vlan-id`: VLAN ID used by the client connection. With redirect-parameters an external portal server can identify the user's SSID, apply different login rules per VLAN, log client MAC/IP for auditing, bind authentication to a specific AP, track which AP users connect to, identify problem VLANs or SSIDs and/or log client locations indirectly. Note that: • These parameters are read-only for the client. • They are not encrypted unless HTTPS is used. • External portals must be able to parse and trust these values appropriately. • Only change default values if your portal can use custom names.
`vrf main captive-portal settings redirect-parameter mac-delimiter {colon | hyphen}`	Sets how MAC values are formatted. `colon` is the default. If the portal requires MAC addresses formatted with hyphens, then change the mac_delimiter to `hyphen`.
`vrf main captive-portal settings external-portal-allow-get-method {true | false}`	Sets how an external captive portal sends login credentials (user name and password) to the Zyxel Device. The default is to use HTTP POST (`false`). If you set the command to `true` then the external captive portal can use HTTP POST or HTTP GET to send login credentials to the Zyxel Device. • `false`: parameters are sent using HTTP POST • `true`: parameters are sent using HTTP POST or HTTP GET (URL query string). Some captive portals may only support GET.
`show config vrf main captive-portal-theme`	Displays the captive portal themes available when the Zyxel Device is connected to Nebula. You can create a custom theme in Nebula.

15.2.1 Redirect Parameter Example

This is an example using the following redirect parameter names. WTP is Wireless Termination Point, which is the MAC address of the Access Point. In this example, the external portal expects hyphens for MAC addresses, so the `mac-delimiter` command is used. `external-portal-allow-get-method` is enabled (`true`), as in this example the external portal can only use HTTP GET to send login credentials to the Zyxel Device.

```
usgflex500h> edit running
USGFLEX500H running config# vrf main captive-portal settings redirect-parameter
ap-ip ap-ip
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter ap-
mac wtp-mac
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter
client-ip client-ip
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter
client-mac client-mac
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter
ssid-name ssid
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter
vlan-id vlan
USGFLEX500H running config#vrf main captive-portal settings redirect-parameter
mac-delimiter hyphen
USGFLEX500H running config#vrf main captive-portal settings external-portal-allow-
get-method true
USGFLEX500H running config#
```

15.3 Walled Garden Commands

With a walled garden, you can define the domains that clients can access without logging in. The following table describes general captive portal commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 47 Walled Garden Commands

COMMAND	DESCRIPTION
`vrf main captive-portal auth-policy <captive-portal-policy-uid> walled-garden enabled {true | false}`	Activate a walled garden, which defines web site address(es) that clients can access without logging in.
`[del] vrf main captive-portal auth-policy <captive-portal-policy-uid> walled-garden trusted-identity-provider <list-name>`	Specifies the predefined walled garden list. Therefore, clients can access the listed domains before authentication. `list-name`: The name of the predefined walled garden list. Use the `show captive-portal walled-garden-signature` command to view the list name. See Section 15.3.1 on page 136 for an example.

Table 47 Walled Garden Commands (continued)

COMMAND	DESCRIPTION
`vrf main captive-portal auth-policy <captive-portal-policy-uid> walled-garden rules <walled-garden-entry-uid> type {object <object-name> | fqdn <fqdn> | cidr <cidr>}`	Sets an object that can access the walled garden. `walled-garden-entry-uid`: The name of the entry you want to configure. If you create an entry using the Web Configurator, you cannot name it. You can see the automatically generated name in the CLI. It starts with "wg" followed by a sequential number in the order the entries are created. `object-name`: Sets an existing object by its name. `fqdn`: Sets an object using FQDN. `cidr`: Sets a range of IP addresses using CIDR notation. For example, 192.168.0.0/16.
`cmd captive-portal walled-garden-signature update`	Updates the predefined walled garden lists. The list is automatically updated periodically and after the Zyxel Device reboots. To update immediately, use this command.
`show captive-portal walled-garden-signature`	Displays the predefined walled garden lists. It includes the domains associated with the OIDC providers.
`show captive-portal walled-garden-signature version`	Displays the version of predefined walled garden lists.
`show captive-portal walled-garden-signature update status`	Displays the update status of predefined walled garden lists.

15.3.1 Walled Garden Example

This example shows how to apply a walled garden list when using Google Workspace as the OIDC server for authentication. See Section 32.2.3 on page 257 for more information on OIDC.

1 Check the walled garden list you want to apply and its associated domains.

```
MyUSGFLEX500H> show captive-portal walled-garden-signature
captive-portal-show-walled-garden-signature
    data
        walled-garden-list-version 1.0.0.20260203.1
        walled-garden-list
            name captive_portal_default_walled_garden
            description "captive portal default walled garden"
            fqdn-list d.myzyxel.com
            fqdn-list d2.myzyxel.com
            .
            .
            ..
        walled-garden-list
            name captive_portal_google_oidc
            description "captive portal walled garden for Google OIDC"
            oidc-provider "Google Cloud Identity / Workspace"
            fqdn-list accounts.google.com
            fqdn-list apis.google.com
            .
            .
            ..
        walled-garden-list
            name captive_portal_microsoft_oidc
            description "captive portal walled garden for Microsoft OIDC"
            oidc-provider "Microsoft Entra ID"
            fqdn-list *.aadcdn.msftauth.net
            fqdn-list *.aadcdn.msftauthimages.net
            .
            .
            ..
        ..
```

2 Apply the walled garden list to the specified captive portal policy.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# vrf main captive-portal auth-policy cp1 walled-
garden trusted-identity-provider captive_portal_google_oidc
MyUSGFLEX500H running config# commit
Configuration committed.
```

CHAPTER 16
IPSec VPN

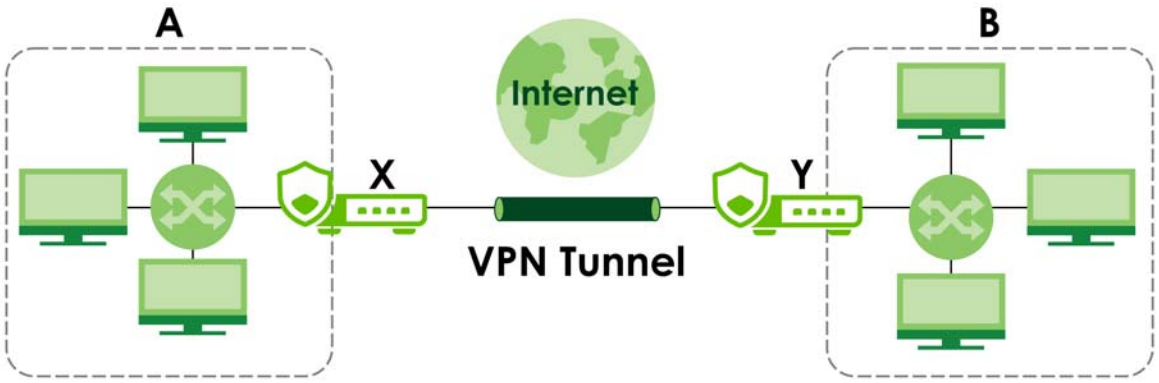
16.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure is one example of a VPN tunnel. Here local Zyxel Device **X** uses an IPSec VPN runnel to remote (peer) Zyxel Device **Y** to connect the local (**A**) and remote (**B**) networks.

Figure 80 VPN: Example



A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the Zyxel Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the Zyxel Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the Zyxel Device and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 81 VPN: IKE SA and IPSec SA

In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

Encryption Methods

In most Zyxel Devices, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.
- **AES-GCM** (Galois/Counter Mode) offers secure (prevents both passive eavesdropping and active tampering), authenticated encryption that is faster than AES as it is optimized for modern CPUs.

Authentication Methods

You can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA384 (Secure Hash Algorithm) produces a 384-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.
- PRF (PseudoRandom Function)-SHA256/384/512 does not encrypt data, but derives keys, authenticates handshake messages and produces strong session keys from initial secrets. It is not used to encrypt or authenticate the VPN data when AES-GCM is the encryption method; it is used to generate the keys that AES-GCM will use.

Diffie-Hellman (DH) Groups

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. ECP (Elliptic Curve Cryptography Prime) and MODP (Modular Exponential) groups are used for the Diffie-Hellman (DH) key exchange protocol in establishing secure VPN tunnels. Higher Diffie-Hellman group numbers of the same algorithm (MODP, ECP NIST, ECP Brainpool) are usually more secure, but also require more processing power to encrypt and decrypt information.

The Zyxel Device supports these Diffie-Hellman groups in increasing order of strength (and required processing power) for each group:

MODP

1 Diffie-Hellman Group 2 (1024-bit)

2 Diffie-Hellman Group 5 (1536-bit)

3 Diffie-Hellman Group 14 (2048-bit)

4 Diffie-Hellman Group 15 (3072-bit)

5 Diffie-Hellman Group 16 (4096-bit)

ECP NIST (National Institute of Standards and Technology)

1 Diffie-Hellman Group 19 (256-bit random)

2 Diffie-Hellman Group 20 (384-bit random)

3 Diffie-Hellman Group 21 (521-bit random)

ECP Brainpool

1 Diffie-Hellman Group 28 (256bp-bit Brainpool elliptic curve group)

2 Diffie-Hellman Group 29 (384bp-bit Brainpool elliptic curve group)

3 Diffie-Hellman Group 30 (512bp-bit Brainpool elliptic curve group)

CFRG (Crypto Forum Research Group)

1 Diffie-Hellman Group 31 (Curve25519 / X25519)

2 Diffie-Hellman Group 32 (Curve448 / X448)

Security strength depends on the DH group as well as the DH group number. The following table lists DH groups by number, not by strength.

Table 48 DH Groups

DH GROUP	CURVE / PRIME	APPROX. SECURITY LEVEL
2	MODP 1024	~80-bit
5	MODP 1536	~96-bit
14	MODP 2048	~112-bit
15	MODP 3072	~128-bit
16	MODP 4096	~152-bit
19	NIST P-256 (secp256r1)	~128-bit
20	NIST P-384 (secp384r1)	~192-bit
21	NIST P-521 (secp521r1)	~256-bit
28	Brainpool ECP group (brainpoolP256r1)	~128-bit
29	Brainpool ECP group (brainpoolP384r1)	~192-bit
30	Brainpool ECP group (brainpoolP512r1)	~256-bit
31	Curve25519 (X25519)	~128-bit
32	Curve448 (X448)	~224-bit

Note: Make sure that both ends of the VPN tunnel use the same DH group number.

As a guideline, for legacy systems where compatibility is needed, use MODP, such as DH Group 14 or DH Group 15.

16.1.1 Recommended VPN Algorithm Table

IKEv1

Table 49 Recommendations for IKEv1

PHASE	PARAMETER	RECOMMENDED (STRONG)	NOTES
Phase 1 (IKE SA)	DH Group	19 (P-256) or 21 (P-521)	Elliptic Curve DH is faster and strong
	Encryption	AES256	AES256 with SHA256
	Integrity / Authentication	SHA256	
	Lifetime	28800 sec	Standard, can reduce for highly dynamic peers
Phase 2 (Child SA / IPsec ESP)	Encryption	AES256-GCM	AEAD mode handles both encryption & integrity
	Integrity	Not required if using AES-GCM	Optional SHA256/SHA384 if using plain AES
	PFS DH Group	19 or 21	Recommended, especially for sensitive traffic
	Lifetime	3600–28800 sec	Typical, adjust per policy

IKEv2

Table 50 Recommendations for IKEv2

PHASE	PARAMETER	RECOMMENDED (STRONG)	NOTES
Phase 1 (IKE SA)	DH Group	19 (P-256) or 21 (P-521)	Elliptic Curve DH is faster and strong
	Encryption	AES256-GCM (preferred AEAD)	If AES-GCM not available, AES256 with SHA256
	Integrity / Authentication	PRF-SHA256	PRF required for key derivation
	Lifetime	28800 sec	Standard, can reduce for highly dynamic peers
Phase 2 (Child SA / IPsec ESP)	Encryption	AES256-GCM	AEAD mode handles both encryption & integrity
	Integrity	Not required if using AES-GCM	Optional SHA256/SHA384 if using plain AES
	PFS DH Group	19 or 21	Recommended, especially for sensitive traffic
	Lifetime	3600–28800 sec	Typical, adjust per policy

Additional Recommendation Notes

- Choose AES-GCM for encryption and integrity.
- Use strong DH groups (14+ for traditional, 19+ for elliptic curve).
- Avoid legacy algorithms: DES, 3DES, MD5, SHA1.
- PRF-SHA256 (or higher) is mandatory for IKEv2 key derivation.
- Phase 2 Perfect Forward Secrecy should use strong DH groups.

16.2 IPSec VPN Command Input Values

The following table describes the values required for many IPSec VPN commands. Other values are discussed with the corresponding commands.

Table 51 IPSec VPN Command Input Values

LABEL	DESCRIPTION
policy-name	The rule name of an IKE SA, remote IPSec router or VPN. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain-name	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
email	An e-mail address. You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters.

16.2.1 IPSec VPN Commands: Site-to-Site

This table lists the commands for site-to-site IPSec VPN.

Table 52 IPSec VPN Commands: Site-to-Site

COMMAND	DESCRIPTION
`vrf main ike enabled {true| false}`	Enables the IPSec VPN connection.
`vrf main ike pre-shared-key <key>`	Enter a password for authentication. Enter 8-128 alphanumeric characters (0-9a-zA-Z) or 8-128 pairs of hexadecimal characters (0-9A-F) beginning with 0x.
`vrf main ike ike-policy-template <policy-name>`	Enter the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`vrf main ike ike-policy-template <policy-name> ike-proposal <proposal> {enc-alg <aes128-cbc | aes192-cbc | aes256-cbc | des-cbc | 3des-cbc> | auth-alg <hmac-md5 | hmac-sha1 | hmac-sha256 | hmc-sha384 | hmac-sha512> | dh-group <modp1024 | modp1536 | modp2048 | modp3072| modp4096 | ecp256 | ecp384 | ecp521 | ecp256bp | ecp384bp | ecp512bp | curve25519 | curve> | aead-alg <aes128-gcm-128 | aes192-gcm-128 | aes256-gcm-128> | prf-alg <hmac-md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512>}`	Sets the encryption and authentication algorithms for each IKE SA proposal. • `aead-alg`: List of combined-mode AEAD (Authenticated Encryption with Associated Data - they encrypt and authenticate data simultaneously) algorithms for IKE SAs. • `auth-alg`: List of authentication algorithms for IKE SAs. • `dh-group`: List of Diffie Hellman groups for key exchange. • `enc-alg`: List of encryption algorithms for IKE SAs. • `prf-alg`: List of pseudo-random algorithms for IKE SAs.
`vrf main ike ike-policy-template <policy-name> {remote-auth-method| local-auth-method} {pre-shared-key| certificate| eap-md5| eap-mschapv2}`	Sets the authentication method for the remote IPSec router or the Zyxel Device. Sets the authentication method to `pre-shared-key` to use a password for authentication. Sets the authentication method to `certificate` to use one of the Zyxel Device certificates for authentication. Sets the authentication method to `eap-md5` or `eap-mschapv2` to use the selected algorithm for authentication.

Table 52 IPSec VPN Commands: Site-to-Site (continued)

COMMAND	DESCRIPTION
`vrf main ike ike-policy-template <policy-name> aggressive {true| false}`	Set `aggressive` to `true` to set IKEv1 to aggressive mode to establish an IKE SA faster. Set `aggressive` to `false` to set IKEv1 to main mode to establish an IKE SA in a more secure way.
`vrf main ike ipsec-policy-template <policy-name>`	Enter the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`vrf main ike ipsec-policy-template <policy-name> esp-proposal <proposal> {enc-alg <aes128-cbc| aes192-cbc| aes256-cbc| des-cbc| 3des-cbc>| auth-alg <hmac-md5| hmac-sha1| hmac-sha256| hmc-sha384| hmac-sha512>| dh-group <modp1024| modp1536| modp2048| modp3072| modp4096| ecp256| ecp384| ecp521| ecp256bp| ecp384bp| ecp512bp>}`	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal.
`vrf main ike ipsec-policy-template <policy-name> dpd-action {clear| restart| trap}`	Sets the Dead Peer Detection (DPD) action the Zyxel Device performs.
`vrf main ike ipsec-policy-template <policy-name> replay-window <0...4096>`	Sets the replay window size. The default value is 32. Sets the value to 0 to disable replay detection.
`vrf main ike ipsec-policy-template <policy-name> rekey-time <180...3000000>`	Sets the IKE SA life time to the specified value. The default value is 28800.
`vrf main ike ipsec-policy-template <policy-name> rekey-packets <0...65535>`	Sets the number of packets the Zyxel Device sends or receives before renegotiating the IKE SA
`vrf main ike ipsec-policy-template <policy-name> rekey-bytes <0...65535>`	Sets the number of bytes the Zyxel Device sends or receives before renegotiating the IKE SA
`vrf main ike vpn <policy-name>`	Sets the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`vrf main ike vpn <policy-name> bind-interface <interface>`	Specifies the local interface which will be used to initiate and receive IKE traffic in this VPN rule.
`vrf main ike vpn <policy-name> ike-policy template <policy-name>`	Sets the IKE SA rule for the VPN rule.
`vrf main ike vpn <policy-name> ipsec-policy template <policy-name>`	Sets the remote IPSec router rule for the VPN rule.
`vrf main ike vpn <policy-name> version <0...2>`	Sets IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. Sets the value to 0 to have the Zyxel Device accept both IKEv1 and IKEv2.
`vrf main ike vpn <policy-name> local-address <ipv4| subnet>`	Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
`vrf main ike vpn <policy-name> remote-address <ipv4| subnet>`	Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.

Table 52 IPSec VPN Commands: Site-to-Site (continued)

COMMAND	DESCRIPTION
`vrf main ike vpn <policy-name> local-id <ipv4| domain-name| email>`	Enter one of the followings to identify the Zyxel Device during authentication. IPv4 - the Zyxel Device is identified by an IP address DNS - the Zyxel Device is identified by a domain name E-mail - the Zyxel Device is identified by the string specified in this field
`vrf main ike vpn <policy-name> remote-id <ipv4| domain-name| email| any| subject-name>`	Enter one of the followings to identify the remote IPSec router during authentication. IPv4 - the remote IPSec router is identified by an IP address DNS - the remote IPSec router is identified by a domain name E-mail - the remote IPSec router is identified by the string specified in this field Any - the Zyxel Device does not check the identity of the remote IPSec router If the Zyxel Device and remote IPSec router use certificates, there is one more choice. Subject Name - the remote IPSec router is identified by the subject name in the certificate
`vrf main ike vpn <policy-name> ipsec-nat vpn-nat-rules <1...20> nat-type {snat| nat-1-1-map}`	Sets the NAT type for the VPN rule. • `snat`: Use this when there are no overlapping local and remote VPN IP addresses. • `nat-1-1-map`: Use this to avoid overlapping local and remote VPN IP addresses. The peer Zyxel Device must create identical mirror configurations.
`vrf main ike vpn <policy-name> ipsec-nat vpn-nat-rules <1...20> source-ip {object object| address address-object |cidr cidr}`	Enter the source IP address from the VPN local policy subnet to be used for NAT. This can be an IP address object `(object)`, a specific IP address (`address-object`), or a CIDR range (`cidr`).
`vrf main ike vpn <policy-name> ipsec-nat vpn-nat-rules <1...20> mapped-ip {object object| address address-object |cidr cidr}`	Specifies the mapped IP address the VPN rule. It the NAT type is `snat`, enter an IP address or subnet in the local IP address range to map the sender's source IP address for the VPN rule. If the NAT type is `nat-1-1-map`, enter an IP address or subnet in the Local IP address range to map the sender's source IP address or subnet for the VPN rule (SNAT). The local IP address range must not conflict with the peer's local IP address range. In the peer IPSec router, the destination IP from the sender is mapped to the local IP address of the receiver (DNAT).

Table 52 IPSec VPN Commands: Site-to-Site (continued)

COMMAND	DESCRIPTION
`vrf main ike vpn <policy-name> security-policy <policy-name> [local-ts | remote-ts] {object <object> | subnet <ipv4-address> | protocol <protocol>}`	Specifies the IP address on the local and remote sites whose traffic will be routed through the VPN tunnel. • `policy-name`: When you add a new entry, a name is automatically generated based on this VPN connection policy name, followed by _sp1. You can also manually change the name. • `object`: The configured host, subnet, or interface subnet object. • `ipv4-address`: The IPv4 address in a single CIDR format (for example, 192.168.10.0/24). • `protocol`: The protocol required for this connection. Enter `1` for ICMP, `6` for TCP, `17` for UDP, `47` for GRE, or `any` for any protocol type.
`vrf main ike global-options retransmit-tries <0..100>`	When the Zyxel Device sends an IKE message and no response arrives within a timeout period, it retransmits the message. This command sets the number of times to retransmit a packet before giving up. It will connect to a secondary gateway, if you have configured a secondary gateway and enabled nailed up. The default is 3, with a range of 0 to 100. 0 means the Zyxel Device gives up if no response is received to the first IKE message.
`vrf main ike global-options retransmit-timeout <0.000 .. 60.000>`	Sets how long to wait in seconds before sending the first retransmit packet. The default is 4.00 seconds.

Table 52 IPSec VPN Commands: Site-to-Site (continued)

COMMAND	DESCRIPTION
`vrf main ike global-options retransmit-base <0.000 .. 10.000>`	Sets the interval for IKE packet retransmissions (exponential backoff) within one negotiation. Exponential backoff means each retransmission waits twice as long as the previous one before retrying. The mathematical formula of retransmission timeout of IKEv2 negotiation is: relative timeout = retransmit-timeout * retransmit-base $^{(n-1)}$ The total time is the sum of the initial timeout and each subsequent retransmission timeout. For example, if the retransmit-base is 1.8, and the retransmit tries is 3, then the retransmission schedule would be as follows. 1. Initial request: The first packet is sent. The first timeout occurs after 4.0 seconds. 2. First retransmission: The second packet is sent after the initial timeout expires. The timeout for the first retransmission is: 4.0 * $1.8^{(2-1)}$ = 7.2 seconds 3. Second retransmission: The third packet is sent after the previous timeout expires. The timeout for the second retransmission is: 4.0 * $1.8^{(3-1)}$ = 12.96 seconds 4. Third retransmission: The fourth and final packet is sent. The timeout for the final retransmission is: 4.0 * $1.8^{(4-1)}$ = 23.33 seconds. The total time before the daemon gives up after 3 retransmissions, is the sum of all timeout intervals: Total time = 4.0 + 7.2 + 12.96 + 23.33 = 47.08 seconds.
`vrf main ike global-options retry-initiate-interval <0..255>`	Defines how long the Zyxel Device waits before starting a new IKE negotiation after the previous negotiation failed, thus preventing excessive negotiations. The default is 0 which disables starting new IKE negotiations.

16.2.2 Site-to-Site Command Example

This command shows the IPSec SA (Security Association) details. For the remote (peer) gateway, [0] means it has a dynamic IP address, [1] means it is using the primary IP address, and [2] means it is using the secondary IP address.

```
show ike ike-sa details
ikev1s2s: #1, ESTABLISHED, IKEv1, b9df641e41db3392_i 244275590870fcf5_r local
'192.168.195.37' @ 192.168.195.37 [500]
remote '192.168.195.55' [0] 192.168.195.55 [500] aes256-cbc/hmac-sha1/hmac-sha1/
modp2048
established 11s ago, rekeying in 82867s
sec_policy1_ikev1s2s: #2, reqid 1, INSTALLED, TUNNEL, esp:aes256-cbc/ installed
11s ago, rekeying in 27991s, expires in 31669s
in cadeбede, 672 bytes, 8 packets out cb8d1649, 672 bytes, 8 packets local
192.168.51.0/24
remote 192.168.61.0/24
```

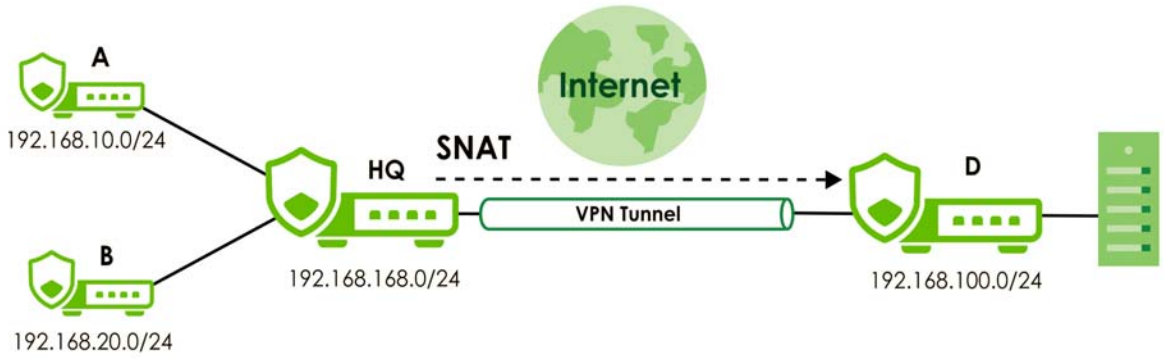
16.2.3 Policy-Based VPN NAT Advanced Scenarios

The following are application scenarios for SNAT and 1-1 NAT.

SNAT VPN Scenario

Here is an example of SNAT VPN scenario. Use this when there are no overlapping local and remote VPN IP addresses. Map the source IP address of the sender to an IP address in the Local IP address range (in the **Mapped IP** field) for the VPN rule. The headquarters (**HQ**) and branch sites **A** and **B** need to access the remote datacenter (**D**). The source IP addresses of sites **A** and **B** are not in the range of the local policy's IP address (192.168.168.0/24) for Phase 2. NAT rules need to be configured to translate the source IP addresses of sites **A** and **B** to an IP address in the 192.168.168.0/24 range before entering the IPsec tunnel.

Figure 82 Policy Based VPN - SNAT Example Scenario



The administrator need to set up VPN policy on both sites.

Table 53 Phase 2 Local/Remote Policy Settings Example

LOCAL POLICY	REMOTE POLICY
192.168.168.0/24	192.168.100.0/24

Table 54 Phase 2 NAT Rule Settings Example

SITE	TYPE	ORIGIN IP	MAPPED IP
Site A	SNAT	192.168.10.0/24	192.168.168.11/32
Site B	SNAT	192.168.20.0/24	192.168.168.12/32

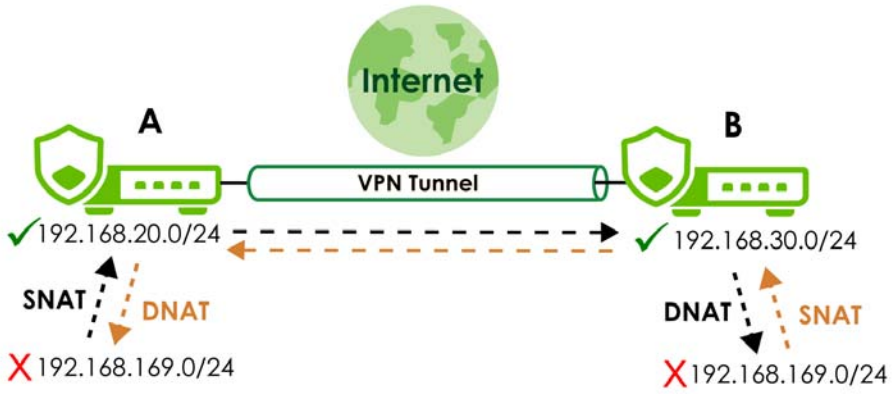
1-1 NAT VPN Scenario

Here is an example of a 1:1 NAT VPN scenario.Use this to avoid overlapping local and remote VPN IP addresses. IPSec router **A** and IPSec router **B** need to access each other, but they have overlapping subnets. To avoid conflicts, both IPSec routers need to create identical 1:1 NAT rules that map their local subnet to a non-overlapping subnet.

In the following example, IPSec router **A** is sending traffic to router **B**. Before data entering the VPN tunnel, the source IP address (set in **Origin IP**) from router **A** is translated to a mapped IP address (set in **Mapped IP**). After data exiting the VPN tunnel, router **B** translates the destination IP address (set in **Mapped IP**) back to the **Origin IP**.

Note: The **Mapped IP** of IPSec router **A** and **B** must not be in conflict.

Figure 83 Policy Based VPN - 1:1 NAT Example Scenario



The administrator need to set up VPN policy on both sites.

Table 55 Phase 2 Local/Remote Policy Settings Example

SITE	LOCAL POLICY	REMOTE POLICY
Site A	192.168.20.0/24	192.168.30.0/24
Site B	192.168.30.0/24	192.168.20.0/24

Table 56 Phase 2 NAT Rule Settings Example

SITE	TYPE	ORIGIN IP	MAPPED IP
Site A	1:1 NAT	192.168.169.0/24	192.168.20.0/24
Site B	1:1 NAT	192.168.169.0/24	192.168.30.0/24

16.2.4 IPSec VPN Commands: Remote Access

This table lists the commands for remote access IPSec VPN.

Table 57 IPSec VPN Commands: Remote Access

COMMAND	DESCRIPTION
`vrf main ike ike-policy-template <policy-name> allowed-users <user>`	Sets up to 256 user or user groups to associate the user or user group to the remote access IPSec VPN policy. `remote-auth-method` must be `eap-radius`.
`vrf main ike ike-policy-template <policy-name> allowed-users {radius-users | ldap-users | ad-users | ncas-users} <ext-group-name>`	Sets up to 256 external user accounts for RADIUS users (`radius-users`), AD users (`ad-users`), or Nebula Cloud Authentication Server users (`ncas-users`) when using IPSec VPN. (Sets up to 256 external user accounts for RADIUS users (`radius-users`), LDAP users (`ldap-users`), AD users (`ad-users`) or Nebula Cloud Authentication Server users (`ncas-users`) when using SSL VPN.) SecuExtender VPN clients must log in with an account of type **User** in the **Menu > Configuration > Get from Server** screen.

Table 57 IPSec VPN Commands: Remote Access (continued)

COMMAND	DESCRIPTION
`vrf main ike ike-policy-template <policy-name> ike-proposal 1 enc-alg {aes128-cbc| aes192-cbc| aes256-cbc| des-cbc| 3des-cbc}`	Sets the key size and encryption algorithm. `des-cbc` - a 56-bit key with the DES encryption algorithm `3des-cbc` - a 168-bit key with the DES encryption algorithm `aes128-cbc` - a 128-bit key with the AES encryption algorithm `aes192-cbc` - a 192-bit key with the AES encryption algorithm `aes256-cbc` - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
`vrf main ike ike-policy-template <policy-name> ike-proposal 1 auth-alg {hmac-md5| hmac-sha1| hmac-sha256| hmac-sha384| hmac-sha512}`	Sets the hash algorithm to use to authenticate packet data. SHA is generally considered stronger than MD5, but it is also slower. The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
`vrf main ike ike-policy-template <policy-name> ike-proposal 1 dh-group <dh-group>`	Sets the Diffie-Hellman key group you want to use to create encryption keys. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. The Zyxel Device and the remote IPSec router must use the same DH key group. Different operating systems may support different DH key groups. Check your operating system documentation. • For Windows VPN clients, Zyxel SecuExtender perpetual VPN clients versions 3.8.203.61.32 and earlier support DH1 to DH14. • For macOS VPN clients, Zyxel SecuExtender subscription VPN clients versions 1.2.0.7 and later support DH14 to DH21. For Windows VPN clients, Zyxel SecuExtender subscription VPN clients versions 5.6.80.007 and later support DH14 to DH21. • Windows versions 7, 10, 11 built-in IKEv2 VPN clients support DH2 by default. • macOS versions 14.2 and later built-in IKEv2 VPN clients support DH14 by default. • iOS versions 10.15 and later built-in IKEv2 VPN clients support DH14 by default.

Table 57 IPSec VPN Commands: Remote Access (continued)

COMMAND	DESCRIPTION
`vrf main ike ike-policy-template <policy-name> ike-proposal 1 {local-auth-method| remote-auth-method} {pre-shared-key| certificate| xauth| eap-md5| eap-mschapv2}`	Sets the authentication method for the remote IPSec router or the Zyxel Device. Sets the authentication method to `pre-shared-key` to use a password for authentication. Sets the authentication method to `certificate` to use one of the Zyxel Device certificates for authentication. Set the authentication method to `xauth` to use extended authentication. Sets the authentication method to `eap-md5` or `eap-mschapv2` to use the selected algorithm for authentication.
`vrf main ike ike-policy-template <policy-name> auth-server <1...2> {local | cloud-auth | <auth-server>}`	Sets the priority of the server for the Zyxel Device to use for authentication. • `local`: Zyxel Device • `cloud-auth`: Nebula Cloud Authentication • *auth-server*: A RADIUS or AD User Object.
`vrf main ike ike-policy-template <policy-name> aggressive {true| false}`	Set `aggressive` to `true` to use aggressive mode to establish an IKE SA faster. Set `aggressive` to `false` to use main mode to establish an IKE SA in a more secure way.
`vrf main ike ike-policy-template <policy-name> rekey-time <180...3000000>`	Sets the IKE SA life time to the specified value. The default value is 86400.
`vrf main ike vpn <policy-name> nat-traversal {ip-address| fqdn}`	If the Zyxel Device is behind a NAT router, enter the public IP address or the domain name that is configured and mapped to the Zyxel Device on the NAT router. Note: To allow a site-to-site VPN connection, the NAT router must have the following ports open: UDP 500, 4500.
`show ike ike-sa details`	Displays details of the IPSec SA (Security Association).

16.3 IPSec VPN Debug Commands

This table lists the IPSec VPN debug commands.

Table 58 IPSec VPN Debug Commands

COMMAND	DESCRIPTION
`cmd debug ipsec trace log debug-level <0...4>`	Generates IPSec debug logs. Enter `0-4` to set the debug-level. The higher the number, the more detailed the log is.
`cmd debug ipsec save log debug-level <0...4>`	Saves the IPSec debug logs to the Zyxel Device with the specified debug level. To see details on errors, download the log file using FTP from /tmp/ipsecvpn.log. Enter `0-4` to set the debug-level. The higher the number, the more detailed the log is.

Table 58 IPSec VPN Debug Commands

COMMAND	DESCRIPTION
`cmd ipsec connect child-sa <ipsec-policy> connectivity-check <ip-address>`	Checks connectivity from the child SA for the specified IPsec policy to the specified IP address. IKE SA (Internet Key Exchange Security Association) establishes the initial secure VPN connection. In IKEv2, a child SA is created within the established IKE SA to encrypt and authenticate data packets transmitted through the VPN tunnel.
`cmd ipsec connect ike-sa <ipsec-policy> connectivity-check <ip-address>`	Checks connectivity from the IKE SA for the specified IPsec policy to the specified IP address.

16.4 IPSec VPN Command Examples

These are some other example IPSec VPN usage commands.

```
usgflex200hp> edit running
usgflex200hp running config# cmd diagnostics ike enabled true
ike-diagnostics-set-active
    data
        result ok
        ..
    ..
usgflex200hp running config# cmd diagnostics ike config level 2
ike-diagnostics-config
    data
        result ok

usgflex200hp running config# cmd debug ipsec trace log
Mar 27 11:38:59 15[IKE] rechecking in 10s
Mar 27 11:39:09 11[IKE] rechecking in 10s
Mar 27 11:39:19 08[IKE] rechecking in 10s
Mar 27 11:39:29 14[IKE] rechecking in 10s
Mar 27 11:39:39 07[IKE] rechecking in 10s
Mar 27 11:39:49 09[IKE] rechecking in 10s
```

16.5 VPN Provisioning Commands

This table lists the commands for VPN provisioning.

Table 59 VPN configuration provisioning

COMMAND	DESCRIPTION
`vrf main provision port <1...65535>`	Specifies the port IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device. If you change the IPSec VPN port on the Zyxel Device, make sure to make the same change to the IPSec VPN client. Specify a port between 1024 to 65535 that is not in use by other services. Note: After changing the provisioning port, create a security policy to allow traffic to pass through the new port.
`del vrf main provision port`	Deletes the configured provision port and restores the default setting, which uses HTTPS (default: port 443) for remote access.
`vrf main provision provision-rule <rule-number> enabled {true | false}`	Enables the specified provision rule.
`del vrf main provision provision-rule <rule-number>`	Deletes the specified provision rule.
`vrf main provision provision-rule <rule-number> ike <ipsec-vpn-profile-name>`	Specifies the VPN profile for the specified provisioning rule.
`vrf main provision provision-rule <rule-number> allowed-user <user-profile>`	Specifies which user or user group is allowed to use the VPN rule and access the network.
`show config vrf main provision`	Displays the current VPN provisioning settings. Note: The provisioning port is using the default setting if no port number is displayed.

16.6 VPN Provisioning Command Examples

This example shows the default setting when the provisioning port is left unchanged.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# show config vrf main provision
provision
    provision-rule 0
        ike RemoteAccess
        enabled true
        allowed-user radius-users
        ..
```

This example shows how to change the default port and then specify a provision rule for retrieving VPN rule settings.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# vrf main provision port 12443
MyUSGFLEX500H running config# vrf main provision provision-rule 0 ike RemoteAccess
MyUSGFLEX500H running config# vrf main provision provision-rule 0 allowed-user
radius-users
MyUSGFLEX500H running config# vrf main provision provision-rule 0 allowed-user ad-
users
MyUSGFLEX500H running config# vrf main provision provision-rule 0 enabled true
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# show config vrf main provision
provision
    port 12443
    provision-rule 0
        ike RemoteAccess
        enabled true
        allowed-user radius-users
        allowed-user ad-users
        ..
    ..
```

CHAPTER 17
SSL VPN

17.1 SSL Access Policy

An SSL access policy allows the Zyxel Device to perform the following tasks:

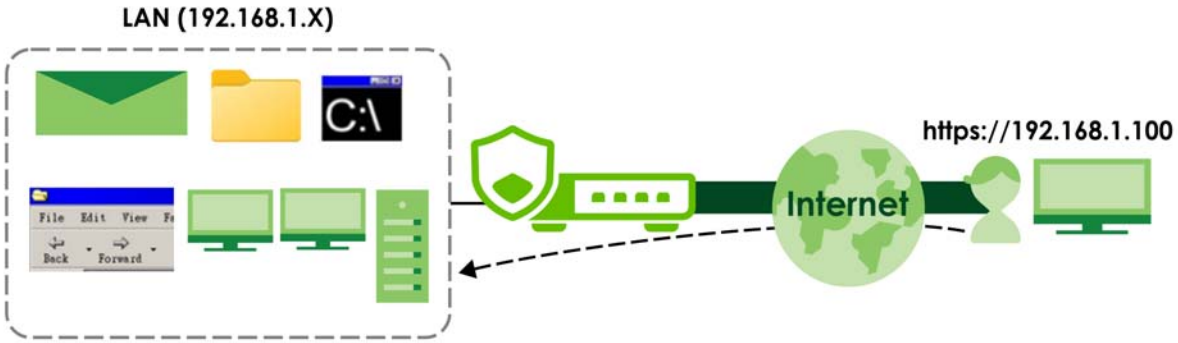
- Limit user access to specific applications or files on the network
- Allow user access to specific networks
- Assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

17.1.1 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

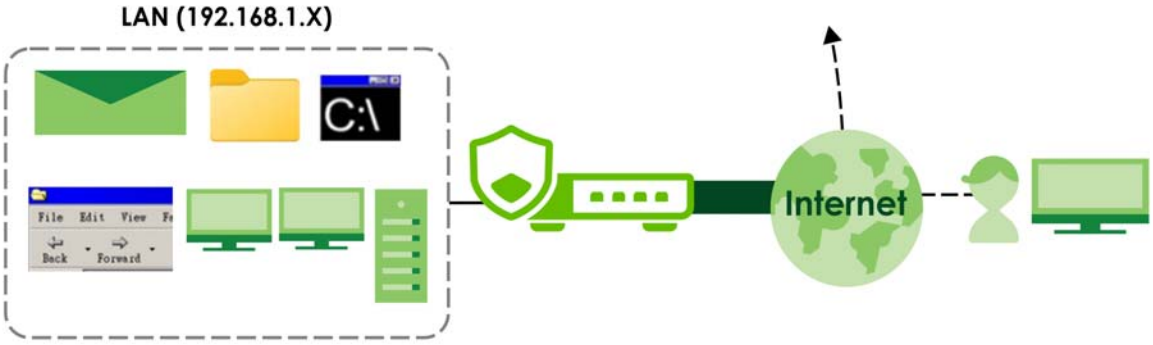
Figure 84 Network Access Mode: Full Tunnel Mode



Split Tunnel Mode

In split tunnel mode, only the traffic going to the networks behind the Zyxel Device is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device and is not encrypted.

Figure 85 Network Access Mode: Split Tunnel Mode



SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the Zyxel Device automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 60 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Sets the user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Sets an SSL application object for specifying the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Sets an address object to define a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Sets address objects for the IP addresses of the DNS and WINS servers that the Zyxel Device sends to the VPN connection users.
VPN Network	Address	Sets an address object for the network segment users are allowed to access through a VPN connection.

Please note that you cannot delete an object that is referenced by other settings.

17.2 SSL VPN Commands

The following table describes the values required for some SSL VPN commands. Other values are discussed with the corresponding commands.

Table 61 Input Values for SSL VPN Commands

LABEL	DESCRIPTION
user-account	The name of a user or 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.

17.2.1 SSL VPN Commands

This table lists the commands for SSL VPN. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 62 SSL VPN Commands

COMMAND	DESCRIPTION
`vrf main sslvpn-server enabled {true| false}`	Enables the SSL VPN policy.
`vrf main sslvpn-server bind-interface <interface>`	Sets the interface or incoming traffic to the Zyxel Device.
`vrf main sslvpn-server listen-port <1...65535>`	Sets the SSL VPN server port of the Zyxel Device for full tunnel mode SLL VPN access. Leave this field to default settings unless it conflicts with another interface.
`vrf main sslvpn-server proto {tcp| udp}`	Sets the SSL VPN server port to use TCP or UDP for communication.
`vrf main sslvpn-server server-subnet <ipv4_cidr>`	Sets IP address pool that is used to assign IP addresses to the VPN clients. Enter an IPv4 address in CIDR format, for example, 10.8.0.0/24.
`vrf main sslvpn-server {keepalive-interval| keepalive-timeout} <1...65535>`	`keepalive-interval`: Sets the interval between each keep alive message sent by the Zyxel Device. The default value is 10. `keepalive-timeout`: Sets the maximum time the Zyxel Device waits to receive a keep alive message from the remote SSL VPN router before it declares that the remote SSL VPN router is dead. The default value is 120. The interval should be less than the wait time.
`vrf main sslvpn-server auth {rsa-sha224| rsa-sha256| rsa-sha384| rsa-sha512}`	Sets the authentication algorithm used to authenticate SSL VPN clients. `rsa-sha224` is less secure but more compatible with different clients and applications. `rsa-sha512` is more secure but less compatible.
`vrf main sslvpn-server cipher {aes-128-cbc| aes-192-cbc| aes-256-cbc}`	Sets the encryption algorithm used to encrypt SSL VPN clients.
`vrf main sslvpn-server auth-server <1...2> <auth-server>`	Sets a specified RADIUS server for the Zyxel Device to use for authentication.
`vrf main sslvpn-server full-tunnel {true| false}`	Enables `full-tunnel` to encrypt all traffic through the VPN.
`vrf main sslvpn-server full-tunnel-through-wan {true | false}`	Enables `full-tunnel-through-wan` to allow traffic encrypted by the Zyxel Device from the remote client to the Internet by changing the (private) source IP addresses of VPN clients to the Zyxel Device WAN interface's public IP address for traffic going to the Internet. If you disable `full-tunnel-through-wan`, then SSL VPN clients can reach internal LAN subnets, but not the Internet, unless you create an outbound NAT rule for the SSL VPN pool.
`vrf main sslvpn-server dns-servers {ZyWALL| ipv4}`	Specifies the IP address of the DNS server whose information the Zyxel Device sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses. `ZyWALL`: the VPN clients use the IP address of the interface you specified and the Zyxel Device works as a DNS relay. `ipv4`: enter a static IPv4 address.

Table 62 SSL VPN Commands (continued)

COMMAND	DESCRIPTION
`vrf main sslvpn-server split-tunnel <ipv4_cidr>`	Enables `split-tunnel` to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation, for example, 10.8.0.0/24. Traffic going to the Internet from this IP address is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device is not encrypted.
`vrf main sslvpn-server allowed-user <user-account>`	Specifies a user or user group to associate the user or user group to the SSL VPN policy.
`vrf main sslvpn-server tls-version-min {tls-v1.2 | tls-v1.3}`	Sets the minimum TLS version required for this SSL access policy. The Zyxel Device requires minimum TLS 1.2 to block insecure protocols (like TLS 1.0/1.1) that have known vulnerabilities. TLS 1.3 provides stronger cipher suites and more secure key exchange methods than earlier versions. TLS connections using a version lower than the one selected here will be blocked.
`vrf main sslvpn-server dev-tunnel {tun | tap}`	Sets the SSL VPN tunnel mode. • (Recommended) Use `tun` to create a virtual IP interface, to route IP packets only. Each VPN client gets an IP address from the SSL VPN pool. • (Not recommended) Use `tap` to bridge SSL VPN clients directly into the LAN. This mode includes an Ethernet header (such as MAC address) and forwards all broadcast packets resulting in slower speeds. This requires corresponding SSL VPN client configuration, so is not recommended.
`vrf main sslvpn-server compress {none | lz4-v2 | lzo}`	Sets the data-compression algorithms used inside the encrypted tunnel to reduce the size of traffic before it is sent. Select `none` unless bandwidth is very constrained. If you need compression, select `lzo` for both SecuExtender and OpenVPN clients and `lz4-v2` if you only have SecuExtender clients.
`vrf main sslvpn-server provision {true | false}`	Sets how SSL VPN clients get or create configurations. Enable (`true`) to allow SSL VPN clients to use the SSL VPN Configuration file. Disable (`false`) to require SSL VPN clients to configure SecuExtender or their OpenVPN client manually.
`vrf main sslvpn-server auth-server <1..2> <AAA-server-object-name>`	Sets the priority (1 or 2) of the specified AAA server.
`vrf main sslvpn-server extended-config <client-profile-number> address-subnet <ipv4_cidr>`	Sets a range or specific IP addresses to assign to clients in the profile. `client-profile-number`: The number of the client profile. `IPv4_cidr`: An IPv4 address in CIDR notation. For example, 192.168.1.0/24 for a range of IP addresses, or 192.168.1.1/32 for a specific IP address. The specified IP addresses should not overlap with IP addresses on the Zyxel Device's local networks and the SSL user's network. The specified IP addresses must be within the range configured for general clients using `vrf main sslvpn-server server-subnet <ipv4_cidr>` command.
`vrf main sslvpn-server extended-config <client-profile-number> adapter-domain-suffix <dns_suffix>`	Sets the DNS suffix appended to hostnames entered by clients in the profile to form a complete domain name. For example, if a user enters only a hostname (fileserver), the DNS suffix (example.com) is appended to form fileserver.example.com.

Table 62 SSL VPN Commands (continued)

COMMAND	DESCRIPTION
`vrf main sslvpn-server extended-config <client-profile-number> full-tunnel {true | false}`	Encrypts all traffic through the VPN for clients in the profile. See Full Tunnel Mode for details.
`vrf main sslvpn-server extended-config <client-profile-number> full-tunnel-through-wan {true | false}`	Enables `full-tunnel-through-wan` to allow traffic encrypted by the Zyxel Device from clients in the profile to the Internet. The client's private IP address is translated to the Zyxel Device's WAN interface public IP address for traffic going to the Internet. The Internet cannot route privately-assigned IP addresses, so the Zyxel Device must perform Source NAT (SNAT) to convert them to the public IP address on its WAN interface. For example, if a client in the profile has a privately assigned IP address such as 192.168.1.88, it is automatically translated to the Zyxel Device's WAN interface IP address, such as 1.1.1.1, when going to the Internet. Note: If you disable `full-tunnel-through-wan`, clients in the profile can access internal LAN subnets but not the Internet, unless you create an outbound NAT rule for the SSL VPN pool. See Chapter 11 on page 110 for details.
`vrf main sslvpn-server extended-config <client-profile-number> split-tunnel <ipv4_cidr>`	Enables `split-tunnel` and sets an IPv4 address to only encrypt traffic going to the networks behind the Zyxel Device for clients in the profile. Traffic going to the Internet from the clients in the profile does not go through the Zyxel Device is not encrypted. `IPv4_cidr`: An IPv4 address in CIDR notation. For example, 192.168.1.0/24 for a range of IP addresses, or 192.168.1.1/32 for a specific IP address.
`vrf main sslvpn-server extended-config <client-profile-number> dns-servers {ZyWALL | <ipv4>}`	Specifies the DNS server whose information the Zyxel Device sends to clients in the profile. This allows them to access devices on the local network using domain names instead of IP addresses. `ZyWALL`: Clients use the IP address of the interface you specified and the Zyxel Device works as a DNS relay. `ipv4`: Enter a static IPv4 address. Specifies up to two DNS servers. Clients use the second DNS server when the first DNS server is not reachable. If no DNS server specified for the profile, clients in the profile use the general setting configured with the `vrf main sslvpn-server dns-servers {ZyWALL|<ipv4>}` command.
`vrf main sslvpn-server extended-config <client-profile-number> user-list <user-account>`	Specifies a user or user group to be associated with the SSL VPN policy of the profile.

Table 62 SSL VPN Commands (continued)

COMMAND	DESCRIPTION
`show config vrf main sslvpn-server`	Displays the current SSL VPN configuration.
`show state certManager sslvpn-certificate <server.crt | sslvpn_ca.crt | client.crt>`	Displays the runtime (state) information of a specific certificate used by SSL VPN on the Zyxel Device. server.crt: Displays details of the SSL VPN server certificate, such as issuer, subject, validity period, key algorithm. sslvpn_ca.crt: Displays details of the CA certificate used by SSL VPN, such as issuer, subject, validity period, key algorithm. client.crt: Displays details of the client certificate information, such as issuer, subject, validity period, key algorithm.

17.2.2 Show Certificate Command Example

These commands display the runtime (state) information of a specific certificate used by SSL VPN on the Zyxel Device.

```
usgflex500h> show state certManager sslvpn-certificate server.crt
sslvpn-certificate server.crt
    ref_count 0
    issuer CN=SSLVPN_CA_D8ECE56094FE
    subject CN=SSLVPN_SERVER_D8ECE56094FE
    validity-not-before "Dec  3 06:23:02 2025 GMT"
    validity-not-after "Dec  1 06:23:02 2035 GMT"
    key-algorithm sha256WithRSAEncryption
    ..

show state certManager sslvpn-certificate sslvpn_ca.crt
sslvpn-certificate sslvpn_ca.crt
    ref_count 0
    issuer CN=SSLVPN_CA_D8ECE56094FE
    subject CN=SSLVPN_CA_D8ECE56094FE
    validity-not-before "Dec  3 06:23:00 2025 GMT"
    validity-not-after "Dec  1 06:23:00 2035 GMT"
    key-algorithm sha256WithRSAEncryption

show state certManager sslvpn-certificate client.crt
sslvpn-certificate client.crt
    ref_count 0
    issuer CN=SSLVPN_CA_D8ECE56094FE
    subject CN=SSLVPN_CLIENT_D8ECE56094FE
    validity-not-before "Dec  3 06:23:02 2025 GMT"
    validity-not-after "Dec  1 06:23:02 2035 GMT"
    key-algorithm sha256WithRSAEncryption
```

CHAPTER 18 Tailscale

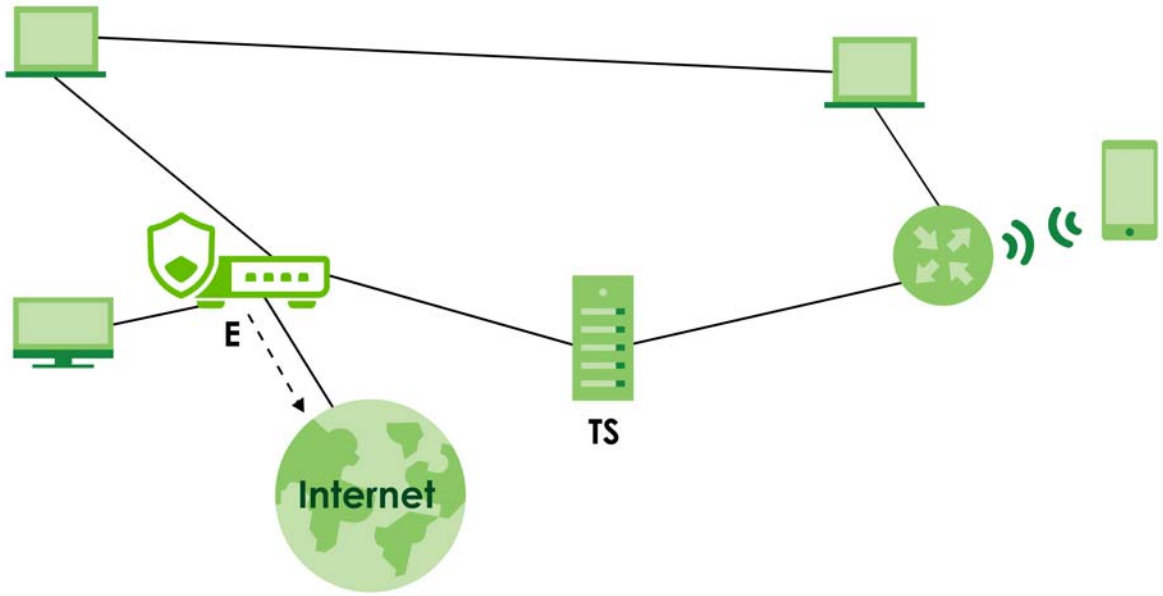
18.1 Overview

The Zyxel Device supports Tailscale, a site-to-site mesh VPN (Virtual Private Network) service that connects client devices (computer, smartphone, router, firewall) across different networks.

By default, Tailscale only routes traffic between client devices running Tailscale and does not protect public Internet traffic. However, there may be times when you want to route traffic from the Tailscale VPN to the public Internet, such as when you need access to an online service only available in another country.

In the following figure, the Tailscale server (**TS**) creates a mesh network, allowing each client device to connect directly with others, resulting in lower latency. The Zyxel Device act as the exit node (**E**) to route the VPN traffic to the public Internet.

Figure 86 Tailscale Example Topology



18.1.1 Tailscale Commands

This table lists the commands for Tailscale. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 63 Tailscale Commands

COMMAND	DESCRIPTION
`vrf main tailscale enabled {true | false}`	Sets Tailscale to run on the Zyxel Device so that VPN clients with Tailscale software can establish a VPN connection.
`vrf main tailscale auth-key-shadow < auth-key >`	Inputs the authentication key from the Tailscale admin console on the Zyxel Device
`vrf main tailscale port <num>`	Sets the port number for the Tailscale service. The default port number is 41641.
`vrf main tailscale exit-node {true | false}`	By default, Tailscale only routes VPN traffic between running client devices, but does not route VPN traffic to the Internet. Enable this if you want Tailscale to route the client devices' Internet traffic through the Zyxel Device. This must also be enabled on the Tailscale admin console.
`vrf main tailscale accept-subnet-routes`	Accepts advertised routes from other Tailscale VPN nodes. If you disable this, the Zyxel Device can only access peer VPN nodes, but not the advertised routes of those nodes.
`vrf main tailscale default-snat`	Sets the IP address of the outgoing interface on the Zyxel Device as the source IP address of the packets it sends out through its WAN trunk interfaces. The Zyxel Device automatically adds local source IP addresses for traffic it routes from internal interfaces to external interfaces.
`vrf main tailscale advertise-routes <addr-object>`	Select an address object of host or subnet type if you want to share them with other Tailscale VPN nodes. The selected subnets are open for access by the Tailscale network. Other client devices in the Tailscale network that accept advertised routes can access these resources through the Zyxel Device. This must also be configured on the Tailscale admin console.
`cmd tailscale status`	Displays Zyxel Device Tailscale status. • `active`: The VPN connection is established and data is being transmitted. • `idle`: The VPN connection is established and ready to be used, but no data is being transmitted. • `-`: No data has ever been sent to or received from the Zyxel Device.
`cmd tailscale show auth-key`	Displays the plain-text authentication key.
`cmd tailscale ip`	Displays the IP address assigned to the Zyxel Device by the Tailscale server.
`cmd tailscale interface`	Displays the interface used on the Zyxel Device by the Tailscale server.
`cmd tailscale ping <hostname | ip-address>`	Pings a host name or IP address from the Zyxel Device through the Tailscale VPN.
`cmd tailscale netcheck`	Displays the status of the network connection to the Tailscale server when Tailscale is enabled.

CHAPTER 19
Bandwidth Management

19.1 Bandwidth Management Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

19.1.1 Bandwidth Management Type

The Zyxel Device supports **shared** bandwidth management. All users to which the rule is applied need to share the bandwidth configured in the rule.

19.2 Bandwidth Management Commands

The following table lists the `bwm` commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 64 BWM Commands

COMMAND	DESCRIPTION
`vrf main bwm enabled {true| false}`	Enables bandwidth management on the Zyxel Device.
`vrf main bwm rule <profile-name> enable {true| false}`	Enables the BWM policy profile.
`vrf main bwm rule <profile-name> user <user-name>`	Enter a user or user group object name of the rule.
`vrf main bwm rule <profile-name> description <description>`	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.
`vrf main bwm rule <profile-name> incoming <interface-name>`	Specifies the source interface of the traffic to which this policy applies.
`vrf main bwm rule <profile-name> outgoing <interface-name>`	Specifies the destination interface of the traffic to which this policy applies.
`vrf main bwm rule <profile-name> source <address-name>`	Sets a source address or address group, including geographic address, for whom this policy applies. Enter `any` if the policy is effective for every source.
`vrf main bwm rule <profile-name> destination <address-name>`	Sets a destination address or address group, including geographic address, for whom this policy applies. Enter `any` if the policy is effective for every destination.

Table 64 BWM Commands (continued)

COMMAND	DESCRIPTION
`vrf main bwm rule <profile-name> service <service-name>`	Sets a service or service group to identify the type of traffic to which this policy applies. `any` means all services.
`vrf main bwm rule <profile-name> application <application-name>`	Sets an application to identify the specific traffic to which this policy applies. If you enter `BitTorrent`, it includes the services listed below at the time of writing: • BitTorrent • BitTorrent_FileTransfer • BitTorrent_Application • BitTorrent_Bundle
`vrf main bwm rule <profile-name> logging to {no| log| log-alert}`	Sets whether to have the Zyxel Device generate a log (`log`), log and alert (`log-alert`) or neither (`no`) when any traffic matches this policy.
`vrf main bwm rule <profile-name> download <0...10000>`	Sets how much inbound bandwidth, in megabits per second, this policy allows the traffic to use when there are other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter `0` to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter `1-10000` to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
`vrf main bwm rule <profile-name> download-maximum <0...10000>`	Sets how much inbound bandwidth, in megabits per second, this policy allows the traffic to use when there are no other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter `0` to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter `1-10000` to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the inbound interface. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
`vrf main bwm rule <profile-name> upload <0...10000>`	Sets how much outbound bandwidth, in megabits per second, this policy allows the traffic to use when there are other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter `0` to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter `1-10000` to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

Table 64 BWM Commands (continued)

COMMAND	DESCRIPTION
`vrf main bwm rule <profile-name> upload-maximum <0...10000>`	Sets how much outbound bandwidth, in megabits per second, this policy allows the traffic to use when there are no other services or applications using the interface's bandwidth. Outbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter `0` to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter `1-10000` to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the inbound interface. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
`vrf main bwm rule <profile-name> priority <0...7>`	Enter a number between 0 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. 0 is for real-time traffic such as video, and 7 is for lowest priority traffic such as background traffic. Traffic with a higher priority is given bandwidth before traffic with a lower priority. When traffic with higher priority has reached the full bandwidth, the traffic with lower priority can use the remaining bandwidth. The Zyxel Device uses priority queuing scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the download and upload limits are both set to Unlimited.
`vrf main bwm rule <profile-name> type {shared | per-user | per-source-ip}`	Sets how bandwidth is shared. • `shared` shares all matched traffic in the bandwidth rule equally. • `per-user` lets each user that matches the rule use up to his/her configured bandwidth. • `per-source-ip` sets the maximum bandwidth for traffic from one source IP address object that may have up to 1,024 IP addresses.
`vrf main bwm rule <profile-name> schedule <schedule-object>`	Sets when the bandwidth rule applies. Create a one-time or recurring schedule object to apply the bandwidth rule only at a specific time.
`vrf main bwm rule <profile-name> vlan-cos enabled {true | false}`	Allows the Zyxel Device to tag outgoing traffic from the VLAN interface with the specified 802.1P priority. Receiving devices will prioritize the traffic according to this tag.
`vrf main bwm rule <profile-name> vlan-cos priority-code <0...7>`	Specifies the 802.1P priority code. This is a 3-bit field within an 802.1Q VLAN tag, used to indicate the priority of outgoing VLAN traffic. '0' is the lowest priority level and '7' is the highest. The priority configured here overrides any existing priority settings on the VLAN interface.
`show bwm-applications`	Shows the applications the Zyxel Device can apply the bandwidth management policy.
`show config vrf main bwm`	Shows configuration details for all the BWM policy profiles.

19.2.1 BWM Command Example

This command shows how to specify which source and destination interfaces to apply the BWM policy. The ‘CathyBWM’ policy applies to traffic coming into the Zyxel Device through the ‘CathyBridge’ interface and to traffic leaving the Zyxel Device through the ge4 interface.

```
usgflex500h> edit running
usgflex500h running config# vrf main bwm rule CathyBWM incoming CathyBridge
usgflex500h running config# vrf main bwm rule CathyBWM outgoing ge4
usgflex500h running config# show config vrf main bwm
bwm
    enabled true
    default_rule
        priority 7
        ..
    rule CathyBWM
        enabled true
        logging no
        user any
        incoming CathyBridge
        outgoing ge4
        source any
        destination any
        service any
        download 1000
        download-maximum 0
        upload 1000
        upload-maximum 0
        priority 4
        ..
    ..
```

CHAPTER 20
Application Patrol

20.1 Application Patrol 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).

Note: The Zyxel Device checks firewall rules before application patrol rules for traffic going through the Zyxel Device. To use a service, make sure both the firewall and application patrol allow the service's packets to go 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, by application, whether or not the Zyxel Device continues to route the connection.

The following sections list the application patrol commands.

20.2 Application Patrol General Commands

The following table describes the application patrol general commands.

Table 65 app Commands: Application Patrol

COMMAND	DESCRIPTION
`show app-patrol-{categories| applications| signature-version}`	`categories`: Displays all the category IDs, names and numbers of applications that belong to each category. `applications`: Displays all the application IDs and names. `signature-version`: Displays the application patrol signature version, signature number and released date.
`show config vrf main app-patrol rule`	Displays the settings of the application patrol rules you configured.
`cmd app-patrol-query {name| category} <app-name| category-id>`	Sets an application name to display all related applications. Sets an application category ID to display all applications that belong to the specified category.
`cmd app-patrol-statistics-flush`	Clears all application patrol statistics.

20.3 Application Patrol Commands

The following table describes the application patrol commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 66 app Commands: Application Patrol

COMMAND	DESCRIPTION
`vrf main app-patrol statistics enabled {true | false}`	Enables application patrol statistics gathering. The `false` command disables it.
`vrf main app-patrol rule <rule-name>`	Creates an application patrol rule with the specified name. You may use 1-30 alphanumeric characters and also underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`description <description>`	Write a description for the application patrol rule.
`allow-only-selected-apps enabled {true| false}`	Enables only applications specified in the application patrol rule to pass.
`allow-only-selected-apps reject-unrecognized-apps {true| false}`	Disallows applications specified in the application patrol rule to pass.
`allow-only-selected-apps log-rejected-apps {true | false}`	Generates a log (`true`) when applications specified in the application patrol rule are rejected.
`multiple-application <0...4294967295> enabled {true| false}`	Rule 1 is `multiple-application 0`. Rule order is important because application rules are applied sequentially.
`multiple-application <0...4294967295> logging {no| log| log-alert}`	Generates a log, log and alert or neither (`no`) when traffic matches the settings you configured in this profile.
`multiple-application <number> action {forward| drop| reject}`	Sets the action when traffic matches the settings you configured in this profile. Actions are: • `forward` - routes packets that matches these signatures. • `drop` - silently drops packets that matches these signatures without notification. • `reject` - drops packets that matches these signatures and sends notification.
`multiple-application <number> sid <sid>`	Enter an application ID to add it to the application patrol profile you are configuring.

20.4 Application Patrol Statistics

The following table describes the commands for displaying application patrol statistics.

Table 67 Commands for Application Patrol Statistics

COMMAND	DESCRIPTION
`show config vrf main app-patrol statistics enabled`	Displays if the application patrol statistics collection is enabled.
`show state vrf main app-patrol statistics top-entry usage entry {app-name| category| usage-byte| usage-percent}`	Queries the top five application patrol statistics by application names, categories, usage by bytes and usage by percent.

20.4.0.1 Application Patrol Command Examples

This command shows details of an application patrol rule created.

```
usgflex200hp> show config vrf main app-patrol rule
rule 1
    multiple-application 4294967295
        sid 15728640
        action drop
        logging log-alert
```

The example below shows you how to create and configure an application patrol rule.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main app-patrol rule config1
usgflex200hp running rule config1# multiple-application 1
usgflex200hp running multiple-application 1# sid 32964608
usgflex200hp running multiple-application 1# sid 15728640
usgflex200hp running multiple-application 1# action drop
usgflex200hp running multiple-application 1# logging log-alert
usgflex200hp running multiple-application 1# commit
Configuration committed.
```

CHAPTER 21
Anti-Malware

21.1 Anti-Malware Overview

Malware is short for malicious software, such as computer viruses, worms and spyware. The Zyxel Device anti-malware feature protects your connected network from malware by scanning traffic coming in from the WAN and going out from the WAN for malware signature matches.

The traffic scanned by the Zyxel Device may include HTTP traffic, FTP traffic and email with attachments. The traffic is scanned for signature patterns found in the Defend Center database.

Viruses, Worms, 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. Spyware infiltrates your device to secretly gather information, such as your network activity, passwords, bank details, and so on.

Types of Malware

The following table describes some of the common malware.

Table 68 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.

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 if the contents of a file have changed. At the time of writing, the MD5 (Message Digest 5) hash algorithm is supported.

Cloud Query

The Zyxel Device queries the **Defend Center** database by sending the file's hash value and receiving the scan results through the Defend Center.

21.2 Anti-Malware Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 69 Input Values for General Anti-Malware Commands

LABEL	DESCRIPTION
md5-pattern *file-pattern*	Use up to 80 single-byte characters to specify a file pattern. Single-byte characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) represents a single character wildcard. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. An asterisk (*) represents a multiple character wildcard. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip" would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. A * in the middle of a pattern has the Zyxel Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the Zyxel Device checks up to the first 80 characters of a file name.

21.2.1 General Anti-Malware Commands

The following table describes general anti-malware commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Note: You must register for the anti-malware service in order to use it.

Table 70 General Anti-Malware Commands

COMMAND	DESCRIPTION
`vrf main anti-malware enabled {true| false}`	Enable the anti-malware service. The anti-malware service depends on anti-malware service registration.
`vrf main anti-malware scan-mode express enabled {true| false}`	Enable or disable the anti-malware scan mode. Express mode is a scan mode in which Zyxel Device scans files that match the list of user-defined file types using cloud query.
`vrf main anti-malware file-size-limit <1...10>`	Sets the limit of the file size in megabyte (MB) the Zyxel Device anti-malware will scan. A file that exceeds the file size you set here will pass without been scanned by the Zyxel Device anti-malware.
`vrf main anti-malware cloud-query file-type`	Adds or removes a file type from the list of user-defined file types that cloud query will scan. Allowed values: 7z, AVI, BMP, BZ2, EXE, Flash, GIF, Gz, JPG, MOV, MP3, MPG, "MS Office", PDF, PNG, RAR, RM, RTF, TIFF, WAV, ZIP.

Table 70 General Anti-Malware Commands (continued)

COMMAND	DESCRIPTION
`vrf main anti-malware eicar-detection enabled {true| false}`	Turns detection of the EICAR test file on or off. 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 real malware. 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.
`vrf main anti-malware default-port enabled {true| false}`	Has the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 21, 25, 80, 110, 143, 443, 465, 990, 993, 995, 3128 and 8080. You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main anti-malware default-port {extra-port| exception-port}` ***port number***	`extra-port`: Adds a port to the default specified port list. `exception-port`: Removes a port from the default specified port list.
`show state vrf main anti-malware default-port-state`	Displays the ports the Zyxel Device will scan when you set `vrf main anti-malware default- port enabled` to `true`.
`vrf main anti-malware default-profile infected-action {none| destroy}`	Sets the action to take when the Zyxel Device detects a malware in a file. The file can be “destroyed” by overwriting a portion of the file with zeros before forwarding to the user.
`vrf main anti-malware default-profile logging {no| log| log-alert}`	Sets whether the Zyxel Device should create a log message and an optional alert if it finds a malware in a file.
`vrf main anti-malware statistics enabled {true| false}`	Has the Zyxel Device collect the anti-malware statistics.
`show config vrf main anti-malware {default-profile| statistics| eicar-detection| cloud-query| allow-list| block-list| default-port| enabled| scan-mode}`	Displays: • default profile, cloud query, scan mode, allow list and block list settings. • if EICAR detection, statistics collection, default port and anti-malware are enabled.

21.2.2 Allow and Block Lists

The following table describes the commands for configuring the allow list and block list. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 71 Commands for the Anti-Malware Allow/Block Lists

COMMAND	DESCRIPTION
`vrf main anti-malware allow-list enabled {true | false}`	Enable or disable the allow list. When activated, the Zyxel Device does not perform anti-malware checks on files that match any of the allow list file patterns.
`vrf main anti-malware allow-list {md5-hash <md5-pattern> | sha256-hash <sha256-pattern> | file-name-pattern <file-pattern>} enabled {true | false}`	Adds an MD5 hash pattern, SHA-256 hash pattern or file name pattern to the allow list if it did not already exist, and then activates or deactivates the pattern. A file name pattern listed in the allow list allows incoming files with names that match the pattern. Note: By default, the Zyxel Device calculates only the SHA-256 hash. Adding an MD5 hash will require additional processing, which will increase CPU usage and slow down system performance.
`vrf main anti-malware allow-list logging {no | log}`	Sets whether the Zyxel Device should create a log message when a packet matches the allow list file patterns.
`show config vrf main anti-malware allow list {md5-hash | sha256-hash | file-name-pattern | enabled | logging}`	Displays the anti-malware allow list settings.
`vrf main anti-malware block-list enabled {true | false}`	Enable or disable the block list. When activated, the Zyxel Device logs and deletes files with names that match any of the block list file patterns.
`anti-malware block-list {md5-hash <md5-pattern> | sha256-hash <sha256-pattern> | file-name-pattern <file-pattern>} enabled {true | false}`	Adds an MD5 hash pattern, SHA-256 hash pattern, or file pattern to the block list if it did not already exist, and then activates or deactivates the pattern. A file name pattern listed in the block list blocks incoming files with names that match the pattern. Note: By default, the Zyxel Device calculates only the SHA-256 hash. Adding an MD5 hash will require additional processing, which will increase CPU usage and slow down system performance.
`vrf main anti-malware block-list logging {no | log}`	Sets whether the Zyxel Device should create a log message when a packet matches the block list file patterns.
`show config vrf main anti-malware block list {md5-hash | sha256-hash | file-name-pattern | enabled | logging}`	Displays the anti-malware block list settings.

21.2.2.1 Allow List Example

This example shows how to enable the allow list and configure an active allow list entry.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware allow-list enabled true
usgflex200hp running config# vrf main anti-malware allow-list logging log
usgflex200hp running config# vrf main anti-malware allow-list md5-hash
BB1372E462191A9C955906A152C59E89
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# enabled true
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# save
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# exit
```

21.3 Anti-Malware Statistics

The following table describes the commands for collecting and displaying anti-malware statistics.

Table 72 Commands for Anti-Malware Statistics

COMMAND	DESCRIPTION
`show state vrf main anti-malware statistics summary malware-detected-count`	Displays the number of times the Zyxel Device detects malware that matches the signatures.
`show state vrf main anti-malware statistics event entry {timestamp| source-ip| destination-ip| hash| virus-name}`	Displays anti-malware statistics entries by time, destination IP address, source IP address, virus name or hash value.
`show state vrf main anti-malware statistics top-entry {virus-name| source-ip| destination-ip}`	Displays the top five anti-malware statistics entries by destination IP address, source IP address or virus name.
`cmd anti-malware-statistics-flush`	Clears the collected statistics.

21.3.1 Anti-Malware Statistics Example

This example shows how to collect and display anti-malware statistics.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware statistics enabled true
usgflex200hp running config# show config vrf main anti-malware statistics enabled
enabled true
usgflex200hp running config# show state vrf main anti-malware statistics summary
summary
malware-detected-count 0
```

21.4 Anti-Malware Debug Commands

The following table describes the commands for collecting and displaying anti-malware statistics.

Table 73 Debug Commands for Anti-Malware

COMMAND	DESCRIPTION
`cmd debug anti-malware cloud-query cache {enable | disable | flush}`	Enables or disables saving of results of anti-malware queries to the cloud on the Zyxel Device. Use flush to clear all previously saved anti-malware queries on the Zyxel Device. You may want to do this if there are false positive query results.
`cmd debug anti-malware local-loop-mode`	Displays anti-malware connection status from the Zyxel Device to the cloud query server.
`cmd debug anti-malware clean-log enabled {true | false}`	Enables or disables removing anti-malware logs saved on the Zyxel Device.

21.4.1 Anti-Malware Debug Commands Examples

This example shows some example anti-malware debug cloud query commands.

Figure 87 Debug Cloud Query Commands

```
usgflex500h> edit running
usgflex500h running config# cmd debug anti-malware cloud-query cache enable
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
 cmd debug anti-malware cloud-query cache disable
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
cmd debug anti-malware cloud-query cache flush
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
```

This example shows an example of the anti-malware debug local loop command.

Figure 88 Debug Local Loop Command

```
usgflex500h> edit running
usgflex500h running config# cmd debug anti-malware local-loop-mode
anti-malware-debug-cloud-query-am-local-loop-mode
    ok
        status "change local-loop-mode Ok.
"
        ..
```

This example shows an example of removing the anti-malware logs from the Zyxel Device.

Figure 89 Debug Remove Anti-Malware Logs Command

```
usgflex500h> edit running
usgflex500h running config#  cmd debug anti-malware clean-log enabled true
anti-malware-debug-cloud-query-clean-log
    ok
        status "change clean-log Ok.
"
        ..
```

CHAPTER 22
Reputation Filter

22.1 Overview

Use the **Reputation Filter** commands to configure settings for IP Reputation, DNS Threat Filter and URL Threat filtering.

IP Reputation

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

URL Threat Filter

URL filtering compares access to specific URLs against a database of blocked or allowed sites. Sites on the database are sorted into categories such as:

Anonymizers	Browser Exploits
Malicious Downloads	Malicious Sites
Phishing	Spam URLs
Spyware Adware Keyloggers	

DNS Threat Filter

DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). The Zyxel Device DNS Threat Filter will either drop the DNS query or reply to the user with a fake DNS response.

The following types of DNS queries are inspected by the Zyxel Device:
- Type "A" ...
- Type "AAAA" ...
- Type "NS" ...
- Type "MX" ...
- Type "CNAME" ...
- Type "PTR" ...
- Type "SOA" ...

The Zyxel Device replies with a DNS reply packet containing a fake IP address for type "A", and replies with a DNS reply packet with server failure code for remaining types.

22.2 IP Reputation Commands

The following table describes general IP reputation commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 74 IP Reputation Commands

COMMAND	DESCRIPTION
`vrf main ip-reputation allow-list enabled {true| false}`	Enables the IP reputation allow list to allow: • Incoming packets that come from the listed IPv4 addresses. • Outgoing packets that go to the listed IPv4 addresses.
`vrf main ip-reputation allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when: • Incoming packets come from the IPv4 addresses listed in the allow list. • Outgoing packets going to the IPv4 addresses listed in the allow list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main ip-reputation allow-list ip-list <`*`IPv4 address`*`> enabled {true| false} [description <`*`description`*`>]`	Adds the specified IPv4 address on the IP reputation allow list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24. A description is optional.
`vrf main ip-reputation block-list enabled {true| false}`	Enables the IP reputation allow list to block: • Incoming packets that come from the listed IPv4 addresses. • Outgoing packets that go to the listed IPv4 addresses.
`vrf main ip-reputation block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when: • Incoming packets come from the IPv4 addresses listed in the block list. • Outgoing packets going to the IPv4 addresses listed in the block list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main ip-reputation block-list ip-list <`*`IPv4 address`*`> enabled {true| false} [description <`*`description`*`>]`	Adds the specified IPv4 address on the IP reputation block list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24. A description is optional.
`vrf main ip-reputation enabled {true| false}`	Enables the IP reputation filtering service on the Zyxel Device. The `false` command disables the IP reputation filtering service.
`vrf main ip-reputation action {allow| block}`	Sets what action the Zyxel Device takes when a packet arrives from or goes to an IPv4 address with a bad reputation. `allow`: The Zyxel Device allows the packet to go through. `block`: The Zyxel Device denies the packet, and then sends a TCP RST to both the packet sender and receiver.
`vrf main ip-reputation system-protect enabled {true | false}`	Blocks packets with a bad reputation going to or arriving from the Zyxel Device.
`vrf main ip-reputation logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when: • Incoming packets come from an IPv4 address with a bad reputation. • Outgoing packets go to an IPv4 address with a bad reputation. The Zyxel Device will not generate a log if you use the `no` command.

Table 74 IP Reputation Commands (continued)

COMMAND	DESCRIPTION
`vrf main ip-reputation priority {high| medium| low}`	Sets the threshold threat level to which the Zyxel Device will take action (**high**, **medium**, and **low**). The threat level is determined by the IP reputation engine, which grades IPv4 addresses as follows: • **high**: An IPv4 address that scores 0 to 20 points. • **medium**: An IPv4 address that scores 0-60 points. • **low**: An IPv4 address that scores 0-80 points.
`vrf main ip-reputation outgoing-category botnets`	Sets the category of packets coming from the Internet or local networks that the Zyxel Device applies IP reputation filtering to.
`vrf main ip-reputation incoming-category {spam-sources| exploits| web-attacks| botnets| scanners| denial-of-service| negative-reputation| phishing| anonymous-proxies}`	Select the categories of packets coming from the Internet that the Zyxel Device applies IP reputation filtering to.
`show config vrf main ip-reputation enabled`	Displays if IP reputation is enabled.
`show config vrf main ip-reputation statistics enabled`	Displays if the collection of IP reputation statistics is enabled.
`show config vrf main ip-reputation statistics allow-list`	Displays the IP reputation allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.
`show state vrf main ip-reputation secureporter-allow-list`	Displays allow lists in the Zyxel Device that were created in SecuReporter.
`show config vrf main ip-reputation statistics block-list`	Displays the IP reputation block list settings
`show config vrf main ip-reputation action`	Displays the action the Zyxel Device takes when a packet arrives from an IPv4 address with a bad reputation.
`show config vrf main ip-reputation logging`	Displays the Zyxel Device log settings when: • Incoming packets come from an IPv4 address with a bad reputation. • Outgoing packets go to an IPv4 address with a bad reputation.

22.2.1 IP Reputation Statistics

The following table describes the commands for collecting and displaying IP reputation statistics.

Table 75 IP Reputation Statistics Commands

COMMAND	DESCRIPTION
`vrf main ip-reputation statistics enabled {true| false}`	Enables the collection of IP reputation statistics.
`show state vrf main ip-reputation summary`	Displays the collected IP reputation statistics.
`show state vrf main ip-reputation top-entry {malicious-ip| victim-host| category}`	Displays the top five IP reputation statistics entries by malicious IP, victim host or threat category.
`show state vrf main ip-reputation event entry {timestamp| malicious-ip| victim-host| threat-category| threat-level| count}`	Displays the IP reputation statistics entries by time, malicious IP victim host, threat category, threat level, or numbers of times threats are detected.
`show ip-reputation-signature-version`	Displays the IP Reputation signature version, signature number and release date

This is an example for IP reputation signatures.

```
usgflex200hp> show ip-reputation-signature-version
ip-reputation-signature-version
    ok
        current-version 1.0.0.20250921.0
        signature-number 439742
        released-date "2025-09-22 02:31:23"
        ..
    ..
```

22.3 DNS Threat Filter Commands

The following table describes general DNS Threat Filter commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 76 DNS Threat Filter Commands

COMMAND	DESCRIPTION
`vrf main dns-threat-filter enabled {true| false}`	Enables DNS threat filter on the Zyxel Device.
`vrf main dns-threat-filter allow-list fqdn-list <`*`FQDN`*`> enabled {true| false} [description <`*`description`*`>]`	Adds a specified Fully Qualified Domain Name (FQDN) to the DNS threat filter allow list. A description is optional.

Table 76 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`vrf main dns-threat-filter allow-list enabled {true| false}`	Enables the DNS threat filter allow list.
`vrf main dns-threat-filter allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when a packet contains an FQDN you configured in the allow list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main dns-threat-filter block-list fqdn-list <FQDN> enabled {true| false} [description <description>]`	Adds a specified Fully Qualified Domain Name (FQDN) to the DNS threat filter block list. A description is optional.
`vrf main dns-threat-filter block-list enabled {true| false}`	Enables the DNS threat filter block list.
`vrf main dns-threat-filter block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains an FQDN you configured in the block list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main dns-threat-filter default_profile action {redirect| pass}`	Sets what the Zyxel Device does when it detects a malicious DNS query packet. `pass`: Have the Zyxel Device allow the DNS query packet and not reply a DNS reply packet with a fake IP for it. `redirect`: Have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address. The default redirect IP is the IP address of the DNS Threat Filter server (dnsft.cloud.zyxel.com).
`vrf main dns-threat-filter default_profile logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when it detects a malicious DNS query packet. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main dns-threat-filter default_profile security-threat-category {anonymizers| malicious-sites| spyware-adware-keyloggers| phishing| spam-urls| browser-exploits| malicious-downloads}`	The Zyxel Device considers DNS queries that match the specified category to be malicious.
`vrf main dns-threat-filter redirect {default| custom-defined}`	Sets whether the Zyxel Device uses the default redirect settings or the custom defined redirect settings when there is a DNS query packet containing an FQDN with a bad reputation.
`vrf main dns-threat-filter custom-redirect-ip <IPv4 address>`	Sets the redirect IP address for malicious DNS queries to the specified IPv4 address.
`vrf main dns-threat-filter malform-detected-action {drop| pass}`	`drop`: Sets the Zyxel Device to drop a DNS query packet if the DNS query is invalid, or if the Zyxel Device cannot read the packet. A DNS query is invalid under any of the following conditions: • The number of entries in the DNS header question count field is 0 • An error occurs while parsing the domain name in the question field • The length of the domain name exceeds 255 characters `pass`: Sets the Zyxel Device to allow malformed DNS packets to pass through.

Table 76 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`vrf main dns-threat-filter malform-detected-logging {no| log}`	Has the Zyxel Device log a DNS query if the DNS query packet is not a standard DNS query, or if the device cannot read the packet. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main dns-threat-filter fake-response-ttl <300...86400>`	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. The default value is 3600. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
`vrf main dns-threat-filter dot-doh-detection enabled {true | false}`	Enables the Zyxel Device to detect if a client is using DNS over HTTPS (DoH) or DNS over TLS (DoT). If a client is using DNS over HTTPS (DoH) or DNS over TLS (DoT), then DNS-threat-filter and content-filter cannot inspect client DNS queries. To allow inspection of client DNS queries, you must block DoH and DoT services. DoT/DoH block signatures are included in the IP reputation signature pack.
`vrf main dns-threat-filter dot-doh-detection action {drop | pass}`	Sets the Zyxel Device to drop or pass a DNS query packet if a client is using DNS over HTTPS (DoH) or DNS over TLS (DoT).
`vrf main dns-threat-filter dot-doh-detection logging {log | no}`	Sets the Zyxel Device to create a log if a client is using DNS over HTTPS (DoH) or DNS over TLS (DoT).
`show config vrf main dns-threat-filer statistics enabled`	Displays if the collection of DNS threat filter statistics is enabled.
`show config vrf main dns-threat-filter allow-list`	Displays the DNS threat filter allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.
`show state vrf main dns-threat-filter secureporter-allow-list`	Displays allow lists in the Zyxel Device that were created in SecuReporter.
`show config vrf main dns-threat-filter block-list`	Displays the DNS threat filter block list settings.
`show config vrf main dns-threat-filter default_profile`	Displays the DSN threat filter default profile settings.
`show config vrf main dns-threat-filter enabled`	Displays if the DNS threat filter is enabled.
`show config vrf main dns-threat-filter redirect`	Displays the DNS threat filter redirect settings when there is a DNS query packet containing an FQDN with a bad reputation.
`show config vrf main dns-threat-filter malform-detected-action`	Displays the action set when the DNS query is invalid.
`show config vrf main dns-threat-filter malform-detected-logging`	Displays if the Zyxel Device logs a DNS query when the DNS query is invalid.

Table 76 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`show config vrf main dns-threat-filter fake-response-ttl`	Displays the time period in second you set for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN.
`show config vrf main dns-threat-filter dot-doh-detection`	Displays if DNS over HTTPS (DoH) or DNS over TLS (DoT) detection is enabled, the action to take, and if a log is created.

22.3.1 Redirecting DNS Query Packets Command Examples

You want to:

- Have the Zyxel Device rely with a DNS replay packet containing a custome-defined IP address when there is a DNS query packet containing an FQDN with a bad reputation.
- Have the Zyxel Device generate logs when there is a DNS query packet containing an FQDN with a bad reputation.

The DNS threat filter general settings use the parameters in the table below. General settings are for all traffic in the Zyxel Device network.

Table 77 DNS Threat General Settings Example

LOG	ACTION	CUSTOM-DEFINED REDIRECT IP ADDRESS
Log	redirect	10.10.10.10

Configure the DNS threat filter general settings as follows.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns-threat-filter default_profile action
redirect
usgflex200hp running config# vrf main dns-threat-filter default_profile logging
log
usgflex200hp running config# vrf main dns-threat-filter custom-redirect-ip
10.10.10.10
usgflex200hp running config# commit
Configuration committed.
```

22.3.2 DNS Threat Filter Statistics

The following table describes the commands for collecting and displaying DNS Threat Filter statistics.

Table 78 DNS Threat Filter Statistics Commands

COMMAND	DESCRIPTION
`vrf main dns-threat-filter statistics enabled {true|false}`	Enables the collection of DNS threat filter statistics.
`show state vrf main dns-threat-filter statistics summary`	Displays the collected DNS Threat Filter domain blocking statistics.

Table 78 DNS Threat Filter Statistics (continued)Commands

COMMAND	DESCRIPTION
`show state vrf main url-threat-filter statistics event entry {timestamp| threat-category| source-ip| dns-name}`	Queries the DNS threat filter statistics entries by time, FQDN, threat category, or source IP.
`show state vrf main dns-threat-filter statistics top-entry {category| dns-name| source-ip}`	Queries the top five DNS threat filter statistics entries by threat category, FQDN or source IP.

22.4 URL Threat Filter Commands

The following table describes general URL Threat Filter commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 79 URL Threat Filter Commands

COMMAND	DESCRIPTION
`vrf main url-threat-filter enabled {true| false}`	Enables URL threat filter on the Zyxel Device.
`vrf main url-threat-filter block redirect-url <`*`url`*`>`	Sets the URL of the web page to which you want to send users when their web access is blocked by the URL Threat 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;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
`vrf main url-threat-filter block message <`*`message`*`>`	Sets a message to be displayed when the URL Threat Filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,”). For example, “Web access is restricted. Please contact the network administrator”.
`vrf main url-threat-filter default_profile action {block| pass}`	Sets what action the Zyxel Device takes when a packet contains a malicious URL. `block`: The Zyxel Device blocks access to the web pages that match the categories you selected. `pass`: The Zyxel Device allows access to the web pages that match the categories you selected.
`vrf main url-threat-filter default_profile logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains a malicious URL. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main url-threat-filter default_profile security-threat-category {anonymizers| malicious-sites| spyware-adware-keyloggers| phishing| spam-urls| browser-exploits| malicious-downloads}`	The Zyxel Device blocks the specified web page categories.

Table 79 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`vrf main url-threat-filter allow-list enabled {true| false}`	Enables the URL threat filter allow list.
`vrf main url-threat-filter allow-list site-list <URL> enabled {true| false} description <description>`	Enables a web site in the URL threat filter allow list. An entry in the allow list is automatically allowed to pass through the Zyxel Device without doing URL Threat checking in the Zyxel Device.
`vrf main url-threat-filter allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when a packet contains a URL you configured in the allow list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main url-threat-filter allow-list site-list <URL> [description <description>]`	Adds a web site to the allow list using the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1...32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.com*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain. for example: zyxel.com. A description is optional.
`vrf main url-threat-filter block-list enabled {true| false}`	Enables the URL threat filter block list.
`vrf main url-threat-filter block-list site-list <URL> enabled {true| false} description <description>`	Enables a web site in the URL threat filter block list. An entry in the block list is automatically blocked without doing URL Threat checking in the Zyxel Device.
`vrf main url-threat-filter block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains a URL you configured in the block list. The Zyxel Device will not generate a log if you use the `no` command.
`vrf main url-threat-filter block-list site-list <URL> [description <description>]`	Adds a web site to the block list using the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1...32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain. for example: zyxel.com. A description is optional.
`vrf main url-threat-filter default-port enabled {true| false}`	Enables this to have the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 80, 443, 3128 and 8080. You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.

Table 79 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`vrf main url-threat-filter default-port {extra-port| exception-port} port number`	Uses the `extra-port` command to add a port to the default specified port list. Uses the `exception-port` command to remove a port from the default specified port list.
`show config vrf main url-threat-filter statistics enabled`	Displays if the collection of URL threat filter statistics is enabled.
`show config vrf main url-threat-filter block message`	Displays the message to be displayed when the URL Threat Filter blocks access to a web page.
`show config vrf main url-threat-filter default_profile`	Displays the URL threat filter default profile settings.
`show config vrf main url-threat-filter allow-list`	Displays the URL threat filter allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.
`show state vrf main url-threat-filter secureporter-allow-list`	Displays allow lists in the Zyxel Device that were created in SecuReporter.
`show config vrf main url-threat-filter block-list`	Displays the URL threat filter block list settings.
`show config vrf main url-threat-filter default-port enabled`	Displays if the default port is enabled.
`show config vrf main url-threat filter enabled`	Displays if URL threat filter is enabled.

22.4.1 URL Threat Filter Command Examples

Use these commands to block users in your network from accessing URLs that are categorized as browser exploits, malicious downloads, malicious sites, phishing or spam URLs. Use these commands if you also want to create a trusted list of URLs to make sure the Zyxel Device will allow incoming packets from these URLs and outgoing packets to these URLs even if they are categorized as URL threats.

The example uses the parameters given below.

Table 80 URL Threat Filter Example

ACTION	LOG	THREAT CATEGORIES	TRUST LIST
block	log-alert	• Browser Exploits • Malicious Downloads • Malicious Sites • Phishing • Spam URLs	• www.google.com • www.yahoo.com

1 Configure the URL threat filer settings as the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main url-threat-filter default_profile action
block
usgflex200hp running config# vrf main url-threat-filter default_profile logging
log-alert
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category browser-exploits
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category malicious-downloads
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category malicious-sites
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category phishing
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category spam-urls
```

2 Enable URL threat filter allow list.

```
usgflex200hp running config# vrf main url-threat-filter allow-list enabled true
```

3 Configure the URL threat filter allow list as the parameters given above.

```
usgflex200hp running config# vrf main url-threat-filter allow-list site-list
www.google.com
usgflex200hp running config# vrf main url-threat-filter allow-list site-list
www.yahoo.com
```

4 Save the current configuration to the Zyxel Device.

```
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# exit
```

22.4.2 URL Threat Filter Statistics

The following table describes the commands for collecting and displaying URL Threat Filter statistics.

Table 81 URL Threat Filter Statistics Commands

COMMAND	DESCRIPTION
`vrf main url-threat-filter statistics enabled {true|false}`	Enables the collection of URL threat filter statistics.
`show state vrf main url-threat-filter statistics summary`	Displays the collected URL Threat Filter IP blocking statistics.

Table 81 URL Threat Filter Statistics (continued)Commands

COMMAND	DESCRIPTION
`show state vrf main url-threat-filter statistics event entry {timestamp| url| threat-category| source-ip| destination-ip}`	Displays the URL threat filter statistics entries by time, URL, threat category, source IP or destination IP.
`show state vrf main url-threat-filter statistics top-entry {category| url| source-ip}`	Displays the top five URL threat filter statistics entries by threat category, URL or source IP.

22.4.3 URL Threat Filter Statistics Example

This example shows how to display URL Threat Filter statistics.

```
usgflex200hp> show state vrf main url-threat-filter statistics summary summary
    scanned-count 0
    hit-count 0
```

22.4.3.1 Security Threat Category Definitions

The following table contains a list of URL Threat Filter categories.

Table 82 Current Category Descriptions

CATEGORY	DESCRIPTION
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.
Browser Exploits	Sites that contain browser exploits. A browser exploit is any content that forces a web browser to perform operations that you do not explicitly intend.
Malicious Downloads	Sites that host files containing malicious content, such as viruses, spyware, rootkits, and ransomware.
Malicious Sites	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.
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.

Table 82 Current Category Descriptions (continued)

Spam URLs	Sites that have been promoted through spam techniques.
Spyware Adware Keyloggers	Sites that contain spyware, adware, or keyloggers. Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to companies. Companies use this information to analyze browsing habits, to gather marketing data, and to sell your information to others. Key logger programs try to capture and steal your passwords and watch and record everything you do on your computer. Adware programs typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.

22.5 External Block Lists

Use these commands to use block IP, FQDN or URL list entries stored in a file on a web server that supports HTTP or HTTPS and is reachable from the Zyxel Device. The Zyxel Device will bypass checking by this feature (if enabled) and block incoming and outgoing packets from the block list entries in this file. In this way, different Zyxel Devices can use the same block list.

The external block list file must be in text format (*.txt) with each entry separated by a new line.

Entries stored in a file on a web server allow the Zyxel Device to use longer lists than the Zyxel Device itself can contain and also allows an admin to use the same block lists across different Zyxel Devices.

List types are:

- IP Reputation
- URL / DNS Threat

22.5.1 IP Reputation External Block List

The following table describes the commands for enabling and configuring an external list of IP addresses to be blocked. The Zyxel Device blocks incoming and outgoing packets from the addresses in this file.

- The external block list file must be in text format (*.txt) with each entry separated by a new line.
- The external block list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a single IPv4 address, a IPv4 subnet in CIDR (Classless Inter-Domain Routing) format, or an IPv4 IP address range. These are examples:
  - 104.244.79.43
  - 188.68.0.255/31
  - 1.1.1.1-1.1.1.3
- The external block list file can contain a maximum of 50,000 entries.

- If the external block list file contains any invalid entries, the Zyxel Device will skip the invalid entries but still block the valid entries.

Table 83 Commands for IP Reputation Statistics

COMMAND	DESCRIPTION
`vrf main external-block-list ip-reputation enabled {true | false}`	Enables or disables the IP Reputation external block list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the block list file.
`vrf main external-block-list ip-reputation profile <profile-name> description <description> source <source>`	Creates an external block list profile. You must give the profile a name, a description consisting of 1–60 characters, and may include letters, numbers, and the following special characters: ()+/:=?!*#@$_%- The source must contain the exact file name, path and IP address of the server containing the external block list file.
`show state vrf main external-block-list ip-reputation all`	Shows all external block list profile details, such as name, count, last-update-time.
`del / vrf main external-block-list ip-reputation profile <profile name>`	Deletes the specified external block list profile.
`cmd external-block-list-update ip-reputation`	Sets the Zyxel Device to check for updates to the external block list immediately
`show state vrf main external-block-list-update-check ip-reputation`	Shows if the update check has completed. Check the log page for the update results.
`vrf main external-block-list ip-reputation auto-update enabled {true | false}`	Sets the Zyxel Device to automatically check for updates to the external block list.
`vrf main external-block-list ip-reputation auto-update schedule-type {every-n-hours | daily | weekly}`	Sets the hourly, daily or weekly frequency for Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
`vrf main external-block-list ip-reputation auto-update schedule every-n-hours <1..23>`	Sets the Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
`vrf main external-block-list ip-reputation auto-update schedule daily meridiem {am | pm} oclock <1..12>`	Sets the Zyxel Device to check for updates to the external block list once per day, at the specified hour. For example, the time format is the 24 hour clock, so '23' means 11 PM.
`vrf main external-block-list ip-reputation auto-update schedule weekly day {sun | mon | tue | wed | thu | fri | sat} meridiem {am | pm} oclock <1..12>`	Sets the Zyxel Device to check for updates to the external block list once per week, on the specified day at the specified hour.

22.5.2 URL /DNS Threat Filter External block List

The following table describes the commands for enabling and configuring an external database of URLs to

be blocked. The Zyxel Device blocks incoming and outgoing packets from the addresses in this file.

- The external block list file must be in text format (*.txt) with each entry separated by a new line.
- The external block list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a URL or domain name. These are examples:
  - https://www.zyxel.com/products_services/smb.shtml?t=s
  - www.zyxel.com
- The external block list file can contain a maximum of 50,000 entries.
- If the external block list file contains any invalid entries, the Zyxel Device will not use the file.

Table 84 Commands for URL / DNS Threat Filter External Block List

COMMAND	DESCRIPTION
`vrf main external-block-list dns-url-threat-filter enabled {true | false}`	Enables or disables the URL / DNS Threat external block list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the block list file.
`vrf main external-block-list dns-url-threat-filter profile <profile-name> description <description> source <source>`	Creates an external block list profile. You must give the profile a name, a description consisting of 1–60 characters, and may include letters, numbers, and the following special characters: ()+/:=?!*#@$_%- The source must contain the exact file name, path and IP address of the server containing the external block list file.
`show state vrf main external-block-list dns-url-threat-filter all`	Shows all external block list profile details, such as name, count, last-update-time.
`del / vrf main external-block-list dns-url-threat-filter profile <profile name>`	Deletes the specified external block list profile.
`cmd external-block-list-update dns-url-threat-filter`	Sets the Zyxel Device to check for updates to the external block list immediately
`show state vrf main external-block-list-update-check dns-url`	Shows if the update check has completed. Check the log page for the update results.
`vrf main external-block-list dns-url-threat-filter auto-update enabled {true | false}`	Sets the Zyxel Device to automatically check for updates to the external block list.
`vrf main external-block-list dns-url-threat-filter auto-update schedule-type {every-n-hours | daily | weekly}`	Sets the hourly, daily or weekly frequency for Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.

Table 84 Commands for URL / DNS Threat Filter External Block List (continued)

COMMAND	DESCRIPTION
`vrf main external-block-list dns-url-threat-filter auto-update schedule every-n-hours <1..23>`	Sets the Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
`vrf main external-block-list dns-url-threat-filter auto-update schedule daily meridiem {am | pm} oclock <1..12>`	Sets the Zyxel Device to check for updates to the external block list once per day, at the specified hour.

CHAPTER 23
IPS Commands

23.1 Overview

IPS (Intrusion Prevention System) protects against network-based intrusions, by detecting malicious or suspicious packets and responding instantaneously.
The IPS commands mostly mirror web configurator features. It is recommended you use the web configurator for IPS features such as searching for web signatures or editing an IPS profile. Some web configurator terms may differ from the command-line equivalent.

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.

Rate Based Signatures

While IPS signatures have the Zyxel Device respond instantaneously, **Rate Based Signatures** are IPS signatures that allow the Zyxel Device to just respond after a number of occurrences (**Count**) within a certain time period (**Period**) you set.

Figure 90 IPS Signatures Example

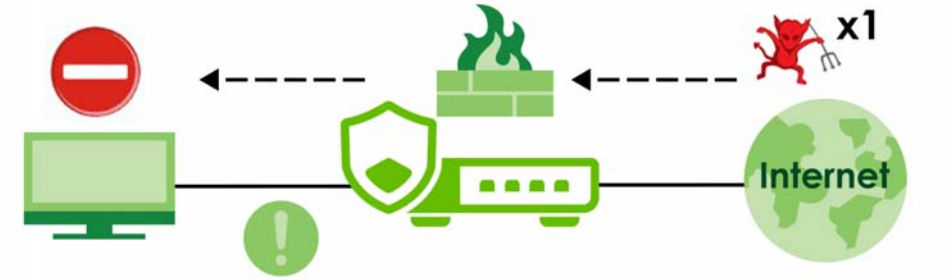
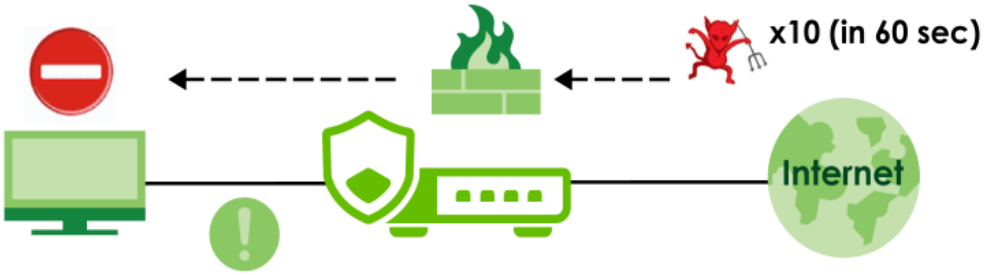


Figure 91 Rate Based Signatures Example



23.2 General IPS Commands

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

This table shows the general IPS commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 85 IPS General Commands

COMMAND	DESCRIPTION
`vrf main ips enabled {true| false}`	Enable IPS on the Zyxel Device. The `false` command disables IPS.
`vrf main ips all-traffic-scan-mode {prevention-mode| detection-mode}`	Sets what the Zyxel Device does when a stream of data matches a malicious signature. • `detection-mode`: The Zyxel Device only creates a log message. • `prevention-mode`: The Zyxel Device performs a user-specified action.
`vrf main ips system-protect enabled {true| false}`	Enables IDP system-protect to scan the packets that are destined for or sent out by the Zyxel Device for malicious or suspicious activities.
`vrf main ips system-protect bypass {tcp-port| udp-port} <1...65536>`	Sets a specified TCP or UDP port to bypass IPS system protection.
`show config vrf main ips {statistics| allow-list| default_profile| default_detect_only| enabled| all-traffic-scan-mode}`	Displays: • if statistics collection and IPS are enabled. • allow list, prevention mode profile and detection mode profile settings. • traffic scan mode.
`show ips-rate-based-signature {default_profile| default_detect_only}`	Displays rate based signatures settings.

23.2.0.1 General IPS Commands Example

This example shows how to activate signature-based IPS and set it to prevention mode on the Zyxel Device.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips enabled true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main ips enabled
enabled true
usgflex200hp running config# vrf main ips all-traffic-scan-mode prevention-mode
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main ips all-traffic-scan-mode
all-traffic-scan-mode prevention-mode
```

23.3 IPS Profile Commands

Use the commands listed below to configure the IPS profiles.

23.3.1 Prevention Mode Profile

Use these commands to configure the IPS profile when the Zyxel Device is in **Prevention Mode**.

Table 86 Prevention Mode Profile Commands

COMMAND	DESCRIPTION
`vrf main ips default_profile`	Enters the sub-command mode to configure the IPS prevention mode profile.
`signature <0...4294967295> enabled {true| false} logging {no| log| log-alert} action {none| drop| reject}`	Sets the action and log for the specified signature.
`signature <0...4294967295> counts <1...300> seconds <1...300> block-period <0...86400>`	`counts`: Sets the number of security events that need to occur within the defined seconds to trigger an action. `seconds`: Sets the length of time in seconds the event should occur from a client the counts number of times to trigger an action. For example, counts is set to 5, and seconds is set to 60. If the Zyxel Device detects 5 or more occurrences of malicious traffic in less than 60 seconds, then action is triggered. `block-period`: Sets the time period the attacker's IP will be blocked.

23.3.2 Detection Mode Profile

Use these commands to configure the IPS profile when the Zyxel Device is in **Detection Mode**.

Table 87 Detection Mode Profile Commands

COMMAND	DESCRIPTION
`vrf main ips default_detect_only`	Enters the sub-command mode to configure the IPS detection mode profile.
`signature <signature-id> enabled {true| false} logging {no| log| log-alert}`	Sets the log for the specified signature.

23.3.2.1 Profile Commands Example

The example below shows you how to:

- configure the prevention mode profile.

- view profile setting.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips default_profile
usgflex200hp running default_profile# signature 112012 enabled true logging log
action drop
usgflex200hp running default_profile# signature 112011 enabled true logging log
action reject
usgflex200hp running default_profile# signature 12010 enabled true logging no
action none
usgflex200hp running default_profile# commit
Configuration committed.
usgflex200hp running default_profile# exit
usgflex200hp> show config vrf main ips default_profile signature
signature 112012
    action drop
    enabled true
    logging log
    ..
signature 112011
    action reject
    enabled true
    logging log
    ..
signature 112010
    action drop
    enabled true
    logging log-alert
    ..
signature 112009
    action none
    enabled true
    logging log
    ..
signature 12010
    action none
    enabled true
    logging no
```

23.3.3 Signature Search

Use this command to search for signatures in the named profile.

Note: It is recommended you use the web configurator to search for signatures.

Table 88 Signature Search Command

COMMAND	DESCRIPTION
show ips-search-signature profile <*profile-name*> sid <*sid*> severity <*severity-mask*> platform <*platform-mask*> classtype <*classtype-mask*> service <*service-mask*> action <*action-mask*> enabled {true| false} logging {no| log| log-alert} name <*signature-name*>	Searches for signature(s) in a profile by the parameters specified. For example, [show ips-search-signature profile default_profile name worm sid 0 severity 0 platform 0 classtype 0 service 0 action 0] searches for all signatures in the default_profile containing the text “worm” within the signature name.

23.3.3.1 Search Parameter Tables

The following table displays the command line severity, platform and class type equivalent values. If you want to combine platforms in a search, then add their respective numbers together. For example, to search for signatures for Windows, Linux and Android then type “2060” as the platform parameter.

Table 89 Severity, Platform and Class Type Command Values

SEVERITY	PLATFORM	CLASS TYPE
0 = Any	0 = Any	0 = Any
1 = Very Low	4 = Windows	1 = Misc
2 = Low	8 = Linux	2 = Web-Attacks
4 = Medium	16 = FreeBSD	4 = Buffer-Overflow
8 = High	32 = Solaris	8 = Backdoor/Trojan
16 = Severe	128 = Other-Unix	16 = Access-Control
	256 = Network-Device	32 = P2P
	512 = Mac-OS	64 = IM
	1024 = iOS	128 = Virus-Worm
	2048 = Android	256 = BotNet
	4096 = Windows-Mobile	512 = Dos-DDos
	8192 = Symbian	1024 = Scan
	32768 = Others	2048 = File-Transfer
		4096 = Mail
		8192 = Stream-Media
		16384 = Tunnel
		32768 = ACL

The following table displays the command line service and action equivalent values. If you want to combine services in a search, then add their respective numbers together. For example, to search for signatures for DNS and FTP services, then type “640” as the service parameter.

Table 90 Service and Action Command Values

SERVICE	ACTION
0 = Any	0 = Any
1 = Misc	1 = None
2 = Exploit	2 = Drop
4 = Web	4 = Reject
8 = Web Client	
16 = Web ActiveX	
32 = Database	
64 = File Format	
128 = FTP	
256 = ICMP	
512 = DNS	
1024 = RDP	
2048 = DHCP	
4096 = SMTP	
8192 = SNMP	
16384 = POP3	
32768 = IMAP	
65536 = NETBIOS	
131072 = SCADA	
262144 = SIP	
DoS = 524288	

23.4 IPS Statistics

The following table describes the commands for collecting and displaying IPSP statistics. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 91 Commands for IPS Statistics

COMMAND	DESCRIPTION
`vrf main ips statistics enabled {true| false}`	Enables the collection of IPS statistics. The `false` command disables the collection of IPS statistics.
`show state vrf main ips statistics summary {scanned-session-count| packet-drop-count| packet-reset-count}`	Displays the collected statistics.

Table 91 Commands for IPS Statistics (continued)

COMMAND	DESCRIPTION
`show state vrf main ips statistics event entry {timestamp| count| souce-ip| destination-ip| sid| name| type| severity}`	Queries IPS statistics entries by time, numbers of times traffic matches the signatures, destination IP address, source IP address, signature ID, signature name or signature severity level.
`show state vrf main ips statistics top-entry {signature-name| source-ip| destination-ip}`	Queries the top five IPS statistics entries by destination IP address, source IP address or signature name.

23.4.1 IPS Statistics Example

This example shows how to display IPS statistics.

```
usgflex200hp> show state vrf main ips statistics summary
summary
    scanned-session-count 0
    packet-drop-count 0
    packet-reset-count 0
```

23.5 IPS Allow List

The Zyxel Device will exclude the incoming packets of the signature(s) in the IPS allow list. These packets won't be intercepted and will be passed through uninspected.

You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 92 Commands for IPS Allow List

COMMAND	DESCRIPTION
`vrf main ips allow-list sid <`*`0...4294967295`*`> logging {no| log}`	Adds the specified signature to the IPS allow list. Sets whether or not to generate a log when the incoming packets match the signatures you set in the allow list.

23.5.1 IPS Allow List Example

This example shows how to configure allow list settings.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips allow-list
usgflex200hp running allow-list# sid 12013 logging no
usgflex200hp running allow-list# sid 12014 logging log
usgfleusgflex200hp running allow-list# commit
Configuration committed.
```

CHAPTER 24
Content Filtering

24.1 Content Filtering Overview

The Zyxel Device content filtering includes HTTP(S) traffic scan and DNS domain scan, see Section 24.1.1 on page 200 and Section 24.1.2 on page 201 for more information.

The Zyxel Device content filtering allows you to block access to specific categories of web site content, and/or block access to specific web sites. You can create different content filtering policies for different addresses, users or groups and content filtering profiles. See Section 24.3.3 on page 209 for an example on how to use the Zyxel Device content filtering.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filtering profile.
- Use address and/or user/group objects to define to whose web access to apply the content filtering profile.
- Apply a content filtering 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.
- 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.

24.1.1 HTTP(S) Traffic Scan

The HTTP(S) Traffic Scan allows the Zyxel Device to block access to specific websites, by inspecting the URL or Server Name Indication (SNI). SNI lets a client indicate which host name it is attempting to connect to at the start of the handshaking process. This allows a server to present one of many certificates to the same IP address and TCP port number, so that different HTTPS websites can be served by the same IP address without requiring those sites to use the same certificate.

HTTP(S) Traffic Scanning Process

1 The Zyxel Device content filtering detects an HTTP(S) connection, and inspects the website sent.

2 If the website contains prohibited material, the HTTP(S) request is redirected to a block page.

Note: If the user's web browser is using encryption, then you must enable SSL Inspection for HTTP(S) Traffic Scan to work.

HTTP(S) Traffic Scanning 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.

HTTPS Domain Filter

HTTPS Domain Filter works with the content filtering 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.

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".

24.1.2 DNS Domain Scan

The DNS Domain Scan allows the Zyxel Device to block access to specific websites by inspecting DNS queries made by users on your network. If the website in the DNS query contains prohibited material, then the Zyxel Device replies to the DNS query with a IP address that points to the block page. Unlike the HTTP(S) Traffic Scan, the DNS Domain Scan works if the user is using TLS 1.3 with ESNI.

DNS Domain Scan Process

1 A user enters a URL into their web browser.

2 The user's computer sends a DNS query for the URL.

3 The DNS Domain Scan inspects the website in the DNS query packet.

4 If the website contains prohibited material, the DNS reply is redirected to a block page.

24.1.3 External Content Filtering Service

When you register for and enable the external Content 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.

External Content Filtering Server Lookup Procedure

The content filtering lookup process is described below.

Figure 92 Content Filtering 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 If the Zyxel Device has no record of the web site, it queries the external content filtering database.

4 The external content filtering 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 filtering profile. The web site's address and category are then stored in the Zyxel Device's content filtering cache.

24.2 Content Filtering Command Input Values

The following table explains the values you can input with the content-filter and dns-content-filter commands.

Table 93 Content Filtering Command Input Values

LABEL	DESCRIPTION
profile-name	The filtering profile defines how to filter web URLs or content. You may use 1-30 alphanumeric characters, and also underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
category	The name of a web category. For a list of category definitions, see Section 24.4 on page 211. {adult-topics | alcohol | anonymizing-utilities | art-culture-heritage | auctions-classifieds | blogs-wiki | business | chat | computing-internet | consumer-protection | content-server | controversial-opinions | cult-occult | dating-personals | dating-social-networking | digital-postcards | discrimination | drugs | education-reference | entertainment | extreme | fashion-beauty | finance-banking | for-kids | forum-bulletin-boards | gambling | gambling-related | game-cartoon-violence | games | general-news | government-military | gruesome-content | health | historical-revisionism | history | humor-comics | illegal-uk | incidental-nudity | information-security | information-security-new | instant-messaging | interactive-web-applications | internet-radio-tv | internet-services | job-search | major-global-religions | marketing-merchandising | media-downloads | media-sharing | messaging | mobile-phone | moderated | motor-vehicles | non-profit-advocacy-ngo | nudity | online-shopping | p2p-file-sharing | parked-domain | personal-network-storage | personal-pages | pharmacy | politics-opinion | pornography | portal-sites | potential-criminal-activities | potential-hacking-computer-crime | potential-illegal-software | private-ip-addresses | profanity | professional-networking | provocative-attire | public-information | pups | real-estate | recreation-hobbies | religion-ideology | remote-access | reserved | residential-ip-addresses | resource-sharing | restaurants | school-cheating-information | search-engines | sexual-materials | shareware-freeware | social-networking | software-hardware | sports | stock-trading | streaming-media | technical-business-forums | technical-information | text-spoken-only | text-translators | tobacco | travel | usenet-news | violence | visual-search-engine | weapons | web-ads | web-mail | web-meetings | web-phone| unrated}
trust-hosts	The IP address or domain name of a trusted web site. Use a host name such as www.good-site.com. Do not use 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”, etc. Use up to 63 case-insensitive characters (0-9a-z-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23.

Table 93 Content Filtering Command Input Values (continued)

LABEL	DESCRIPTION
forbid-hosts	The IP address or domain name of a forbidden web site. Use a host name such as www.bad-site.com into this text field. Do not use 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", etc. Use up to 63 case-insensitive alphanumeric characters (0-9a-zA-Z). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23.
keyword	A keyword or a numerical IP address to search URLs for and block access to if they contain it. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in double quotes. For example enter "Bad_Site" to block access to any web page that includes the exact phrase "Bad_Site". This does not block access to web pages that only include part of the phrase (such as "Bad" in this example).
message	The message to display when a web site is blocked. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in quotes. For example, "Web access is restricted. Please contact the network administrator."
redirect-url	The URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message. Use "http://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes. For example, "http://192.168.1.17/blocked access".

24.3 Content Filtering Commands

The following table lists the commands that you can use for content filtering configuration, such as creating a denial of access message or specifying a redirect URL. Use the `edit running` command to

enter the configuration mode to be able to use these commands. See Table 93 on page 203 for details about the values you can input with these commands.

Table 94 Content Filtering General Commands

COMMAND	DESCRIPTION
`vrf main content-filter https-domain-filter enabled {true| false]`	Enable HTTPS domain filter which lets the Zyxel Device take action on HTTPS web pages using the 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 Content Filter and then take appropriate action. The keyword match is for the domain name only. The `false` command disables the HTTPS domain filter.
`vrf main content-filter https-domain-filter block-page-enabled {true| false}`	Enable HTTPS domain filter block page to have the Zyxel Device display a warning page instead of a black page when an HTTPS connection is redirected.
`vrf main content-filter default-port enabled {true| false}`	Has the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 21, 25, 80, 110, 143, 443, 465, 990, 993, 995, 3128 and 8080. You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main content-filter default-port {exception-port| extra-port} <0...65535>`	`extra-port`: Adds a port to the default specified port list. `exception-port`: Removes a port from the default specified port list.
`vrf main content-filter block redirect-url <redirect-url>`	Sets the URL of the web page to which to send users when their web access is blocked by the Content Filter.
`vrf main content-filter block message <message>`	Sets the message to display when the Content Filter blocks access to a web page.
`vrf main content-filter offline action {pass| block}`	Sets the action for attempted access to web pages if the external web filtering database is unavailable.
`vrf main content-filter offline logging {no| log}`	Sets whether to generate logs for attempted access to web pages if the external web filtering database is unavailable.
`vrf main content-filter dns-scan enabled {true| false}`	Lets the Zyxel Device inspect DNS queries made by users on your network.
`vrf main content-filter dns-scan custom-redirect-ip <IPv4 address>`	Sets the redirect IP address for prohibited DNS queries to the specified IPv4 address. The default redirect IP address is the IP address of the DNS domain scan server (dnsft.cloud.zyxel.com).
`vrf main content-filter dns-scan fake-response-ttl <300...86400>`	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. The default value is 3600. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
`vrf main content-filter dns-scan redirect {default| custom-defined}`	Sets whether the Zyxel Device uses the default redirect settings or the custom defined redirect settings when users on your network try to access blocked FQDNs.

Table 94 Content Filtering General Commands (continued)

COMMAND	DESCRIPTION
`show config vrf main content-filter https-domain-filter {enabled| block-page-enabled}`	Displays if the HTTPS domain filter and the HTTPS domain filter blocked page is enabled.
`show config vrf main content-filter default-port {enabled| exception-port| extra-port}`	Displays: • if the default port is enabled. • exception port and extra port settings.
`show config vrf main content-filter statistics enabled`	Displays if the content filter statistics collection is enabled.
`show config vrf main content-filter blocked {redirect-url| message}`	Displays the redirect URL and blocked message settings when the Content Filter blocks access to a web page.
`show config vrf main content-filter offline {action| logging}`	Displays the action and log settings when there are attempts to access web pages if the external web filtering database is unavailable.
`show config vrf main content-filter dns-scan {enabled| redirect| custom-redirect-ip| fake-response-ttl}`	Displays the DNS domain scan settings.
`cmd content-filter-cache-flush`	Clears the history of the websites the Zyxel Device content filter has scanned. Use this command when you think the content filter categories stored on the Zyxel Device is not up to date.
`cmd content-filter-statistic-flush`	Clears the collected statistics.

24.3.1 Content Filtering Profile Commands

The following table lists the commands that you can use to configure a content filtering profile. Use the `edit running` command to enter the configuration mode to be able to use these commands. See Table 93 on page 203 for details about the values you can input with these commands.

Table 95 Content Filtering Profile Commands Summary

COMMAND	DESCRIPTION
`show config vrf main content-filter profile`	Displays the content filtering profiles settings.
`vrf main content-filter profile <profile-name>`	Creates a content filtering profile and enters the sub-command mode.
`sslv3 drop {true | false}`	Blocks HTTPS web sites using SSL V3 or a previous version.
`sslv3 logging {no | log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access an HTTPS web site that is using SSL V3 or a previous version. The Zyxel Device will not generate a log if you use the `no` command.
`match action {pass | block}`	Sets the action for attempted access to web sites that match the profile's selected managed categories.

Table 95 Content Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`match logging {no | log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site that matches the profile's selected managed categories. The Zyxel Device will not generate a log if you use the `no` command.
`allow-list logging {no | log}`	Sets whether the Zyxel Device generates a log when the user on your network accesses a web site listed in the allow list you configured. The Zyxel Device will not generate a log if you use the `no` command.
`allow-list site-list <web-sites>`	Adds a trusted web site entry in the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1..32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain
`block-list logging {no | log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site listed in the block list you configured. The Zyxel Device will not generate a log if you use the `no` command.
`block-list site-list <web-sites>`	Adds a forbidden web site entry in the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1..32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain
`url-keyword logging {no | log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site with an URL that contains certain keywords in the domain name or IP address. The Zyxel Device will not generate a log if you use the `no` command.

Table 95 Content Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`url-keyword keyword-list <keyword>`	Adds a forbidden keyword or IP address to the profile's list. Please note the Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking. When the Zyxel Device inspects the URL queries made by users on your network, the Zyxel Device will check both the URL domain name and file path for keywords that are blocked. When the Zyxel Device inspects the DNS queries made by users on your network, the Zyxel Device will only check the URL domain name for keywords that are bocked, but not the file path.
`description <description>`	Sets a description for the content filtering profile to help identify the purpose of the profile.
`allow-only-enabled {true | false}`	Has the Zyxel Device only allow access to the web sites listed in the allow list configured individually for this profile using `content-filter profile <profile> allow-list site-list <web-site>`.
`log-allowed-traffic {true | false}`	Has the Zyxel Device generate logs for all allowed traffic.
`dns-safesearch-activate {true | false}`	Enforces safe search mode in the Yahoo, Google, MSN Live Bing, and Yandex search engines to prevent inappropriate or adult-oriented search results in these search engines.
`dns-safesearch-youtube-mode {strict | moderate}`	Sets the restriction level for YouTube search. • `strict` filters out many videos, including those with potentially harmful or adult content. This may be suitable for younger viewers. • `moderate` filters out potentially objectionable content, but allows access to more mature educational or informational content.
`category <category>`	Adds a managed category to the profile list. See Table 97 on page 211.
`cmd url-category-query search {URL | FQDN}`	Searches for a specific URL or FQDN in any profile using managed categories.
`show content-filter genai-application`	Displays the filtered AI websites in the genai-application managed category at the time of writing.

24.3.2 Content Filtering Statistics

The following table describes the commands for collecting and displaying content filtering statistics.

Table 96 Content Filtering Statistics Commands

COMMAND	DESCRIPTION
`vrf main content-filter statistics enabled {true| false}`	Enable the collection of content filtering statistics. The `false` command disables the collection of content filtering statistics.
`vrf main content-filter statistics summary`	Displays the collected Content Filter statistics.

Table 96 Content Filtering Statistics (continued)Commands

COMMAND	DESCRIPTION
`vrf main content-filter statistics blocked-event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays the traffic Content Filter has blocked by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics allowed-event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays the traffic Content Filter has allowed to pass by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays content filtering statistics entries by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics top-entry {blocked-source-ip| blocked-category| blocked-url| allowed-source-ip| allowed-category| allowed-url}`	Displays the top five content filtering statistics entries by blocked source IP address, blocked category, blocked URL, allowed source IP address, allowed category and allowed URL.

24.3.3 Content Filtering Example

This is an example of using the Zyxel Device to block access to a specific network service. A company wants to prevent its employees from using Facebook during their time in the office, but still allows access to other web pages, such as Office 365, Google, Wikipedia... The company wants to make sure any traffic going from the LAN to the Internet cannot access Facebook whether the traffic goes through the Zyxel Device or not.

Figure 93 Content Filtering Example

Follow the steps below to block the Zyxel Device LAN users from accessing Facebook.

1 Create a content filtering profile named **facebook_block**.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main content-filter profile
facebook_block
```

2 You then enter sub-command mode for the **facebook_block** profile to configure the content filtering profile's list of forbidden keywords.

```
usgflex200hp running profile facebook_block#
```

3 Enter ***.facebook*.com** to block access to websites with URLs that contain **facebook**. Use asterisks (*) as a wildcard to match any string in trusted and forbidden websites. Exit sub-command mode.

```
usgflex200hp running profile facebook_block# url-keyword keyword-list
*.facebook*.com
usgflex200hp running profile facebook_block# commit
Configuration committed.
usgflex200hp running profile facebook_block# exit
```

4 To block traffic that goes through the Zyxel Device from the LAN to the Internet, you need to apply the content filtering profile **facebook_block** to the security policies **LAN1_Outgoing** and **LAN2_Outgoing**. Enter sub-command mode for configuring the security policy **LAN1_Outgoing**.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main secure-policy rule 1
usgflex200hp running rule 1#
```

5 Apply the content filter profile **facebook_block** to the security policies' content filtering profile. Set the log to **log by-profile** to generate a log for all traffic that matches criteria in the profile. Exit sub-command mode.

```
usgflex200hp running rule 1# content-filter-profile profile name
facebook_block enabled true log by-profile
usgflex200hp running rule 1# commit
Configuration committed.
```

6 Repeat step 7 and step 8 to apply the content filtering profile **facebook_block** to the security policy **LAN2_Outgoing**.

24.3.4 Content Filtering Statistics Example

This example shows how to display content filtering statistics.

```
usgflex200hp> show state vrf main content-filter statistics summary
summary
    total-inspected 0
    blocked 0
    passed 0
    allow-list-hit 0
    block-list-hit 0
    url-keyword-hit 0
    service-unavailable-passed 0
    service-unavailable-blocked 0
    sslv3-block-hit 0
```

24.4 Content Filtering Category Definitions

The following table listed the managed categories available.

Table 97 Managed Category Descriptions

CATEGORY	DESCRIPTION
Adult Topics	Web pages that contain content or themes that are generally considered unsuitable for children.
Alcohol	Web pages that mainly sell, promote, or advocate the use of alcohol, such as beer, wine, and liquor. This category also includes cocktail recipes and home-brewing instructions.
Anonymizing Utilities	Web pages that result in anonymous web browsing without the explicit intent to provide such a service. This category includes URL translators, web-page caching, and other utilities that might function as anonymizers, but without the express purpose of bypassing filtering software. This category does not include text translation.
Art Culture Heritage	Web pages that contain virtual art galleries, artist sites (including sculpture and photography), museums, ethnic customs, and country customs. This category does not include online photograph albums.
Auctions Classifieds	Web pages that provide online bidding and selling of items or services. This category includes web pages that focus on bidding and sales. This category does not include classified advertisements such as real estate postings, personal ads, or companies marketing their auctions.
Blogs/Wiki	Web pages containing dynamic content, which often changes because users can post or edit content at any time. This category covers the risks with dynamic content that might range from harmless to offensive.
Business	Web pages that provide business-related information, such as corporate overviews or business planning and strategies. This category also includes information, services, or products that help other businesses plan, manage, and market their enterprises, and multi-level marketing. This category does not include personal pages and web-hosting web pages.
Chat	Web pages that provide web-based, real-time social messaging in public and private chat rooms. This category includes IRC. This category does not include instant messaging.
Computing Internet	Web pages containing reviews, information, buyer's guides of computers, computer parts and accessories, computer software and internet companies, industry news and magazines, and pay-to-surf sites.
Consumer Protection	Websites that try to rob or cheat consumers. Some examples of their activities include selling counterfeit products, selling products that were originally provided for free, or improperly using the brand of another company. This category also includes sites where many consumers reported being cheated or not receiving services. This category does not include phishing, which tries to perpetrate fraud or theft by stealing account information.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Content Server	URLs for servers that host images, media files, or JavaScript for one or more sites and are intended to speed up content retrieval for existing web servers, such as Apache. This category includes domain-level and sub-domain-level URLs that function as content servers. This category does not include: • Web pages for businesses that provide the content servers • Web pages that allow users to browse photographs. See the Media Sharing category. • URLs for servers that serve only advertisements. See the Web Ads category.
Controversial Opinions	Web pages that contain opinions that are likely to offend political or social sensibilities and incite controversy. Much of this content is at the extremes of public opinion. This category does not include opinion or language clearly intended to promote hate or discrimination.
Cult Occult	Sites relating to non-traditional religious practices considered to be false, unorthodox, extremist, or coercive.
Dating Personals	Web pages that provide networking for online dating, matchmaking, escort services, or introductions to potential spouses. This category does not include sites that provide social networking that might include dating, but are not specific to dating.
Dating Social Networking	Web pages that focus on social interaction such as online dating, friendship, school reunions, pen-pals, escort services, or introductions to potential spouses. This category does not include wedding-related content, dating tips, or related marketing.
Digital Postcards	Web pages that allow people to send and receive digital postcards and greeting cards via the Internet.
Discrimination	Web pages, which provide information that explicitly encourages the oppression or discrimination of a specific group of individuals. This category does not include jokes and humor, unless the focus of the entire site is considered discriminatory.
Drugs	Websites that provide information on the purchase, manufacture, and use of illegal or recreational drugs. This category does not include sites with exclusive health or political themes.
Education Reference	Web pages devoted to academic-related content such as academic subjects (mathematics, history), school or university web pages, and education administration pages (school boards, teacher curriculum).
Entertainment	Web pages that provide information about cinema, theater, music, television, infotainment, entertainment industry gossip-news, and sites about celebrities such as actors and musicians. This category also includes sites where the content is devoted to providing entertainment on the web, such as horoscopes or fan clubs.
Extreme	Web pages that provide content considered gory, perverse, or horrific.
Fashion Beauty	Web pages that market clothing, cosmetics, jewelry, and other fashion-oriented products, accessories, or services. This category also includes product reviews, comparisons, and general consumer information, and services such as hair salons, tanning salons, tattoo studios, and body-piercing studios. This category does not include fashion-related content such as modeling or celebrity fashion unless the site focuses on marketing the product line.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Finance Banking	Web pages that provide financial information or access to online financial accounts. This category includes stock information (but not stock trading), home finance, and government-related financial information.
For Kids	Web pages that are family-safe, specifically for children of approximate ages ten and under. This category can also be used as an exception to allow web pages that do not pose a risk to children, or to access sites that have a primary educational or recreational focus for children, but are in other categories such as Games, Humor/Comics, Recreation/Hobbies, or Entertainment.
Forum Bulletin Boards	Web pages that provide access (http://) to Usenet newsgroups or hold discussions and post user-generated content, such as real-time message posting for an interest group. This category also includes archives of files uploaded to newsgroups. This category does not include message forums with a business or technical support focus.
Gambling	Web pages that allow users to wager or place bets online, or provide gambling software that allows online betting, such as casino games, betting pools, sports betting, and lotteries. This category does not include web pages related to gambling that do not allow betting online.
Gambling Related	Web pages that offer information about gambling, without providing the means to gamble. This category includes casino-related web pages that do not offer online gambling, gambling links, tips, sports picks, lottery results, and horse, car, or boat racing.
Game Cartoon Violence	Web pages that provide fantasy or fictitious representations of violence within the context of games, comics, cartoons, or graphic novels. This category includes images and textual descriptions of physical assaults or hand-to-hand combat, and grave injury and destruction caused by weapons or explosives.
Games	Web pages that offer online games and related information such as cheats, codes, demos, emulators, online contests or role-playing games, gaming clans, game manufacturer sites, fantasy or virtual sports leagues, and other gaming sites without chances of profit. This category includes gaming consoles.
Gen AI Application	Select this to have the Zyxel Device block Generative AI (GenAI) web pages and cloud services such as, ChatGPT, Claude, Gemini, Copilot, X, DeepSeek and so on, that generate text, code, images, audio, or other content. Note: You must apply the profile with **GenAI Application** enabled to a security policy to block GenAI for the traffic flow in that policy. The block page suggests you access these pages and services through *anyinsight.ai*. With an account, *anyinsight.ai* can filter, mask, and enforce company policies between users and these GenAI web pages and cloud services. See *anyinsight.ai* and **System > External Integrations > Heartbot** for more information.
General News	Web pages that provide online news media, such as international or regional news broadcasting and publication. This category includes portal sites that provide news content.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Government Military	Web pages that contain content maintained by governmental or military organizations, such as government branches or agencies, police departments, fire departments, civil defense, counter-terrorism organizations, or supranational organizations, such as the United Nations or the European Union. This category includes military and veterans' medical facilities.
Gruesome Content	Web pages with content that can be considered tasteless, gross, shocking, or gruesome. This category does not include web pages with content pertaining to physical assault.
Health	Web pages that cover all health-related information and health care services. This category does not include cosmetic surgery, marketing/selling pharmaceuticals, or animal-related medical services.
Historical Revisionism	Web pages that denounce, or offer different interpretations of, significant historical facts, such as holocaust denial. This category does not include all re-examination of historical facts, only historical events that are highly sensitive.
History	Web pages that provide content about historical facts. This category includes content suitable for higher education, but the Education category includes content for primary education. For example, a site with Holocaust photographs might be offensive, but have academic value.
Humor Comics	Web pages that provide comical or funny content. This category includes sites with jokes, sketches, comics, and satire pages. This category might also include graphic novel content, which is often associated with comics.
Illegal UK	Web pages that contain child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK.
Incidental Nudity	Web pages that contain non-pornographic images of the bare human body like those in classic sculpture and paintings, or medical images. This category enables you to allow or block sites in order to address cultural or geographic differences in opinion about nudity. For example, you can use this category to block access to nudity, but allow access when nudity is not the primary focus of a site, such as news sites or major portals.
Information Security	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Information Security New	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Instant Messaging	Web pages that provide software for real-time communication over a network exclusively for users who joined a member's contact list or an instant-messaging session. Most instant-messaging software includes features such as file transfer, PC-to-PC phone calls, and can track when other people log on and off.
Interactive Web Applications	Web pages that provide access to live or interactive web applications, such as browser-based office suites and groupware. This category includes sites with business, academic, or individual focus. This category does not include sites providing access to interactive web applications that do not take critical user data or offer security risks, such as Google Maps.
Internet Radio TV	Web pages that provide software or access to continuous audio or video broadcasting, such as Internet radio, TV programming, or podcasting. Quick downloads and shorter streams that consume less bandwidth are in the Streaming Media or Media Downloads categories.
Internet Services	Web pages that provide services for publication and maintenance of Internet sites such as web design, domain registration, Internet Service Providers, and broadband and telecommunications companies that provide web services. This category includes web utilities such as statistics and access logs, and web graphics like clip art.
Job Search	Web pages related to a job search including sites concerned with resume writing, interviewing, changing careers, classified advertising, and large job databases. This category also includes corporate web pages that list job openings, salary comparison sites, temporary employment, and company job-posting sites. This category does not include make-money-at-home sites.
Major Global Religions	Web pages with content about religious topics and information related to major religions. This category includes sites that cover religious content such as discussion, beliefs, non-controversial commentary, articles, and information for local congregations such as a church or synagogue homepage. The religions in this category are Baha'i, Buddhism, Chinese Traditional, Christianity, Hinduism, Islam, Jainism, Judaism, Shinto, Sikhism, Tenrikyo, Zoroastrianism.
Marketing Merchandising	Web pages that promote individual or business products or services on the web, but do not sell their products or services online. This category includes websites that are generally a company overview, describing services or products that cannot be purchased directly from these sites. Examples include automobile manufacturer sites, wedding photography services, or graphic design services. This category does not include: • Other categories that imply marketing such as Alcohol, Auctions/Classifieds, Drugs, Finance/Banking, Mobile Phone, Online Shopping, Real Estate, School Cheating Information, Software/Hardware, Stock Trading, Tobacco, Travel, and Weapons. • Sites that market their services only to other businesses. See the Business category. • Sites that rob or cheat consumers. See the Consumer Protection category.
Media Downloads	Web pages that provide audio or video files for download such as MP3, WAV, AVI, and MPEG formats. The files are saved to, and played from, the user's computer. This category does not include audio or video files that are played directly through a browser window. See the Streaming Media category.
Media Sharing	Web pages that allow users to upload, search for, and share media files and photographs, such as online photograph albums.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Messaging	Examples include text messaging to mobile phones, PDAs, fax machines, and internal website user-to-user messaging or site-to-site messaging. This category does not include real-time chat or instant messaging, or message posts that can be viewed by anyone but the intended recipient.
Mobile Phone	Web pages that sell media, software, or utilities for mobile phones that can be downloaded and delivered to mobile phones. Examples include ringtones, logos/skins, games, screen-savers, text-based tunes, and software for SMS, MMS, WAP, and other mobile phone protocols.
Moderated	Bulletin boards, chat rooms, search engines, or web mail sites that are monitored by an individual or group who has the authority to block messages or content considered inappropriate. This category does not include sites with posted rules against offensive content. See the Forum/Bulletin Boards category.
Motor Vehicles	Websites for manufacturers and dealerships of consumer transportation vehicles, such as cars, vans, trucks, SUVs, motorcycles, and scooters. This category also includes sites that provide product marketing, reviews, comparisons, pricing information, auto fairs, auto expos, and general consumer information about motor vehicles. This category does not include automotive accessories, mechanics, auto-body shops, and recreational hobby pages. This category does not include sites that provide business-to-business-only content regarding motor vehicles.
Non Profit Advocacy NGO	Web pages from charitable or educational groups that fulfill a stated mission, benefiting the larger community, such as clubs, lobbies, communities, non-profit organizations, labor unions, and advocacy groups. Examples are Masons, Elks, Boy and Girl Scouts, or Big Brothers.
Nudity	Web pages that have non-pornographic images of the bare human body. This category includes classic sculpture and paintings, artistic nude photographs, some naturism pictures, and detailed medical illustrations. This category does not include high-profile sites where nudity is not a concern for visitors. See the Incidental Nudity category.
Online Shopping	Web pages that sell products or services online. Web pages selling a broad range of products might pose a risk to users by offering access to items that are normally in other categories such as Pornography, Weapons, Nudity, or Violence. Web pages selling such content exclusively are in their respective categories.
P2P File Sharing	Web pages that allow the exchange of files between computers and users for business or personal use, such as downloadable music. P2P clients allow users to search for and exchange files from a peer-user network. They often include spyware or real-time chat capabilities. This category includes BitTorrent web pages.
PUPs	Web pages that contain Potentially Unwanted Programs (PUPs). PUPs are often made for a beneficial purpose but they alter the security of a computer or the computer user's privacy. Computer users who are concerned about security or privacy might want to be informed about this software, and in some cases, they might want to remove this software from their computers.
Parked Domain	Web pages that once served content, but their domains have been sold or abandoned and are no longer registered. Parked domains do not host their own content, but usually redirect users to a generic page that states the domain name is for sale, or redirect users to a generic search engine and portal page, some of which provide valid search engine results.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Personal Network Storage	Web pages that allow users to upload folders and files to an online network server in order to backup, share, edit, or retrieve files or folders from any web browser.
Personal Pages	Personal home pages that share a common domain such as those hosted by ISPs, university/education servers, or free web page hosts. This category also includes unique domains that contain personal information, such as a personal home page. This category does not include home pages of public figures.
Pharmacy	Web pages that provide reviews, descriptions, and market or sell prescription-based drugs, over-the-counter drugs, birth control, or dietary supplements.
Politics Opinion	Web pages covering political parties, individuals in political life, and opinion on various topics. This category might also cover laws and political opinion about drugs. This category includes URLs for political parties, political campaigning, and opinions on various topics, including political debates.
Pornography	Web pages that contain materials intended to be sexually arousing or erotic. This category includes fetish pages, animation, cartoons, stories, and illegal pornography.
Portal Sites	Web pages that serve as major gateways or directories to content on the web. Many portal sites also provide a variety of internal site features or services such as search engines, email, news, and entertainment. Mailing list sites with a variety of content are in this category. This category does not include sites with topic-specific content.
Potential Criminal Activities	Web pages that provide instructions to commit illegal or criminal activities. Instructions include committing murder or suicide, sabotage, bomb-making, lock-picking, service theft, evading law enforcement, or spoofing drug tests. This category might also include information on how to distribute illegal content, perpetrate fraud, or consumer scams. This category does not include computer-related fraud.
Potential Hacking Computer Crime	Web pages that provide instructions, or otherwise enable, fraud, crime, or malicious activity that is computer-oriented. This category includes web pages related to computer crime include malicious hacking information or tools that help individuals gain unauthorized access to computers and networks (root kits, kiddy scripts). This category also includes other areas of electronic fraud such as dialer scams and illegal manipulation of electronic devices. This category does not include illegal software.
Potential Illegal Software	Web pages, which the filter believes offer information to potentially ‘pirated’ or illegally distribute software or electronic media, such as copyrighted music or film, distribution of illegal license key generators, software cracks, and serial numbers. This category does not include peer-to-peer web pages.
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.
Profanity	Web pages that contain crude, vulgar, or obscene language or gestures.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Professional Networking	Web pages that provide social networking exclusively for professional or business purposes. This category includes sites that provide personal or group profiles, and enable their members to interact through real-time communication, message posting, public bulletins, and media sharing. This category also contains alumni sites that have a networking function. This category does not include social networking sites where the focus might vary, but include friendship, dating, or professional focuses.
Provocative Attire	Web pages with pictures that include alluring or revealing attire, lingerie and swimsuits, or supermodel or celebrity photograph collections, but do not involve nudity. This category does not include sites with swimwear or similar attire that is not intended to be provocative. For example, Olympic swimming sites are not in this category.
Public Information	Web pages that provide general reference information such as public service providers, regional information, transportation schedules, maps, or weather reports.
Real Estate	Web pages that provide commercial or residential real estate services and information. Service and information includes sales and rental of living space or retail space and guides for apartments, housing, and property, and information on appraisal and brokerage. This category includes sites that allow you to browse model homes. This category does not include content related to personal finance, such as credit applications.
Recreation Hobbies	Web pages for recreational organizations and facilities that include content devoted to recreational activities and hobbies. This category includes information about public swimming pools, zoos, fairs, festivals, amusement parks, recreation guides, hiking, fishing, bird watching, or stamp collecting. This category does not include activities that need no active participation, such as watching a movie or reading celebrity gossip.
Religion Ideology	Web pages with content related to religious topics and beliefs in human spirituality that are not within the major religions. This category includes religious discussion, beliefs, articles, and information for local congregations or groups such as a church homepage, unless the site is already in the Major Global Religions category. This category also includes comparative religion, or sites that include religions and ideologies. This category does not include astrology and horoscope sites
Remote Access	Web pages that provide remote access to a program, online service, or an entire computer system. Although remote access is often used legitimately to run a computer from a remote location, it creates a security risk, such as backdoor access. Backdoor access, written by the original programmer, allows the system to be controlled by another party without the user's knowledge.
Reserved	This category is reserved for future use.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Residential IP Addresses	IP addresses (and any domains associated with them) that access the Internet by DSL modems or cable modems. Because this content is not generally intended for Internet access via HTTP, access to the Internet through these IP addresses can indicate suspicious behavior. This behavior might be related to malware located on the home computer or homegrown gateways set up to allow anonymous Internet access.
Resource Sharing	Web pages that harness idle or unused computer resources to focus on a common task. The task can be on a company or an international basis. Well known examples are the SETI program and the Human Genome Project, which use the idle time of thousands of volunteered computers to analyze data.
Restaurants	Web pages that provide information about restaurants, bars, catering, take-out and delivery, including online ordering. This category includes sites that provide information about location, hours, prices, menus and related dietary information. This category also includes restaurant guides and reviews, and cafes and coffee shops. This category does not include groceries, wholesale food, non-profit and charitable food organizations, or bars that do not focus on serving food.
School Cheating Information	Web pages that promote plagiarism or cheating by providing free or fee-based term papers, written essays, or exam answers. This category does not include sites that offer student help, discuss literature, films, or books, or other content that is often the subject of research papers.
Search Engines	Web pages that provide search results that enable users to find information on the Internet based on key words. This category does not include site-specific search engines.
Sexual Materials	Web pages that describe or depict sexual acts, but are not intended to be arousing or erotic. Examples of sexual materials include sex education, sexual innuendo, humor, or sex related merchandise. This category does not include web pages with content intended to arouse.
Shareware Freeware	Web pages that are repositories of downloadable copies of shareware and freeware. This category does not include subscription-based software.
Social Networking	Web pages that enable social networking for a variety of purposes, such as friendship, dating, professional, or topics of interest. These sites provide personal or group profiles and enable interaction among their members through real-time communication, message posting, public bulletins, and media sharing. This category does not include sites that are exclusive to dating, matchmaking, or a specific professional networking focus.
Software Hardware	Web pages related to computing software and hardware, including vendors, product marketing and reviews, deployment and maintenance of software and hardware, and software updates and add-ons such as scripts, plug-ins, or drivers. Hardware includes computer parts, accessories, and electronic equipment used with computers and networks. This category includes the marketing of software and hardware, and magazines focused on software or hardware product reviews or industry trends.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Sports	Web pages related to professional or organized recreational sports. This category includes sporting news, events, and information such as playing tips, strategies, game scores, or player trades. This category does not include fantasy leagues, sports centers, athletic clubs, fitness or martial arts clubs, and non-league billiards, darts, or other such activities.
Stock Trading	Web pages that offer purchasing, selling, or trading of shares online. This category also includes ticker-tape information that enables viewing of real-time stock prices and financial spread betting in the stock market. Other betting is in the Gambling category. This category does not include sites that offer information about stocks, but do not offer purchasing, selling, or trading of shares.
Streaming Media	Web pages that provide streaming media, or contain software plug-ins for displaying audio and visual data before the entire file has been transmitted. This category does not include audio or video files that are downloaded to a user's computer before being played.
Technical Business Forums	Web pages with a technical or business focus that provide online message posting or real-time chatting, such as technical support or interactive business communication. Although users can post any type of content, these forums tend to present less risk of containing offensive content. Sites that offer a variety of forums with themes, including technical and business content, are only in the categories of Forum/Bulletin Boards or Chat.
Technical Information	Web pages that provide computing information with an educational focus in areas such as Information Technology, computer programming, and certification. Examples include Linux user groups, UNIX commands, software tutorials, or dictionaries of technical terms. Most sites in this category might be subdirectories of larger domains. For example, a software site with a tutorial page is in this category only at the tutorial page URL. This category does not include content about information security.
Text Spoken Only	Content that is text or audio only, and does not contain pictures. This category can be used as an exception to allow explicit text and recorded material to be accessed when you want pictures blocked using the Pornography, Violence, or Sexual Materials categories. Libraries or universities can use this category to prevent the display of offensive graphics in their public facilities.
Text Translators	Web pages that allow users to type phrases or a block of text to translate it from one language into another. This category also includes language identifier web pages. URL translation is in the Anonymizing Utilities category.
Tobacco	Web pages that sell, promote, or advocate the use of tobacco products, tobacco paraphernalia, including cigarettes, cigars, pipes, snuff and chewing tobacco.
Travel	Web pages that promote personal or business travel, such as hotels, resorts, airlines, ground transportation, car rentals, travel agencies, and general tourist and travel information. This category also includes sites for buying tickets or accommodation. This category does not include personal vacation photographs.

Table 97 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Usenet News	Web pages that provide access (http://) to Usenet newsgroups and archives of files uploaded to newsgroups. This category also includes online groups that offer similar community-oriented content posting.
Violence	Web pages that contain real or lifelike images or text that portray, describe, or advocate physical assaults against people, animals, or institutions, such as depictions of war, suicide, mutilation, or dismemberment.
Visual Search Engine	Web pages that provide image-specific search results such as thumbnail pictures. This category does not include sites that offer site-specific visual search engines.
Weapons	Web pages that provide information about buying, making, modifying, or using weapons, such as guns, knives, swords, paintball guns, and ammunition, explosives, and weapon accessories. This category also includes sites that contain content for: weapons for personal or military use, homemade weapons, non-lethal weapons such as mace, pepper spray, or Taser guns, weapons facilities, such as shooting ranges, and government or military oriented weapons. This category does not include political action groups, such as the NRA.
Web Ads	Web pages that provide advertisement-hosting or programs that create advertisements. Examples include links, source code or applets for banners, popups, and other kinds of static or dynamically generated advertisements that appear on web pages. This category is intended to block advertisements on web pages, not the companies that provide the advertisements or advertising services. This category does not include aggressive advertising adware. See the Spyware/ Adware category.
Web Mail	Web pages that enable users to send or receive email through the Internet.
Web Meetings	Web pages that host live meetings, video conferences, and interactive presentations mainly for businesses. Web meetings generally include streaming audio and video, and allow data transfer or office-oriented application sharing, such as online presentations.
Web Phone	Web pages that enable users to make telephone calls via the Internet or obtain information or software for this purpose. Web Phone service is also called Internet Telephony, or VoIP. Web phone service includes PC-to-PC, PC-to-phone, and phone-to-phone services connecting via TCP/ IP networks.
Unrated	Web pages that cannot be categorized into the categories listed above.

CHAPTER 25
Sandboxing

25.1 Sandboxing Overview

Zyxel sandbox is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Files with unknown or untrusted programs and codes are uploaded to the cloud. These files are executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs). The zero-day malware refers to malware that is unknown to any software vendor or developer. It is dangerous because there is no available defenses against it at the time of discovery.

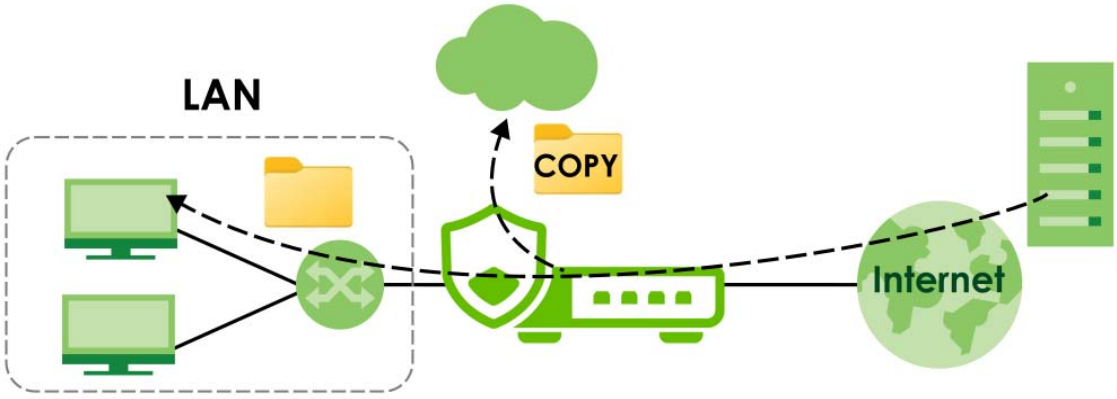
The zero-day malware and APTs may evade the Zyxel Device's detection, such as anti-malware. Results of cloud sandbox are sent from the server to the Zyxel Device.

After checking the received files against its local cache, the Zyxel Device sandbox uploads a copy of the files for inspection if the files are not recorded in the local cache. The scan result from the cloud is added to the Zyxel Device cache and used for future inspection. When a file with malicious or suspicious code is detected, the Zyxel Device takes specific actions on the threats.

By default, the Zyxel Device sandbox forwards all files that have not been checked before to the clients behind the Zyxel Device.

Note: The scan results will be removed from the Zyxel Device cache after the Zyxel Device restarts. When the scan results stored reach the limit, new scan results automatically overwrite existing scan results, starting with the oldest scan result first.

Figure 94 Zyxel Sandbox Inspection



The Zyxel Device forwards files that are not recorded in the local cache to the client behind the Zyxel Device before sandbox has completed checking. The scan result will display in the logs. We suggest you to inform your client not to open the file until sandbox has completed checking. If the client already opened it, then please urge the client 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.

25.2 Sandbox Commands

The following table describes the sandbox commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 98 Sandbox Commands

COMMAND	DESCRIPTION
`vrf main sandbox enabled {true| false}`	Turns on sandbox on the Zyxel Device. The `false` command disables sandbox.
`vrf main sandbox statistics enabled {true| false}`	Enable to have the Zyxel Device collect sandbox statistics, such as the time, type and name of the files scanned.
`vrf main sandbox malicious action {allow| destroy} logging {no| log| log-alert}`	Sets whether the Zyxel Device deletes (`destroy`) or forwards (`allow`) malicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a malicious file is detected. Malicious files are files given a high score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.
`vrf main sandbox suspicious action {allow| destroy} logging {no| log| log-alert}`	Sets whether the Zyxel Device deletes (`destroy`) or forwards (`allow`) suspicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a suspicious file is detected. Suspicious files are files given a medium score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.
`vrf main sandbox file-type {archives| executables| ms-office-document| macromedia-flash-data| pdf| rtf}`	Specifies the type of files to be sent for sandbox inspection. • `archives`: A zip file is a file used to compress multiple files together into a single file. A zip file can reduce the overall size of a collection of files. • `executables`: An executable file is a file that contains a program or application which your computer can run • `ms-office-document`: This category includes Microsoft Word files, Microsoft Excel files and Microsoft PowerPoint files. MS Office Document are files that are created using software developed by Microsoft. • `macromedia-flash-data`: A flash file (.swf) is a file that contains animations, multimedia elements or games. A flash file is often embedded into a web page. • `pdf`: A Portable Document Format (PDF) file is a file that maintains the presentation and formatting of documents across different platform and devices. • `rft`: A Rich Text Format (RTF) file is a file that allows you to create text with different formats, such as bold or italics.
`show state vrf main sandbox statistics {summary| top-entry| event}`	Displays: • a summary of the collected sandbox statistics. • top log entries by destination IP, source IP and type. • the time, type, file name, hash, destination IP and source IP of the files scanned.

25.2.1 Sandbox Command Examples

This command shows how to enable sandbox on the Zyxel Device and displays the status of security services.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main sandbox enabled true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show state vrf main sandbox statistics summary
summary
    scanning 0
    scanned 0
    destroyed-files 0
    malicious-files 0
    suspicious-files 0
    safe-files 0
    other 0
```

This command sets the Zyxel Device to delete malicious files and generate a log when a malicious file is detected.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main sandbox malicious action destroy logging log
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 26
SSL Inspection

26.1 SSL Inspection Overview

Secure Socket Layer (SSL) traffic, such as HTTPS, POP3+SSL, and SMTPS, is encrypted and therefore cannot be inspected using Unified Threat Management (UTM) profiles such as App Patrol, Content Filter, Intrusion Prevention System (IPS), 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.

The Zyxel Device supports the following SSL/TLS versions and cipher suites:

- TLS1.0 AES-CBC
- TLS1.2 AES-CBC/AES-GCM
- TLS1.3

SSL inspection does not support the following:

- Compression
- Client Authentication
- SSLv3 AES-CBC

26.2 SSL Inspection Command Input Values

The following table describes the values required for many SSL inspection commands. Other values are discussed with the corresponding commands.

Table 99 SSL Inspection Command Input Values

LABEL	DESCRIPTION
profile-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.
description	This is additional information about this SSL Inspection profile. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
cert-name	This is a name of a certificate.

26.3 SSL Inspection General Commands

The table lists the SSL inspection general commands.

Table 100 SSL Inspection General Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection server-sign-cert mode {rsa-1024| rsa-2048| ecdsa-rsa-1024| ecdsa-rsa-2048}`	Select how to validate a client accessing an HTTPS website using RSA or ECDSA encryption through the Zyxel Device. ECDSA is required by certain clients such as iOS 13. The Zyxel Device must check that the client's certificate and public key are valid and were issued by a Certificate Authority (CA) listed in the Zyxel Device's list of trusted CAs. The default value is 1024. • `ecdsa-rsa-1024` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-1024 if the client does not support ECDSA-256. • `ecdsa-rsa-2048` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-2048 if the client does not support ECDSA-256. Note: You should flush the SSL inspection certificate cache after changing the server signing mode.
`vrf main ssl-inspection default-port enabled {true| false}`	Sets the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 443 (HTTPS), 465 (SMTP), 993 (IMAP) and 995 (POP3). You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main ssl-inspection default-port {extra-port| exception-port}` *`port number`*	Uses the `extra-port` command to add a port to the default specified port list. Uses the `exception-port` command to remove a port from the default specified port list.
`show config vrf main ssl-inspection server-sign-cert mode`	Displays the type of encryption used to validate a client accessing an HTTPS website through the Zyxel Device.
`show config vrf main ssl-inspection default-port enabled`	Displays if the default port is enabled.
`show state vrf main ssl-inspection default-cert-version`	Displays: • The current certificate set version. • The date and time the current certificate set was released.
`show state vrf main ssl-inspection default-port-state`	Displays the Zyxel Device default ports.
`show state vrf main ssl-inspection cert-list`	Displays certificates used in SSL Inspection.

26.4 SSL Inspection Exclusion Commands

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 passes through the Zyxel Device uninspected.

This table lists the SSL inspection exclusion-related commands.

Table 101 SSL Inspection Exclusion Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection exclude-list-settings log-enabled {true| false}`	Create a log for traffic that bypasses SSL inspection. The `false` command disables SSL exclusion list logging.
`vrf main ssl-inspection exclude-list <exclude-list entry>`	Create an entry in one of the following ways: • Type an IPv4. For example, type 192.168.1.35 • Type an IPv4 block in CIDR notation. For example, type 192.168.1.1/24 • Type an IPv4 address range by entering the start and end addresses separated by a hyphen (-). For example, type 192.168.1.1-192.168.1.35 • Type a DNS name. For example, type www.zyxel.com.tw. • Type 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. • Type an email address. For example, type abc@zyxel.com.tw
`show config vrf main ssl-inspection exclude-list-settings log-enabled`	Displays whether the Zyxel Device will create a log for traffic that bypasses SSL inspection.
`show config vrf main ssl-inspection exclude-list`	Displays the SSL inspection exclude list settings.

26.5 SSL Inspection Profile Settings

This table lists the SSL inspection profile setting commands.

Table 102 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection profile <profile-name>`	Creates an SSL inspection profile, and then enters the SSL inspection profile sub-command mode. The profile name may consist of 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`description <description>`	Enter additional information about this SSL inspection entry. You can enter up to 60 characters (0-9az-A-Z’()+:=?;!*#@$_%-”).
`support-version-min version {tls1_0| tls1_1| tls1_2}`	The Zyxel Device only inspects SSL traffic if the SSL version is equal to this value or higher.

Table 102 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
support-version-min logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic that matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
unsupported-suite action {pass| block}	Select to pass or block unsupported traffic, such as traffic using unsupported cipher suites, compression, or client authentication.
unsupported-suite logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic tat matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
untrusted-cert-chain action {pass| block| inspect}	Sets whether to pass, inspect, or block an untrusted certification 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
untrusted-cert-chain logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic tat matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
certificate <*cert-name*>	Sets the certificate for this profile.
show config vrf main ssl-inspection profile	Displays the SSL inspection profiles settings.

26.6 SSL Inspection Certificate Update

Use these commands to update the latest certificates of servers using SSL connections to the Zyxel Device network. You must have Internet access and have activated SSL Inspection on the Zyxel Device at myZyxel.com.

This table lists the SSL inspection certificate cache commands.

Table 103 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
cmd ssl-inspection cert-update now	Download the latest certificate set from the myZyxel.com and update it on the Zyxel Device.
vrf main ssl-inspection cert-update auto {true| false}	The Zyxel Device automatically updates the certificate set when a new one becomes available on myZyxel.com.
show config vrf main ssl-inspection cert-update auto	Displays if automatically updating the certificate set is configured on the Zyxel Device.

26.7 SSL Inspection Statistics

This table lists the SSL inspection statistics commands.

Table 104 SSL Inspection Statistics Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection statistics enabled {true| false}`	Enables SSL inspection statistics collection. The `false` command disables SSL exclusion statistics collection.
`show config vrf main ssl-inspection statistics enabled`	Displays if SSL inspection statistics collection is enabled.
`show state vrf main ssl-inspection statistics summary`	Displays SSL inspection statistics such as time up, maximum concurrent sessions, concurrent sessions, total SSL sessions, sessions inspected, decrypted Kilobytes, encrypted Kilobytes, sessions blocked and sessions passed.
`show state vrf main ssl-inspection statistics summary {time | maximum-concurrent-sessions | concurrent-sessions | total-tls-sessions | sessions-inspected | decrypted | encrypted | sessions-blocked | sessions-passed}`	Displays specific details on the specified SSL inspection criteria.

26.8 SSL Inspection Debug Command

This table lists the SSL inspection debug commands.

Table 105 SSL Inspection Debug Commands

COMMAND	DESCRIPTION
`cmd debug ssl-inspection console enabled {true | false}`	Enables SSL inspection debug logs regarding data encryption and decryption on the Command Line Interface (CLI). The `false` command disables SSL inspection debug logs on the CLI.
`cmd debug ssl-inspection daemon console enabled {true | false}`	Enables daemon debug logs regarding certificate queries on the CLI. The `false` command disables daemon debug logs on the CLI.

26.9 SSL Inspection Command Examples

These are some other example SSL Inspection usage commands.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ssl-inspection statistics enabled true
usgflex200hp running config# vrf main ssl-inspection exclude-list 1.1.1.1
usgflex200hp running config# vrf main ssl-inspection exclude-list 2.2.2.2
usgflex200hp running config# vrf main ssl-inspection profile Config1
usgflex200hp running profile Config1# support-version-min version tls1_1
usgflex200hp running profile Config1# support-version-min logging log
usgflex200hp running profile Config1# unsupported-suite action block
usgflex200hp running profile Config1# unsupported-suite logging log-alert
usgflex200hp running profile Config1# untrusted-cert-chain action block
usgflex200hp running profile Config1# untrusted-cert-chain logging log-alert
usgflex200hp running profile Config1# certificate default
usgflex200hp running profile Config1# commit
Configuration committed.
usgflex200hp running profile Config1# exit
usgflex200hp> edit running
usgflex200hp running config# show config vrf main ssl-inspection profile
profile Config1
    certificate default
    support-version-min
        version tls1_1
        logging log
        ..
    unsupported-suite
        action block
        logging log-alert
        ..
    untrusted-cert-chain
        action block
        logging log-alert
        ..
usgflex200hp running config# show config vrf main ssl-inspection exclude-list
exclude-list 1.1.1.1
exclude-list 2.2.2.2
```

CHAPTER 27
IP Exception

27.1 IP Exception Overview

IP Exception allows incoming IP packets to bypass specific security services based on the packet's source or destination address. Bypassing a security service means the security service does not intercept nor inspect the packet.

For example, 192.168.100.100 is a trusted LAN computer. Add the IP address of the LAN computer to **Source** in **IP Exception** so the Zyxel Device will not perform security checking on traffic coming from this computer.

Figure 95 IP Exception Bypass Source Example

You can also add a trusted destination to bypass security checking. For example, 2.2.2.2 is a trusted web site. Add the IP address of the trusted web site to **Destination** in **IP Exception** so the Zyxel Device will not perform security checking when you access the web site to save resources.

Figure 96 IP Exception Bypass Destination Example

IP Exception supports bypassing the following security services:

- Anti-Malware
- URL Threat Filter
- IPS (Intrusion Prevention System)
- IP Reputation.
- DNS Threat Filter

27.2 IP Exception Command Input Values

The following table identifies the values required for many IP Exception commands.

Table 106 IP Exception Command Input Values

LABEL	DESCRIPTION
profile-name	The name of an IP Exception rule. You may use 2-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address-name	The source or destination address of an IP packet. The address name can be any of the following: • Address object name • Address group object name • FQDN object name For details on addresses, see Chapter 29 on page 243.

27.3 IP Exception Commands

The Zyxel Device excludes incoming packets that match any IP Exception rule. Each IP Exception rule contains a source address, destination address, and a list of bypassed services.

The following table lists the IP Exception commands.

Table 107 IP Exception Commands

COMMAND	DESCRIPTION
`vrf main ip-exception profile <profile-name>`	Creates an IP exception profile, and then enters the IP exception profile sub-command mode. The profile name may consist of 2-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`enabled {true| false}`	Enables or disables the specified profile.
`source address-object {ipv4-address address-name| ipv4-group address-name| any}`	Sets an address object of the source IP address for this profile. Uses the `any` command to have no restriction on the source IP address.
`destination address-object {ipv4-address address-name| ipv4-group address-name| any}`	Sets an address object of the destination IP address for this profile. Uses the `any` command to have no restriction on the destination IP address.
`logging {no| log}`	Sets whether the Zyxel Device creates a log when the incoming traffic matches the settings you configured in the profile.

Table 107 IP Exception Commands (continued)

COMMAND	DESCRIPTION
{anti-malware| url-threat-filter| ips| ip-reputation| dns-threat-filter} {pass| bypass}	Sets the service that IPv4 packets will bypass. To bypass multiple services, run the command multiple times.
show config vrf main ip-exception profile	Displays the IP exception profiles settings.

CHAPTER 28
User/Group

28.1 User Account Overview

This chapter 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.

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

28.1.1 User Types

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

Table 108 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP, Console
Viewer	Look at the Zyxel Device settings (web) Perform basic diagnostics (CLI)	WWW, SSH, Console
Access Users		
User	Access network services	WWW
Ext-User	External user account	WWW

28.2 User/Group Command Input Values

The following table identifies the values required for the user/group commands. Other input values are discussed with the corresponding commands.

Table 109 User/Group Command Input Values

LABEL	DESCRIPTION
username	The name of the 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.
groupname	The name of the 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. It cannot be the same as the user name.

28.3 User Commands

The first table lists the commands for users. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 110 User/Group Commands: Users

COMMAND	DESCRIPTION
`object user-object admin <username> role {admin| viewer}`	Creates an admin account and sets the user type to admin or viewer. Presses enter to enter the sub-command mode.
`object user-object user <username> role {user| ext-user}`	Creates a user account and sets the user type to user or ext-user. Presses enter to enter the sub-command mode.
`object user-object admin <username> gui theme-mode {light | dark}`	Specifies the theme of the Web Configurator for the specified user.
`object user-object admin <username> enabled {true | false}`	Enables or disables the local administrator. A disabled administrator cannot log in to the Zyxel Device. This function is available only to local administrators with the “admin” user type. At least one administrator must remain enabled on the Zyxel Device. Note: Be careful not to disable your own account.
`object user-object user {radius-users | ldap-users | ad-users | ncas-users | ctc-users | oidc-users}`	Enters sub-command mode for the selected user group: RADIUS (Remote Authentication Dial-In User Service), LDAP (Lightweight Directory Access Protocol), AD (Active Directory), NCAS (Nebula Cloud Authentication Server), CTC (Captive Portal Clients), or OIDC (OpenID Connect).
`role {user| ext-user | ext-group-user | mac-address | ctc-user}`	Sets the user type of the default user account for the selected user group.
`password <encrypted-password>`	Sets the password for the user account. Uses the `password` command followed by the encrypted password, to set this encrypted password in a saved configuration file
`password-shadow <password>`	Sets the password for the user account. Uses the `password-shadow` command followed by the password in plain text, to encrypt this password in a saved configuration file. Valid plain text characters are [0-9][a-z][A-Z]['(){}<>^`+/:!*#@&=$.~%|;-"] The password requires: • From 6 to 63 characters • At least 1 upper case letter • At least 1 digit • At least 1 special character.
`description <description>`	Sets the description for the specified user. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.

Table 110 User/Group Commands: Users (continued)

COMMAND	DESCRIPTION
logon-lease-time {default| *0...7200*}	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The default value is 1440 (minutes).
logon-reauth-time {default| *0...7200*}	Sets the reauthorization time for the specified user. The default value is 1440 (minutes).
enabled {true | false}	Enables or disables the user account. All user accounts are enabled by default. Make sure to notify the account owner before you disable a user account. Be careful not to disable your own account.
mobile <*mobile-number*>	Sets the mobile phone number for the account. You can use up to 20 character length, including numbers 1~9 and characters +*#()-
aaa-server	Binds an external group user-object (ext-group-user) to a valid authentication server profile (AD, LDAP, OIDC, or RADIUS). This is required for external group users (ext-group-user), but not for external users (ext-user).
group-id <*group-identifier*>	Enter the name of the attribute that the Zyxel Device is to check to determine to which group this user group belongs.
email <*email-address*>	Specifies up to two email addresses for a user account.
password-policy {admin| user} complexity	Sets a complexity rule for the user account password. The new rule will take effect the next time you change your password.
enabled {true| false}	Enables or disables the complexity rule for the user account password. All the following requirements are disabled by default.
length-limit min-length *<min-length>* enabled {true| false}	Specifies a minimum number of characters (4–20) for the user account password.
upper-char-limit enabled {true| false}	Sets if the password must include an uppercase letter.
digit-char-limit enabled {true| false}	Sets if the password must include a number.
special-char-limit enabled {true| false}	Sets if the password must include a special character [`'"~!@#$%^&*()_-+={}|,<>/:;.].
prehibit-same-username enabled {true| false}	Sets if the password must not be the same as the username.
reuse-limit enabled {true| false}	Sets if the password must not be reused from previously configured passwords.
reuse-limit count <*1-12*>	Sets how many previous passwords cannot be reused.
show config object user-object {admin| user}	Displays general information of admin accounts and user accounts, such as: • The account role. • If the account is enabled. • Authentication timeout settings.

Table 110 User/Group Commands: Users (continued)

COMMAND	DESCRIPTION
`show state object user-object {admin| user}`	Displays detailed information of admin accounts and user accounts, such as: • Account password in cipher text. • Account email and mobile number. • The date the account is created. • The password is modified.
`show config password-policy`	Displays information about the complex rule for the user account password requirements.

28.3.1 User Command Examples

The following example shows how to create a password shadow for the admin, 'Boss'. Use the show command to see what the encrypted password in a saved configuration file will be.

```
usgflex500h> edit running
usgflex500h running config# object user-object admin Boss
usgflex500h running admin Boss# password-shadow S3cret!
usgflex500h running admin Boss# show config password-shadow S3cret!
password $5$tsXB3bzHko2t5UWK$aZP1USJVYIhC/6qbhCduZiAreRNyBEvcxEq0pk2LKj3
usgflex500h running admin Boss# commit
Configuration committed.
usgflex500h running admin Boss#
```

The following example list the requirements with bullets for the user account password.

```
usgflex500h> edit running
usgflex500h running config# password-policy admin complexity enabled true
usgflex500h running config# password-policy admin complexity length-limit min-
length 6
usgflex500h running config# password-policy admin complexity upper-char-limit
enabled true
usgflex500h running config# show config password-policy admin
admin
    complexity
        enabled true
        length-limit
            enabled true
            min-length 6
            ..
        upper-char-limit
            enabled true
            min-upper 1
            ..
        digit-char-limit
            enabled false
            min-digit 1
            ..
        special-char-limit
            enabled false
            min-special 1
            ..
        ..
    ..
```

28.4 Group Commands

This table lists the commands for groups of users. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 111 User/Group Commands: Groups

COMMAND	DESCRIPTION
`object user-object group <groupname>`	Creates the specified user group and enters sub-command mode.
`object user-object group <groupname> description <description>`	Sets the description for the specified user group. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`object user-object group <groupname> user-list <username>`	Adds the specified user to the specified user group.
`object user-object group <groupname> group-list <groupname>`	Adds the specified user group to the user group you're configuring.

Table 111 User/Group Commands: Groups (continued)

COMMAND	DESCRIPTION
`show config object user-object group`	Displays general information of the group settings, such as group names and users included in each group.
`show state object user-object group`	Displays detailed information of the group settings, such as group names, users included in each group and the number of times a group is used in other settings.

28.5 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 112 User/Group Commands: Setting

COMMAND	DESCRIPTION
`system user-setting default-logon-lease-time {admin| user| ext-user} <0...7200>`	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time.
`system user-setting default-logon-reauth-time {admin| user| ext-user} <0...7200>`	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time.
`system user-setting pwd-expiry force-change-pwd {true| false}`	Forces users to change their password after a certain period of time.
`system user-setting pwd-expiry expiration-days <1...365>`	Sets how often users must change their password.
`system user-setting pwd-expiry link-to-device <IP/FQDN>`	Enters an IP address or FQDN to associate the password expiration settings to a specific Zyxel Device.
`system user-setting simultaneous-logon administration-enforce {true| false}`	Sets a limit on the number of simultaneous logins by admin users. Disables this to allow admin users to log in as many times as they want at the same time using the same or different IP addresses.
`system user-setting simultaneous-logon administration-limit <1...300>`	Sets the maximum number of simultaneous logins by each admin user.
`system user-setting simultaneous-logon access-enforce {true| false}`	Enables this to set a limit on the number of simultaneous logins by non-admin users. Disables this to allow non-admin users to log in as many times as they want as long as they use different IP addresses.
`system user-setting simultaneous-logon access-enforce <1...300>`	Sets the maximum number of simultaneous logins by each non-admin user.
`system user-setting simultaneous-logon kick-previous {true| false}`	Sets the action the Zyxel Device will take when the limit you set for the numbers of simultaneous logins by admin users or non-admin users has exceeded. Enables this to have the Zyxel Device remove the earliest login account. Disables this to have the Zyxel Device block any accounts that try to log in.

Table 112 User/Group Commands: Setting

COMMAND	DESCRIPTION
`system user-setting retry-limit enabled {true| false}`	Enables the retry limit for users.
`system user-setting retry-limit retry-count <1...99>`	Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The default value is five.
`system user-setting retry-limit lockout-period <1...6553>`	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The default value is 30.
`system user-setting update-lease-auto {true| false}`	Enables this to let users automatically renew their lease time. Disables this to prevent them from automatically renewing it.
`show config system user-setting`	Displays the user settings you configured on the Zyxel Device.
`show state system user-setting`	Displays the status of user settings on the Zyxel Device.

28.5.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
usgflex200hp> edit running
usgflex200hp running config# system user-setting simultaneous-logon
administration-enforce true
usgflex200hp running config# system user-setting simultaneous-logon
administration-limit 50
usgflex200hp running config# system user-setting simultaneous-logon access-enforce
true
usgflex200hp running config# system user-setting simultaneous-logon access-limit 50
usgflex200hp running config# system user-setting simultaneous-logon kick-previous
true
usgflex200hp running config# commit
Configuration committed.
```

28.5.2 Create User Accounts Command Examples

Lease time is the idle timeout for a specific user. A logged in user must use the web configurator or CLI before he is logged out.

Reauthentication time is the number of minutes the user can be logged into the Zyxel Device in one session before the user has to log in again.

For example, suppose you've set the lease time to 30 minutes and the reauthentication time to 60 minutes. See the comparison table below for more information on the differences between lease time and reauthentication time.

Table 113 Lease Time and Reauthentication Time Comparison Table

	USER ACTION	RESULT
Lease Time	The user has used the Zyxel Device web configurator or CLI within 30 minutes.	The user will not be logged out.
	The user has not used the Zyxel Device web configurator or CLI for over 30 minutes.	The user will be logged out.
Reauthentication Time	The user has used the Zyxel Device web configurator or CLI within 60 minutes.	After 60 minutes, the user will be logged out. He must log in again.
	The user has not used the Zyxel Device web configurator or CLI for over 60 minutes.	

You want to log the admin account **Max** out if 60 minutes of idle time have passed, that is, he has not been using the Zyxel Device web configurator or CLI.

You want to make the number of minutes unlimited so the admin account **Max** will not have to log in again after a certain time period.

Table 114 Create User Account Example

USER NAME	PASSWORD	USER TYPE
Max	1234	admin

1 Create an admin account using the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object user Max role user
usgflex200hp running config# object user-object user Max
usgflex200hp running user Max# password
Enter value for password>
Confirm value for password>
usgflex200hp running user Max# logon-lease-time 60
usgflex200hp running user Max# logon-reauth-time 0
```

2 Save the current configuration to the Zyxel Device.

```
usgflex200hp running user Max# commit
Configuration committed.
```

28.5.3 User/Group Additional Commands

This table lists additional commands for users.

Table 115 User/Group Additional Commands

COMMAND	DESCRIPTION
`show users`	Displays information about the users logged onto the Zyxel Device.
`show lockout-users`	Displays users who are currently locked out.
`cmd lockout-users unlock ip <IP-Address>`	Unlocks the specified IP address.
`cmd users force-logout {user | ip | service}`	Logs out the specified login.

CHAPTER 29
Addresses

29.1 Address 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.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The Zyxel Device automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, 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.

29.2 Address Command Input Values

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

Table 116 Address Commands Input Values

LABEL	DESCRIPTION
object-name	The name of 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.
group-name	The name of 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.
interface	The name of the interface. This depends on the Zyxel Device model. Use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your Zyxel Device model.

29.2.1 Address Object Commands

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 **CIDR** (Classless Inter-Domain Routing)
- **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

This table lists the commands for address objects. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 117 Address Object Commands: Addresses

COMMAND	DESCRIPTION
`object address-object address <object-name> description <description>`	Enters the description associated with the zone. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are note allowed.
`object address-object address <object-name> type {host IP| cidr cidr| range IP-range| geography country-code| interface-ip interface| interface-subnet interface| interface-gateway interface}`	Creates or edits the specified IPv4 address object using the specified parameters. • IP: Enter an IPv4 address. • IP Range: Enter an IPv4 address range. • CIDR: Enter an IPv4 subnet in CIDR format. For example, 192.168.1.0/32. • Country Code: Enter a country or continent code (represents an IP address for that country/continent). • Interface IP/Interface Subnet/ Interface Gateway: Enter an interface name or virtual interface name.
`show state object address-object address`	Displays the status of the address object settings, such as the address object type, interface, IP address and the number of times an address object is used in other settings.
`show config object address-object address`	Displays the address object settings you configured, such as the address object description, type, interface and IP address.

29.2.1.1 Address Object Command Examples

The following example creates IPv4 address objects.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address Example1 type host
192.168.1.1
usgflex200hp running config# object address-object address Example2 type cidr
192.168.1.0/24
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object address-object address Example1
address Example1 type host 192.168.1.1
usgflex200hp running config# show config object address-object address Example2
address Example2 type cidr 192.168.1.0/24
```

29.2.2 Address Group Commands

This table lists the commands for address groups. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 118 Address Object Commands: Groups

COMMAND	DESCRIPTION
`object address-object group <group-name>`	Creates the specified address group and enters sub-command mode.
`object address-object group <group-name> description <description>`	Sets the description to the specified value. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`object address-object group <group-name> address-list <address-object>`	Adds the specified address to the specified address group.
`object address-object group <group-name> group-list <group-name>`	Adds the specified address group to the address group you're configuring.
`show config object address-object group`	Displays the address group settings you configured, such as the address group name and the address included in the address group.
`show state object address-object group`	Displays the status of the address group settings, such as the address group name, the address included in the address group and he number of times an address group is used in other settings.

29.2.2.1 Address Group Command Examples

The following commands create address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address A0 type host 192.168.1.1
usgflex200hp running config# object address-object address A1 type range
192.168.1.2-192.168.2.20
usgflex200hp running config# object address-object address A2 type cidr
192.168.3.0/24
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# object address-object group RD
usgflex200hp running group RD# address-list A0 address-list A1 address-list A2
usgflex200hp running group RD# commit
Configuration committed.
usgflex200hp running group RD# exit
usgflex200hp> show config object address-object group
group RD
    address-list A0
    address-list A1
    address-list A2
```

29.2.3 Address FQDN Commands

This table lists the commands for address objects of type FQDN. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 119 Address Object Commands: FQDN

COMMAND	DESCRIPTION
`object address-object fqdn enabled {true| false}`	Enables or disables the address objects of type FQDN from querying IP addresses. You may disable this for debugging.
`object address-object address <object-name> type fqdn <fqdn_name> expire_ttl {true| false}`	Creates or edits an address object of type FQDN using the specified parameters: • FQDN: Enter the FQDN of the website that this address object represents. You can enter a wildcard in the first position. For example, '*.zyxel.com'. • Expire TTL: Enable this to automatically clear the cache when the duration for storing a DNS record in the DNS cache has expired. Disable this if you want to keep the DNS record in the DNS cache after it has expired.
`object address-object fqdn query-period <1..1440>`	Sets how often (1 to 1440 minutes) the Zyxel Device should query the IPv4 address of an address object of type FQDN.
`cmd object address-object fqdn flush-cache`	Clears all DNS records in the DNS cache.
`show state object address-object address <object-name>`	Displays the address type, the number of times it was referenced, and the FQDN the object represents.
`show object address-object fqdn wildcard <object-name>`	Displays whether the address object is an FQDN type with a wildcard.

29.2.4 Geo IP

Use these commands to update the database of country-to-IP address mappings and manually configure custom country-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.

29.2.5 Geo IP Commands

Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 120 Geo IP Commands

COMMAND	DESCRIPTION
`geoip database-update auto {true| false}`	Enables the Zyxel Device to automatically check for the latest country-to-IP-address database version on myZyxel.com and allows it to be automatically updated when there is newer version available.
`geoip database-update weekly {mon| tue| wed| thu| fri| sat| sun}`	Specifies the weekly day the Zyxel Device should check for the latest country-to-IP-address database version on myZyxel.com if automatic checking is enabled.
`geoip database-update time`	Specifies the time the Zyxel Device should check for the latest country-to-IP-address database version on myZyxel.com if automatic checking is enabled.

Table 120 Geo IP Commands (continued)

COMMAND	DESCRIPTION
`geoip customize rule <rule-name> ip-type {host IP| range IP-range| cidr cidr} cc-type {continent continent| country country}`	Creates or edits a Geo IP rule using the specified parameters. • IP: Enter an IPv4 address. • IP Range: Enter an IPv4 address range. • CIDR: Enter an IPv4 subnet in CIDR format. For example, 192.168.1.0/32. • Country/Continent: Enter a country or continent code to maps it to the IP address you specified.
`show config geoip database-update {auto | weekly | time}`	Displays if the Zyxel Device is allowed to automatically update to the latest country-to-IP-address database available.
`show config geoip customize rule`	Displays the Geo IP rule settings.

29.2.6 Geo IP Command Examples

The following shows Geo IP command examples.

```
usgflex200hp> edit running
usgflex200hp running config# geoip database-update auto true weekly fri time 22
usgflex200hp running config# geoip customize rule Exmaple1 ip-type host 1.1.1.1
cc-type country AM
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config geoip database-update
database-update auto true weekly fri time 22
usgflex200hp running config# show config geoip customize rule
rule Test cc-type country ZW ip-type host 1.1.1.1
rule Exmaple1 cc-type country AM ip-type host 1.1.1.1
```

CHAPTER 30 Services

30.1 Services Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages that you refer to in features such security policies. You can also create service groups to refer to multiple service objects in other features such as policy routes.

See the appendices in the web configurator's User Guide for a list of commonly-used services.

30.2 Services Commands Input Values

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

Table 121 Service Command Input Values

LABEL	DESCRIPTION
group-name	The name of the service group. This value is case-sensitive. You may use 1-30 single-byte characters, including 0-9a-zA-Z!"#$%'()+,-/;:=?@_, but the first character cannot be a number. &.<>{|}[\]'^are not allowed.
object-name	The name of the service. This value is case-sensitive. You may use 1-30 single-byte characters, including 0-9a-zA-Z!"#$%'()+,-/;:=?@_, but the first character cannot be a number. &.<>{|}[\]'^are not allowed.

30.2.1 Service Object Commands

The first table lists the commands for service objects. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 122 Service Object Commands

COMMAND	DESCRIPTION
`object service-object service <`*`object-name`*`> description <`*`description`*`>`	Enters the description used to refer to the service. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`object service-object service <object-name> type {tcp| udp} {`*`<1...65535>`*`| <`*`1...65535`*`>-<`*`1...65535`*`>}`	Creates the specified TCP service or UDP service using the specified parameters.

Table 122 Service Object Commands (continued)

COMMAND	DESCRIPTION
`object service-object service <object-name> type icmp <icmp-value>`	Creates the specified ICMP message using the specified parameters. `icmp-value`: <0..255> | echo-reply |router-solicitation | time exceeded | parameter problem| timestamp request| timestamp reply| destination unreachable| redirect| echo| router advertisement| any
`object service-object service <object-name> type icmp6 <icmp6-value>`	Creates the specified ICMPv6 message using the specified parameters. `icmp6-value`: <0..255> | destination unreachable| echo request| echo reply| router solicitation| router advertisement| neighbor solicitation| neighbor advertisement| redirect message| packet too big| time exceeded| time exceeded| parameter problem| any
`object service-object service <object-name> type protocol <1...255>`	Creates the specified user-defined service using the specified parameters.
`show config object service-object service`	Displays the service object settings you configured.
`show state object service-object service`	Displays the status of service objects, such as the number of times a service object is used in other settings.

30.2.1.1 Service Object Command Examples

The following commands create four services and displays them.

```
usgflex200hp> edit running
usgflex200hp running config# object service-object service TELNET type tcp
23
usgflex200hp running config# object service-object service FTP type tcp 20-
21
usgflex200hp running config# object service-object service RIP type icmp
any    0      3      5      8      9      10     11     12     13     14
usgflex200hp running config# object service-object service RIP type icmp 5
usgflex200hp running config# object service-object service MULTICAST type
protocol 2
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object service-object service
TELNET
service TELNET type tcp 23
usgflex200hp running config# show config object service-object service FTP
service FTP type tcp 20-21
usgflex200hp running config# show config object service-object service RIP
service RIP type icmp 5
usgflex200hp running config# show config object service-object service
MULTICAST
service MULTICAST type protocol 2
```

30.2.2 Service Group Commands

The first table lists the commands for service groups. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 123 Service Group Commands

COMMAND	DESCRIPTION
`object service-object group <group-name>`	Creates or edits the specified service group and enters sub-command mode.
`object service-object group <group-name> service-list <object-name>`	Adds the specified service to the specified service group.
`object service-object group <group-name> group-list <group-name>`	Adds the specified service group to the service group you're configuring.
`object service-object group <group-name> description <description>`	Enters the description used to refer to the service.You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`show config object service-object group`	Displays the service group settings you configured.
`show state object service-object group`	Displays the status of service groups, such as the number of times a service object is used in other settings.

30.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
usgflex200hp> edit running
usgflex200hp running config# object service-object group ICMP_ECHO
usgflex200hp running group ICMP_ECHO# commit
Configuration committed.
usgflex200hp running group ICMP_ECHO# exit
usgflex200hp> edit running
usgflex200hp running config# object service-object group SG1
usgflex200hp running group SG1# commit
Configuration committed.
usgflex200hp running group SG1# exit
usgflex200hp> edit running
usgflex200hp running config# object service-object group ICMP_ECHO group-
list SG1
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object service-object group
ICMP_ECHO
group ICMP_ECHO
    group-list SG1
```

CHAPTER 31 Schedules

31.1 Schedule Overview

The Zyxel Device supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

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

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 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.

31.2 Schedule Commands Summary

The following table describes the values required for many schedule commands. Other values are discussed with the corresponding commands.

Table 124 Input Values for Schedule Commands

LABEL	DESCRIPTION
object-name	The name of the schedule. You may use 2-30 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group-name	The name of the schedule group. You may use 2-30 alphanumeric characters underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
hh:mm	24-hour time, hours and minutes; <0..23>:<0..59>.

31.2.1 Schedule Commands

The following table lists the schedule commands. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 125 Schedule Commands

COMMAND	DESCRIPTION
`object schedule-object schedule <object-name> description <description>`	Enters the description used to refer to the schedule. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/ :=?;!*#@$_%-" Spaces are not allowed.
`object schedule-object schedule <object-name> type one-time <yyyy-mm-ddThh:mm>~<yyyy-mm-ddThh:mm>`	Creates or updates a one-time schedule.
`object schedule-object schedule <object-name> type recurring <mon| tue| wed| thu| fri| sat| sun Thh:mm>~<mon| tue| wed| thu| fri| sat| sun Thh:mm>`	Creates or updates a recurring schedule.
`show config object schedule-object schedule`	Displays the schedule settings.
`show state object schedule-object schedule`	Displays the status of the schedule, such as the number of times a schedule is used in other settings.

31.2.2 Schedule Command Examples

The following commands create recurring schedule Schedule1 and one-time schedule Schedule2.

```
usgflex200hp running config# exit
usgflex200hp> edit running
usgflex200hp running config# object schedule-object schedule Schedule1 type
recurring monT08:00~wedT08:00
usgflex200hp running config# object schedule-object schedule Schedule2 type
one-time 2022-11-04T08:00~2022-11-04T15:00
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object schedule-object schedule
schedule Config1 type one-time 2000-08-10T10:00~2000-08-10T12:00
schedule Schedule1 type recurring monT08:00~wedT08:00
schedule Schedule2 type one-time 2022-11-04T08:00~2022-11-04T15:00
```

31.2.3 Schedule Group Commands

The following table lists the schedule group commands. Use schedule groups when you want to apply several schedules to a rule, such as a security policy.

Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 126 Schedule Group Commands

COMMAND	DESCRIPTION
`object schedule-object group <group-name> description <description>`	Enters a description of the schedule group.You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/ :=?;!*#@$_%-" Space are allowed.
`object schedule-object group <group-name> schedule-list <object-name>`	Adds the specified schedule to the specified schedule group.
`object schedule-object group <group-name> group-list <group-name>`	Adds the specified schedule group to the schedule group you're configuring.
`show config object schedule-object group`	Displays the schedule group settings.
`show state object schedule-object group`	Displays the status of the schedule group, such as the number of times a schedule group is used in other settings.

31.2.4 Schedule Group Command Examples

The following commands create schedule group Group1 and Group2, then add Group 2 to Group1.

```
usgflex200hp> edit running
usgflex200hp running config# show config object schedule-object schedule
schedule Config1 type one-time 2000-08-10T10:00~2000-08-10T12:00
schedule Schedule1 type recurring monT08:00~wedT08:00
schedule Schedule2 type one-time 2022-11-04T08:00~2022-11-04T15:00
usgflex200hp running config# object schedule-object group Group1 schedule-
list Schedule1
usgflex200hp running config# object schedule-object group Group2 schedule-
list Schedule2
usgflex200hp running config# object schedule-object group Group1 group-list
Group2
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object schedule-object group
group Group1
    schedule-list Schedule1
    group-list Group2
    ..
group Group2
    schedule-list Schedule2
```

CHAPTER 32
AAA Server

32.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of AAA servers 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.

32.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

32.2.1 AD Server Group Commands

The following table lists the commands you use to configure a group of AD servers

Table 127 AD Server Group Commands

COMMAND	DESCRIPTION
`aaa group server ad <profile-name>`	Sets a descriptive name for identification purposes. It must begin with a letter and may use up to 31 single-byte characters, including 0-9a-zA-Z_-. Spaces are not allowed.
`aaa group server ad <profile-name> description <description>`	Enter the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`aaa group server ad <profile-name> port <port>`	Sets the AD port number. Enter a number between 1 and 65535. The default is 389.

Table 127 AD Server Group Commands (continued)

COMMAND	DESCRIPTION
`aaa group server ad <profile-name> ssl {true| false}`	Enables the Zyxel Device to establish a secure connection to the AD server. The `false` command disables this feature.
`aaa group server ad <profile-name> case-sensitive {true| false}`	Enables this to have the server checks the case of the usernames. The `false` command disables this feature.
`aaa group server ad <profile-name> group-attribute <group-identifier>`	Enter the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
`aaa group server ad <profile-name> binddn <binddn>`	Sets the user name the Zyxel Device uses to log into the default AD server.
`aaa group server ad <profile-name> binddn-base <binddn>`	`binddn` is the user name plus `binddn-base`. The default `binddn-base` is: cn=Users,dc=zyxel,dc=com. This is an example `binddn-base` entry: ou=adminGroup,dc=zyxel,dc=com. The user must be located in the adminGroup organization unit, in the zyxel.com domain.
`aaa group server ad <profile-name> password-shadow <password>`	Sets the bind password. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the `show config aaa group server ad` command, the encrypted password displays.
`aaa group server ad <profile-name> cn-identifier <uid>`	Sets the type of identifier the users are to use to log in. The default is sAMAccountName.
`aaa group server ad <profile-name> alternative-cn-identifier <uid>`	Enter a second type of identifier that the users can use to log in if there is one.
`aaa group server ad <profile-name> search-time-limit <1...300>`	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.
`aaa group server ad <profile-name> host <ad-server>`	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name.
`aaa group server ad <profile-name> domain-name <domain-name>`	Sets the domain name to which AD server belongs. The Zyxel Device uses this to access the AD server.
`aaa group server ad <profile-name> username <user-name>`	Sets the user name that the Zyxel Device uses to access the AD server.
`show config aaa group server ad`	Displays the AD server profiles settings.
`show state aaa group server ad`	Displays the status of the AD server profile settings, such as the number of times an AD server profile is used in other settings.
`show aaa ad-domain-auth-status`	Displays the authentication status of the AD domain.
`cmd aaa join-ad-domain`	Adds the Zyxel Device to the currently configured AD domain. Note: The Zyxel Device can only join one AD domain at a time. Adding a new AD domain will replace existing domain associations. Note: Ensure that the Domain Zone Forwarder configuration is correct before joining a domain.
`cmd aaa leave-ad-domain`	Removes the Zyxel Device from the AD server domain.

Table 127 AD Server Group Commands (continued)

COMMAND	DESCRIPTION
`aaa join-ad-domain ad-profile <profile-name>`	Adds the Zyxel Device to a specific AD domain. Enter the profile name of the AD domain you want to join. You can only use this command when your user type is admin.
`aaa join-ad-domain ad-netbios-name <netbios-name>`	Sets the NetBIOS domain name of the AD domain for the Zyxel Device to join. You can only use this command when your user type is admin, but it is required by the AD server.
`aaa join-ad-domain ad-admin-name <user-name>`	Sets the user name for the Zyxel Device to join the AD domain. You can use 1-20 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". You can only use this command when your user type is admin.
`aaa join-ad-domain ad-admin-password-shadow <password>`	Sets the password associated with the user name. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the `show config aaa join-ad-domain` command, the encrypted password displays. You can only use this command when your user type is admin.

32.2.2 LDAP Server Group Commands

The following table lists the commands you use to configure a group of LDAP servers.

Table 128 LDAP Server Group Commands

COMMAND	DESCRIPTION
`aaa group server ldap <profile-name> description <description>`	Enters the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`aaa group server ldap <profile-name> basedn <based`n`>`	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies a LDAP directory.
`aaa group server ad <profile-name> port <port>`	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389.
`aaa group server ldap <profile-name> ssl {true| false}`	Enables the Zyxel Device to establish a secure connection to the LDAP server. The `false` command disables this feature.
`aaa group server ldap <profile-name> case-sensitive {true| false}`	Enables this to have the server checks the case of the usernames. The `false` command disables this feature.
`aaa group server ldap <profile-name> group-attribute <group-identifier>`	Enters the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
`aaa group server ldap <profile-name> binddn <binddn>`	Sets the DN of the user the Zyxel Device uses to log into the default LDAP server.
`aaa group server ldap <profile-name> password-shadow <password>`	Sets the bind password. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the `show config aaa group server ldap` command, the encrypted password displays.
`aaa group server ldap <profile-name> cn-identifier <uid>`	Sets the unique common name (cn) to identify a record.

Table 128 LDAP Server Group Commands (continued)

COMMAND	DESCRIPTION
`aaa group server ldap <profile-name> alternative-cn-identifier <uid>`	Enters a second type of identifier that the users can use to log in if there is one.
`aaa group server ldap <profile-name> search-time-limit <1...300>`	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.
`aaa group server ldap <profile-name> host <ldap-server>`	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name.
`show config aaa group server ldap`	Displays the LDAP server profiles settings
`show state aaa group server ldap`	Displays the status of the LDAP server profile settings, such as the number of times a LDAP server profile is used in other settings.

32.2.3 OIDC Server Group Commands

An OIDC server passes primary authentication from an Identity Provider (IdP) such as Microsoft or Google to the Captive portal and SSL VPN applications. Users must have a Microsoft Entra ID account (set up by the company administrator) or a Google workspace account. Refer to the Zyxel Account Authentication appendix in the User's Guide.

32.2.3.1 User Authentication and Authorization Flow with OIDC

1. A user visits the Captive portal or SSL VPN login page.
2. The Zyxel Device redirects user to the IdP (with client_id, redirect_uri, scope, and so on.)
3. The user signs in at the IdP.
4. The IdP sends an authorization code to the user's browser using the **Redirect URI**.
5. The Zyxel Device sends the authorization code, client ID, client secret, Redirect URI, and grant_type=authorization_code to a Token Endpoint, a back end API URL on the Identity Provider (IdP).
6. The Zyxel Device receives an ID Token and Access Token from the IdP. The ID Token is used to identify the login user. The Access Token is used to authorize access to the service, such as Captive portal or SSL VPN.
7. The Zyxel Device retrieves the JWKS (JSON Web Key Set), the public keys from the IdP, in order to verify token signatures.
8. The Zyxel Device checks the token signature and claims.
9. If they are valid, the user is logged into the Captive portal or SSL VPN application from step 1.

32.2.3.2 Process Overview for Microsoft Entra ID

This is what you, as the administrator, have to do at the Entra Microsoft portal to set up OIDC for your users. This section is for your reference. These are the menu names and paths used at the time of writing. See the help at the below portal for more up-to-date or more detailed information.

1. Go to *https://entra.microsoft.com/* to create an OIDC Application with a Microsoft Entra ID.

2 In **App registration**, click **New registration**. Configure an **App Name** and **Supported account types**, then click **Register**.

3 In the new registration **Overview**, copy the **Application (client) ID**.

4 Under **Endpoints**, select and copy the beginning of **OpenID Connect metadata document** up to v2.0 as the **Issuer-url**. For example, copy 'https://login.microsoftonline.com/{tenant}/v2.0', where {tenant} is a variable. This will be used in the Zyxel Device web configurator in the **Issuer URL** field.

5 Next, click **Add a certificate or secret**. Under **Client secrets**, click **New client secret**. Type a name in the Description, then click **Add**. Copy the entry under **Value** for the newly created client secret. This will be used as the **Client-Secret** in the Zyxel Device web configurator.

6 Next, in **Overview**, click **Add a Redirect URI**.

7 In **Authentication**, click **Add a platform**, then select a platform such as **Web**.

8 In the Zyxel Device CLI set the `redirect-address` to be where the **OIDC server** can connect to the Zyxel Device. For example:

- For **Captive Portal**, this can be an interface IP, external interface IP, Captive portal redirect FQDN, external FQDN or a DNS record for the Zyxel Device.
- For **SSL VPN**, this can be an external interface IP, external FQDN or an IP address that can connect to the Zyxel Device.

9 Copy the above **Redirect Address** and paste it into **Redirect URI** under **Authentication**.

10 Select **ID tokens used for implicit and hybrid flows**, then click **Configure**.

11 In the Zyxel Device CLI, use the `issuer-url`, `client-id` and `client-secret` you copied from Microsoft Entra ID (above).

32.2.3.3 Process Overview For Google Workspace

This is what you, as the administrator, have to do at Google Workspace to set up OIDC for your users. This section is for your reference. These are the menu names and paths used at the time of writing. See the help at the below portal for more up-to-date or more detailed information.

1 Go to *https://console.cloud.google.com/*.

2 Click **Open project picker**, then **New project**.

3 Enter a **Project name**, **Organization** and **Location**, then click **Create**.

4 Go to your new project, then go to **APIs & Services > OAuth consent.**

5 Enter an **App name**, **User support email**, and then click **Next**.

6 In **Audience** set the user type to **Internal** (recommended), then click **Next**.

7 In **Contact Information,** set your **Email address**, then click **Next**.

8 In **Finish**, read, then select **I agree to the Google API Services: User Data Policy**, click **Continue**, and then click **Create**.

9 Next, in **Overview**, click **Create OAuth client**.

10 Set an **Application type** such as **Web application**, and then enter the **Name** of the OAuth client. This is used as the **Client ID** in the Zyxel Device web configurator to identify an app to the Google OAuth servers.

11 In the Zyxel Device CLI set the `redirect-address` to be where the **OIDC server** can connect to the Zyxel Device. FQDN is required for Google. For example:

- For **Captive Portal**, this can be the Captive portal redirect FQDN, external FQDN or a DNS record for the Zyxel Device.
- For **SSL VPN**, this can be an external FQDN or a DNS record for the Zyxel Device.

12 Copy the **Redirect Address** above and enter it as a URL under **Authorized redirect URIs.**

13 Next click the Edit Client icon and copy the **Client ID** and **Client secret**.

14 In the Zyxel Device CLI, use the `issuer-url`, `client-id` and `client-secret` you copied from Google Workspace (above). Set the `issuer-url` as *https://accounts.google.com*.

Use these commands to create a new OIDC server entry or edit an existing one.

Table 129 OIDC Server Group Commands

COMMAND	DESCRIPTION
`aaa group server oidc <server-name>`	Sets the name of the OIDC server. Use up to 31 single-byte characters, including the following characters within the square brackets: [0-9a-zA-Z_-]. 'local' and 'cloud-auth' are reserved names.
`aaa group server oidc <server-name> description <description>`	Sets the description of the OIDC server. Use up to 512 single-byte printable characters, including the following characters within the square brackets: [0-9a-zA-Z'()+,/:=?;!*#@$_%-"].
`aaa group server oidc <server-name> issuer-url <url>`	Sets the URL that uniquely identifies the OIDC server. This is the address from which the Zyxel Device retrieves the configuration and public keys for the Captive portal or SSL VPN user login. It must begin with “https://” and have a maximum of 256 single-byte characters. Examples are: • https://accounts.google.com • https://login.microsoftonline.com/{tenant}/v2.0 • https://mycompany.auth0.com/ • https://idp.company.com/.
`aaa group server oidc <server-name> client-id <id>`	Sets the a public identifier ‘user name’ for your Captive portal or SSL VPN application. This is for the OIDC server to identify which application is making requests. It must be between 10 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z._-]. This is an example: ssl-vpn-client
`aaa group server oidc <server-name> client-secret-shadow <secret>`	Uses the `client-secret-shadow` command followed by the secret in plain text, to encrypt this secret in a saved configuration file. The OIDC server stores the secret shadow to verify client authentication instead of the real plain text client secret. The plain text client secret is discarded. The shadow cannot be reversed to obtain the original secret. Valid characters include the following characters within the square brackets: [0-9a-zA-Z`~!@#$%^&*()_-+={}|;:<>,./"'\] The secret requires: • From 6 to 63 characters • At least 1 upper case letter • At least 1 digit • At least 1 special character.

Table 129 OIDC Server Group Commands (continued)

COMMAND	DESCRIPTION
`aaa group server oidc <server-name> client-secret <encrypted-secret>`	Sets the secret for application verification on the specified OIDC server. Uses the `client-secret` command followed by the encrypted secret, to save this encrypted secret in a saved configuration file.
`aaa group server oidc <server-name> additional-scope <scope>`	Tells the IdP what data and permissions the client is requesting. The scope openid is required by default, and email is recommended. Separate scopes with spaces. Other examples are: • email: get user's email • phone: get user's telephone number • address: get user's mailing address • profile: get user's profile • groups: map groups to local user roles • offline_access: allow long-lived sessions using refresh tokens
`aaa group server oidc <server-name> user-attr-name <name>`	Sets the user name claim for login. It must be in the claims. When a user authenticates through OIDC, the IdP sends an ID Token, which is a JSON Web Token (JWT) containing user attributes called claims. The **Login Name Attribute** tells the Zyxel Device which claim should be used as the user's username to identify the user. Typical values include: • Microsoft Entra ID: preferred_username (recommended), name, upn (User Principal Name), email, oid (Object ID) • Google: name (recommended), email The name must match the external user name pattern and be between 1 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z`~!@#$%^&*()_-+={}|;:<>,./"'\]. Spaces are allowed but are replaced by underlines.
`aaa group server oidc <server-name> redirect-address <ipv4 | fqdn>`	Sets the IP address or FQDN to where the OIDC server sends an authorization code (or token) after the user successfully signs in at an Identity Provider (IdP) such as Microsoft or Google. You must copy this exact URL into the Identity Provider's **Allowed Redirect URIs** during app registration.
`cmd aaa validate-oidc-profile <name>`	Tests login to the specified OIDC server with the above settings. If the login fails, check and edit the above settings.

32.2.4 RADIUS Server Group Commands

The following table lists the commands you use to configure a group of RADIUS servers.

Table 130 RADIUS Server Group Commands

COMMAND	DESCRIPTION
`aaa group server radius <profile-name> description <description>`	Sets the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`aaa group server radius <profile-name> key-shadow <secret>`	Sets a password (up to 63 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device.
`aaa group server radius <profile-name> timeout <1...300>`	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.

Table 130 RADIUS Server Group Commands (continued)

COMMAND	DESCRIPTION
`aaa group server radius <profile-name> group-attribute <group-identifier>`	Sets the name and number of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
`aaa group server radius <profile-name> case-sensitive {true| false}`	Lets the server check the case of the usernames. The `false` command disables this feature.
`aaa group server radius <profile-name> host <radius-server>`	Sets the RADIUS server address. Enter the IP address (in dotted decimal notation) or the domain name.
`aaa group server radius <profile-name> acct-secret <secret>`	Sets a password (up to 63 alphanumeric characters) as the key to be shared between the RADIUS accounting server and the Zyxel Device. This key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
`aaa group server radius <profile-name> acct-retry-count <0...10>`	Specifies 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. The default value is 3. For example, you set this value to 5. If the Zyxel Device does not get a response from the primary RADIUS server, it tries again up to five times. If there is no response, the Zyxel Device tries the secondary RADIUS server up to five 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.
`aaa group server radius <profile-name> acct-interim {true| false}`	Enables to have the Zyxel Device send subscriber status updates to the RADIUS server at the interval you specify.
`aaa group server radius <profile-name> acct-interim-interval <1...1440>`	Specifies the time interval in minutes for how often the Zyxel Device is to send a subscriber status update to the RADIUS server.
`aaa group server radius <profile-name> nas-ip <ipv4>`	Sets the IPv4 address of the NAS (Network Access Server). The default IP is 127.0.0.1.
`aaa group server radius <profile-name> nas-id <id>`	Specifies the NAS (Network Access Serve) identifier attribute.
`show config aaa group server radius`	Displays the RADIUS server profiles settings
`show state aaa group server radius`	Displays the status of the RADIUS server profile settings, such as the number of times a RADIUS server profile is used in other settings.

32.2.5 AAA Group Server Command Examples

The following example shows you how to:

- Set the server host to 172.21.10.100 and authentication port to 1800.

- Set the secret key and timeout period of a RADIUS server group to “876543210” and 80 seconds.

```
usgflex200hp> edit running
usgflex200hp running config# aaa group server radius Profile1 key-shadow
876543210
usgflex200hp running config# aaa group server radius Profile1 timeout 80
usgflex200hp running config# aaa group server radius Profile1 host
172.21.10.100 auth-port 1800
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 33
Authentication Objects

33.1 Admin Two-Factor Authentication

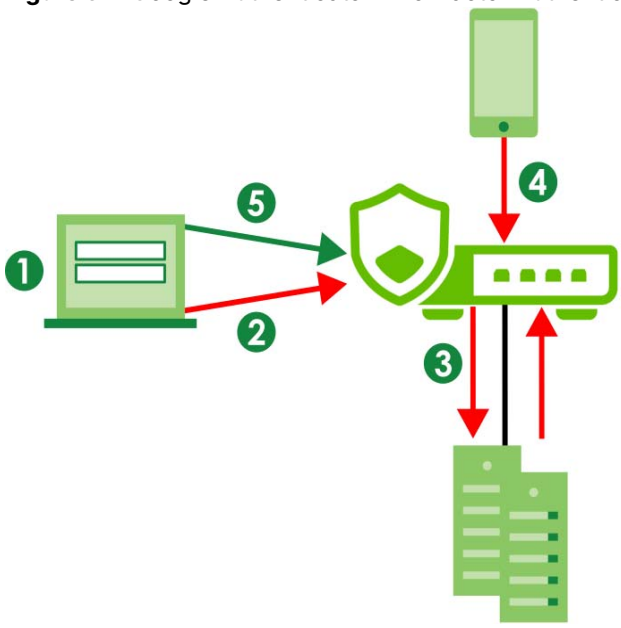
Two-factor authentication adds an extra layer of security for users logging into the Zyxel Device. When two-factor authentication is enabled, a user has to first enter their username and password, and then enter a one-time password when logging in.

You can enable two-factor authentication for administrators who are logging into the Web Configurator or CLI to configure the Zyxel Device.

33.1.1 Two-Factor Authentication with Google Authenticator

This section introduces how Google Authenticator two-factor authentication works.

Figure 97 Google Authenticator Two-Factor Authentication



Admin Access (Web Configurator, SSH)

The following steps explain the procedure when an admin logs into the Zyxel Device.

1 An admin connects to the Zyxel Device through the Web Configurator or SSH.

2 The Zyxel Device requests the admin's username and password.

3 The Zyxel Device authenticates the admin's username and password using a local Zyxel Device database. If this authentication is successful, the Zyxel Device requests the admin's Google Authenticator code.

4 The admin enters the code displayed in the Google Authenticator app.

5 If the Google Authenticator code is correct, the admin can log into the Zyxel Device.

33.2 Two-Factor Authentication Admin Commands

Use the following commands to configure whether **Web** or **SSH** require two-factor authentication for the admin user.

Table 131 Two-Factor Authentication Admin Access Commands

COMMAND	DESCRIPTION
`two-factor-auth admin-access enabled {true| false}`	`True` requires two-factor authentication to access a secured network behind the Zyxel Device via the Web Configurator or SSH as an admin. The `false` command disables two-factor authentication for admin access.
`two-factor-auth admin-access user-list user <username>`	Adds the specified admin user accounts to the two-factor authentication user list to require two-factor authentication when they log in.
`two-factor-auth admin-access valid-time <1...5>`	Sets the maximum time (1-5 minutes) that the admin must enter the code displayed in the Google Authenticator app in order to get authorization for logins via the Web Configurator or SSH.
`two-factor-auth admin-access service {web| ssh}`	Sets which services require two-factor authentication for the admin.
`cmd two-factor-auth google-auth user <username> verify-code <verification-code>`	Verifies whether the code currently displayed in the Google Authenticator app is correct or not to confirm the admin account is binded to the correct Google Authenticator account. The Zyxel Device also creates a temporary secret key file if one does not already exist.
`cmd two-factor-auth google-auth user <username> backup-code create`	Generates new Google Authenticator backup codes. All previously generated backup codes become invalid. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`cmd two-factor-auth google-auth user <username> revoke`	Unbinds the specified admin account in the Google Authenticator app.
`show two-factor-auth user <username> qrcode`	Displays the Google Authenticator QR code for this account. You can link this user account with Google Authenticator by pressing **Enter Provided Key** in the Google Authenticator app.
`show two-factor-auth user <username> backup-code`	Displays the Google Authenticator backup codes for this user account. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`show config two-factor-auth admin-access`	Displays the two-factor authentication settings.
`show state two-factor-auth admin-access`	Displays the two-factor authentication settings and hits.

33.2.1 Admin Access Two-Factor Command Examples

The following example shows how to set up two-factor authentication for an admin.

33.2.1.1 Admin Access Two-Factor Command Example: Email

Follow the steps below to enable two-factor authentication for a Zyxel Device account. The example uses the parameters below.

Table 132 Admin Account Example

USER NAME	PASSWORD	USER TYPE
Mary	1234	admin

Table 133 Two-Factor Authentication Settings Example

AUTHENTICATION METHOD	VALID TIME
Google Authenticator	5 minutes

1 Create an admin account using the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object admin Mary role admin
usgflex200hp running config# object user-object admin Mary password
Enter value for password>
Confirm value for password>
usgflex200hp running config# commit
Configuration committed.
```

2 Enable two-factor authentication for the admin account **Mary**.

```
usgflex200hp running config# two-factor-auth admin-access user-list user Mary
```

3 Configure the two-factor authentication settings using the parameters given above.

```
usgflex200hp running config# two-factor-auth admin-access enabled true
usgflex200hp running config# two-factor-auth admin-access valid-time 5
```

4 Save the current configuration to the Zyxel Device.

```
usgflex200hp running config# commit
Configuration committed.
```

5 Link the account **Mary** with your Google Authenticator account by pressing **Enter Provided Key** in the **Google Authenticator** app.

```
usgflex200hp# cmd two-factor-auth google-auth user Mary verify-code xxxxxx
```

33.3 Two-Factor Authentication VPN Access Commands

Use the following commands to configure whether local users authenticated on the Zyxel Device require two-factor authentication for IPSec / SSL VPN tunnel remote access.

Table 134 Two-Factor Authentication VPN Access Commands

COMMAND	DESCRIPTION
`two-factor-auth vpn-access enabled {true | false}`	`True` requires two-factor authentication to remotely access an IPSec / SSL VPN tunnel for local users authenticated on the Zyxel Device. The `false` command disables two-factor authentication for IPSec / SSL VPN tunnel remote access.
`two-factor-auth vpn-access auth-link http-type {http | https}`	Specifies whether the two-factor authentication link that the user receives should be http or https.
`two-factor-auth vpn-access auth-link auth-interface <interface>`	Specifies the interface on which to receive two-factor verification from the user.
`two-factor-auth vpn-access auth-link auth-url {domain name | ipv4 address | ipv6 address}`	Specifies the domain name or IPv4 address in the two-factor authentication link sent to the user. An IPv6 address is not yet supported.
`two-factor-auth vpn-access auth-link port <1...65535>`	Specifies the port to use for the two-factor authentication link sent to the user.
`two-factor-auth vpn-access valid-time <1...5>`	Sets the maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization for IPSec / SSL VPN tunnel remote access.
`two-factor-auth vpn-access service {ike | sslvpn | service} enabled {true | false}`	`True` requires two-factor authentication for IPSec / SSL VPN tunnel remote access for local users authenticated on the Zyxel Device using the selected service.
`two-factor-auth vpn-access service {ike | sslvpn | service} valid-time <1...5>`	Sets the maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization for IPSec / SSL VPN tunnel remote access.
`cmd two-factor-auth google-auth user <username> verify-code <verification-code>`	Verifies whether the code currently displayed in the Google Authenticator app is correct or not to confirm the admin account is binded to the correct Google Authenticator account using the selected service. The Zyxel Device also creates a temporary secret key file if one does not already exist.
`cmd two-factor-auth google-auth user <username> backup-code create`	Generates new Google Authenticator backup codes. All previously generated backup codes become invalid. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`cmd two-factor-auth google-auth user <username> revoke`	Unbinds the specified admin account in the Google Authenticator app.
`show two-factor-auth google-auth user <username> qrcode`	Displays the Google Authenticator QR code for this account. You can link this user account with Google Authenticator by pressing **Enter Provided Key** in the Google Authenticator app.
`show two-factor-auth google-auth user <username> backup-code`	Displays the Google Authenticator backup codes for this user account. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.

Table 134 Two-Factor Authentication VPN Access Commands (continued)

COMMAND	DESCRIPTION
`show two-factor-auth google-auth qrcode backup-code`	Displays the Google Authenticator backup codes for this Google Authenticator QR code. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`show two-factor-auth google-auth backup-code qrcode`	Displays the Google Authenticator QR code for this Google Authenticator backup code.
`show config two-factor-auth vpn-access user-list`	Displays configured local users that require two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
`show config two-factor-auth vpn-access enabled`	Displays whether two-factor authentication to remotely access an IPSec / SSL VPN tunnel is configured.
`show config two-factor-auth vpn-access valid-time`	Displays the configured maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization to remotely access an IPSec / SSL VPN tunnel.
`show state two-factor-auth vpn-access users`	Displays the runtime status of local users that require two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
`show state two-factor-auth vpn-access enabled`	Displays the runtime status of two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
`show state two-factor-auth vpn-access valid-time`	Displays the runtime status of maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization to remotely access an IPSec / SSL VPN tunnel.

CHAPTER 34 Certificates

34.1 Certificates Overview

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

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

34.2 Certificates Commands Input Values

The following table explains the values you can input with the certificate commands.

Table 135 Certificates Commands Input Values

LABEL	DESCRIPTION
certificate-name	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
cn-ipv4-address	A common name IP version 4 address identifies the certificate's owner.
cn-fqdn	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
cn-email	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
organizational-unit	Identifies the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, hyphen (-) and underscore (_).
organization	Identifies 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.
country-code	A two-letter country code, which identifies the nation where the certificate owner is located. For example US, UK, ES, FR.

Table 135 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
key-type	Encryption algorithms: • **RSA**: Rivest, Shamir and Adleman public-key algorithm. • **DSA**: Digital Signature Algorithm public-key algorithm. • **ECDSA**: Elliptic Curve Digital Signature Algorithm. Signature hash algorithms: • SHA256 • SHA384 • SHA512 RSA and SHA256 are less secure but more compatible with different clients and applications. ECDSA and SHA512 are more secure but less compatible.
extend-key	Extended key usage: • **serverAuth**: Uses this to have the Zyxel Device generate and sore a request for server authentication certificate. • **clientAuth**: Uses this to have the Zyxel Device generate and store a request for client authentication certificate. • **ikeIntermediate**: Uses this to have the Zyxel Device generate and store a request for IKE intermediate authentication certificate.
key-length	Specifies the length of the key, in bits. Allowed values:. • ECDSA: 256, 384 • RSA/DSA: 512, 768, 1024, 1536, 2048, 4096 Typically, the longer the key, the more secure it is. A longer key also uses more PKI storage space. ECDSA keys are significant shorter than RSA and DSA keys, while offering equal or higher security.
city	Identifies the city or town in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example “New York”.
province	Identifies the state, province, or region in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example “New Mexico”.
valid-years	Sets how long the certificate is valid, in years. The value must be between 1 and 10. Note: Software such as web browsers might not trust a certificate that has a long lifetime.

34.3 Certificates Commands

The following table lists the commands that you can use to display and manage the Zyxel Device's summary list of certificates and certification requests. You can also create certificates or certification requests.

Table 136 Certificate Commands

COMMAND	DESCRIPTION
`cmd certManager generate self-signed {name` ***`certificate-name`*** `| country` ***`country-code`*** `| state` ***`province`*** `| locality` ***`city`*** `| organization` ***`organization`*** `| organization-unit` ***`organization-unit`*** `| valid-years` ***`1...10`*** `} cn {fqdn` ***`cn-fqdn`*** `| ip` ***`cn-ipv4-address`*** `| email` ***`cn-email`*** `} key-type {ECDSA| RSA| DSA} key-len <`***`key-length`***`> extend-key {serverAuth| clientAuth| ikeIntermediate}`	Creates a self-signed certificate. `key-type`: Sets the certificate's encryption algorithm and signature hash algorithm. `extend-key`: Adds extended use cases for the certificate. The choices are: • `serverAuth`: Has the Zyxel Device generate and store a request for server authentication certificate. • `clientAuth`: Has the Zyxel Device generate and store a request for client authentication certificate. • `ikeIntermediate`: Has the Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
`cmd certManager generate signing-request {name` ***`certificate-name`*** `| country` ***`country-code`*** `| state` ***`province`*** `| locality` ***`city`*** `| organization` ***`organization`*** `| organization-unit` ***`organization-unit`*** `} cn {fqdn` ***`cn-fqdn`*** `| ip` ***`cn-ipv4-address`*** `| email` ***`cn-email`*** `} key-type {ECDSA| RSA| DSA} key-len <`***`key-length`***`> extend-key {serverAuth| clientAuth| ikeIntermediate}`	Generates a certificate request. `key-type`: Sets the certificate's encryption algorithm and signature hash algorithm. `extend-key`: Adds extended use cases for the certificate. The choices are: • `serverAuth`: Has the Zyxel Device generate and store a request for server authentication certificate. • `clientAuth`: Has the Zyxel Device generate and store a request for client authentication certificate. • `ikeIntermediate`: Has the Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
`cmd certManager delete {certificate| trusted-certificate} name <`***`certificate-name`***`>`	Deletes the specified certificate. The Zyxel Device keeps all of your certificates unless your specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.
`cmd certManager certificate-mail send-now file-name <`***`certificate-name`***`> subject <`***`email-subject`***`> recipient <`***`recipient-address`***`> content <`***`email-content`***`>`	Sends a certificate to the specified email address. • `certificate-name`: Sets the name of the certificate you want to send. • `email-subject`: Sets the subject line for the outgoing email. It can contain 1 to 60 characters. It can include letters, numbers, and the following special characters: '()+,./ :=?;!*#@$%-." • `recipient-address`: Sets the email address to which the outgoing email is delivered. It can contain up to 83 characters. • `email-content`: Sets the email content in English. It can use up to 250 keyboard characters. The following special characters are allowed: [0-9a-zA-Z!"#$%&'()*+,-./ :;<=>@\[]^_'{}|]. Spaces are not allowed.

Table 136 Certificate Commands (continued)

COMMAND	DESCRIPTION
`show certManager {certificate| trusted-certificate} {certpath name` ***certificate-name*** `| name| raw name` ***certificate-name*** `| base64 name` ***certificate-name*** `| json name` ***certificate-name*** `}`	Displays the certificate in the form you specified. For example, if you enter `show certManager base64 name` ***certificate-name***, you will see the certificate you specified in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters and numerals to convert a binary certificate into a printable form.
`show state certManager`	Displays the certificate settings and the percentage of the Zyxel Device's PKI storage space that is currently in use.

34.4 Certificates Commands Examples

The following example creates a self-signed certificate with FQDN www.zyxel.com as the common name. It uses the RSA key type with SHA256.

```
usgflex200hp> edit running
usgflex200hp running config# cmd certManager generate self-signed name Example
valid-years 2 cn fqdn www.zyxel.com key-type RSA sha256 key-len 512
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show certManager certificate name Example
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            62:96:ad:db:72:08:ef:fc:de:e1:a2:07:5b:b5:ab:89:a7:84:e0:c7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.zyxel.com
        Validity
            Not Before: Mar 16 08:58:53 2023 GMT
            Not After : Mar 15 08:58:53 2025 GMT
        Subject: CN = www.zyxel.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (512 bit)
                Modulus:
                    00:b1:05:73:43:83:cb:6e:66:88:c7:2d:83:08:eb:
                    86:35:fd:40:ee:49:01:44:e0:71:91:aa:91:e8:6d:
                    8d:95:0f:40:3d:0e:c7:47:5e:cd:62:85:44:9d:a7:
                    91:00:92:8c:85:cd:02:6d:2e:0a:df:77:b3:31:b1:
                    a1:65:24:36:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Subject Key Identifier:
                E6:92:39:DA:71:8D:92:24:02:4E:BF:1B:BE:B4:90:A7:66:3D:16:D4
            X509v3 Key Usage: critical
               Digital Signature, Key Encipherment, Data Encipherment, Certificate
Sign
            X509v3 Subject Alternative Name:
                DNS:www.zyxel.com
    Signature Algorithm: sha256WithRSAEncryption
         6e:47:53:f0:f4:a6:cf:1f:97:39:3c:00:2e:c7:61:ff:6c:03:
         ec:d4:48:b2:4d:12:82:80:2e:c1:40:15:c6:de:da:6f:81:51:
         7e:a2:37:52:cc:21:d1:4c:49:54:b8:71:a7:85:4f:d3:c2:71:
         d6:f1:dc:76:7b:e4:ef:b1:61:f0
```

CHAPTER 35
AP Management

35.1 AP Management Overview

The Zyxel Device allows you to remotely manage all of the Access Points (APs) on your network. You can manage a number of APs without having to configure them individually as the Zyxel Device automatically handles basic configuration for you.

The commands in this chapter allow you to add, delete, and edit the APs managed by the Zyxel Device. An AP must be moved from the wait list to the management list before you can manage it. If you do not want to use this registration mechanism, you can disable it and then any newly connected AP is registered automatically.

35.2 General AP Management Commands

The following table describes the commands available for general AP management. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 137 Command Summary: AP Management

LABEL	DESCRIPTION
`del wlan-setting group <group-name>`	Removes all the APs from the specified group from being managed by the Zyxel Device.
`[del] wlan-setting single-ap <mac-address>`	Sets or removes the WLAN settings for the specified AP. This take priority over the settings for the AP group.
`wlan-setting single-ap <mac-address> override-fullpower-enabled false`	Enable this if your AP is using a PoE injector that does not support PoE negotiation. Otherwise, the AP cannot draw full power from the power sourcing equipment. Enable this power mode to improve the AP's performance in this situation.
`[del] wlan-setting single-ap <mac-address> override-tag <tag-name>`	Assigns or removes a tag for the specified AP. You can assign up to 32 tags to one AP. A tag name can contain 1–32 single-byte characters, including [A–Z], [a–z], [0–9], [@#-_]. You can then assign the AP tag to a WiFi network name (SSID). When the tags of an SSID and an AP in the same group match, the SSID will be broadcast. Note: An AP's tags are removed when you move it to another AP group.
`wlan-setting single-ap <mac-address> sysname <system-name>`	Enter a name to identify the AP on a network.
`wlan-setting single-ap <mac-address> location <location>`	Specify the name of the place where the AP is located.

Table 137 Command Summary: AP Management (continued)

LABEL	DESCRIPTION
`wlan-setting single-ap <mac-address> override-if enabled {true| false}`	Sets when you can override group AP's IP address settings for the specified AP.
`wlan-setting single-ap <mac-address> override-if dhcp {true| false}`	Sets TCP IP assignment method for the specified AP. • `true`: Have the AP act as a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server. • `false`: Specify the IP address, subnet mask, gateway and DNS server address manually.
`wlan-setting single-ap <mac-address> override-if address <ip-address> netmask <netmask> gateway <gateway> dns <dns-server>`	Sets when you can override the following group AP settings for the specified AP. • `ip-address`: Enter an IP address for the AP. • `netmask`: Enter the subnet mask of the AP in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all devices in the network. • `gateway`: Enter the IP address of the gateway. The AP sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the AP. • `dns-server`: Enter the IP address of the DNS server.
`wlan-setting single-ap <mac-address> override-mgnt-vlan enabled {true| false}`	Sets when you can override the group AP's management VLAN for the specified AP.
`wlan-setting single-ap <mac-address> override-mgnt-vlan id <vlan-id>`	Sets when you can override a group AP's VLAN ID for the specified AP.
`wlan-setting single-ap <mac-address> override-mgnt-vlan vlan-tag {tag| untag}`	Sets when you can override group AP's VLAN tag setting for the specified AP. • `tag`: make the Zyxel Device adds the Management VLAN ID to outbound traffic transmitted through its Ethernet port. • `untag`: the outbound traffic transmitted through the Zyxel Device Ethernet port will not be tagged with the Management VLAN ID.
`wlan-setting single-ap <mac-address> override-rogue-ap-setting {true | false}`	Specifies whether the rogue AP detection settings of the AP group can be overridden for the specified managed AP.
`wlan-setting single-ap <mac-address> enabled-rogue-ap {true | false}`	Allows the Zyxel Device to monitor the specified managed AP for rogue AP detection.
`wlan-setting single-ap <mac-address> led-suppress enabled {true | false}`	Sets or disables all LEDs for the specified AP.
`wlan-setting single-ap <mac-address> led-suppress override-led-group-setting {true | false}`	Allows the specified AP `led-suppress` setting (on or off) to override the AP group setting.
`wlan-setting single-ap <mac-address> led-locator blink-timer <1 - 60>`	Sets how often in minutes the AP's Locator LED should blink. It blinks once every 10 minutes by default.

Table 137 Command Summary: AP Management (continued)

LABEL	DESCRIPTION
`wlan-setting single-ap <mac-address> selectable-antenna config {ceiling | wall}`	Adjusts antenna coverage for an AP with a physical antenna switch, depending on whether the specified AP is mounted on a ceiling (default) or a wall.
`wlan-setting single-ap <mac-address> ble slot {n} index {1...5} enabled {true | false}`	Enables or disables the specified beacon (`index`) for the specified Bluetooth Low Energy (BLE) slot (`ble slot`) for the selected AP (`mac-address`). The selected AP needs to have built-in Bluetooth support or have a supported Bluetooth USB dongle connected to it. Bluetooth acts as a beacon to broadcast packets.
`wlan-setting single-ap <mac-address> index {1...5} uuid <string> major {0...65535} minor {0...65535}`	Sets the UUID major and minor numbers for the specified AP. Advertising packets contain a Universally Unique Identifier (UUID) major number and minor number to identify a service, a device, a manufacturer or an owner. The 2-byte major number is to identify and distinguish a group, and the 2-byte minor number is to identify and distinguish an individual.
`wlan-setting single-ap <mac-address> storm-control ethernet {broadcast | multicast} enabled {true | false} pps <1..10000>`	Sets the maximum traffic rate in packets-per-second (pps) for broadcast or multicast traffic received on the AP Ethernet port. Storm control prevents excessive broadcast/multicast traffic on the AP Ethernet port by dropping packets that arrive over the specified pps rate.
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting override-group-setting {true | false}`	Allows you to override the AP group's Smart Mesh setting, so you can manage this AP individually.
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting enabled {true | false}`	Enables or disables Smart Mesh on the specified AP. Smart Mesh is a WiFi network consisting of a controller for management and APs / Repeaters to extend coverage and reduce WiFi dead zones in the coverage area.
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting ap referred-band-mode {auto | 2G | 5G | 6G}`	Sets the preferred wireless band for the specified AP to use. • `auto` allows the specified AP to select the best radio band available in the mesh network. • `2G` uses the 2.4 GHz band radio band in the mesh network. This is good for regular Internet surfing and downloading. • `5G` or `6G` uses the 5 GHz or 6 GHz radio band in the mesh network. This is good for time sensitive traffic like high-definition video, music, and gaming.

Table 137 Command Summary: AP Management (continued)

LABEL	DESCRIPTION
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting mesh-mlo {off | auto | 2.4G+5G | 2.4G+6G | 5G+6G}`	Disables MLO uplink on the specified AP, or sets the preferred wireless bands the specified AP uses for MLO uplink. With MLO (Multi-Link Operation), a WiFi7 client can connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Uplink refers to the connection from the root AP to the Zyxel Device, or from a repeater to the root AP, and so on. • `off` disables MLO. • `auto` allows the specified AP to choose a higher radio band mesh controller. • `2.4G+5G` uses the 2.4 GHz and 5 GHz bands for uplink connection. • `2.4G+6G` uses the 2.4 GHz and 6 GHz bands for uplink connection. • `5G+6G` uses the 5 GHz and 6 GHz bands for uplink connection. Below are the differences between each frequency band. Choose the bands to use based on your network usage. • 2.4 GHz: Long range, slower speed. It is good for regular Internet surfing and downloading. • 5 GHz: Medium range, fast speed. It is good for streaming, video calls. • 6 GHz: Short range, very fast speed. It is good for gaming, VR, and other high-performance use.
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting downlink {true | false}`	Enables or disables other APs from connecting to the specified AP.
`wlan-setting single-ap <mac-address> ap-smart-mesh-setting wireless-bridge-enabled {true | false}`	Allows two Zyxel Devices to automatically bridge two network segments through a WiFi connection. Set this when the Zyxel Device is connected to a root AP, so as to allow traffic through the Ethernet port on the Zyxel Device to a wired network When enabled, the system will automatically create VLAN and bridge interfaces based on the allowed VLANs you configure. The Zyxel Device can continue data transmission through its Ethernet port(s) even after the smart-mesh link is established. Note: Be careful to avoid bridge loops. A bridge loop occurs when there are two layer-2 paths between the same endpoints, causing broadcast packets to be send back and forth indefinitely.
`wlan-setting single-ap <mac-address> wlan-slot 2 zero-wait-dfs {true | false}`	Allows the AP to continue forwarding traffic without interruption during Dynamic Frequency Selection (DFS) events on the 5 GHz band. DFS can cause service interruptions because an AP must pause transmission to scan for radar signals and switch to a different channel when operating on the 5 GHz band. Note: This feature is not supported on all models. You can use `show state apc ap` to check whether your AP supports this feature, and check `zero-wait-dfs` under `sw-capability` to verify support.
`del wlan-setting group <from-group> ap-mac <mac-address>`	Removes the specified AP from the specified AP group.

Table 137 Command Summary: AP Management (continued)

LABEL	DESCRIPTION
`wlan-setting group <to-group> ap-mac <mac-address>`	Moves the specified AP to the specified AP group.
`cmd apc ap-mac <mac-address> reboot`	Restarts the specified AP.
`cmd dcs now <mac-address>`	Sets the specified AP to use DCS (Dynamic Channel Selection) to allow the AP to automatically find a less-used channel in an environment where there are many APs and there may be interference.
`cmd apc ap-mac <mac-address> fw-updating`	Updates the specified APs' firmware.
`cmd apc ap-mac <mac-address> cloud`	Switches the AP to cloud mode, keeping the current IP address and VLAN ID.
`cmd apc ap-mac <mac-address> cloud vlan <vlan-id> {tag| untag} {ip address <ip-address> | netmask <netmask> | gateway <gateway> | dns <dns-server>}`	Switches the AP to cloud mode and sets the following. • `mac-address`: the MAC address of the AP to switch to cloud mode. • `vlan-id`: the new VLAN ID for the AP. • `tag/untag`: whether to tag or untag the VLAN ID. • `ip-address`: the new IP address for the AP. • `netmask`: the subnet mask of the AP. • `gateway`: the IP address of the router through which this AP will send WAN traffic. • `dns-server`: the IP address of the DNS server.
`cmd apc ap-mac <mac-address> factory-default`	Returns the specified AP settings to the factory defaults.
`cmd apc firmware update source {official | <version>}`	Specifies the firmware for updating the managed APs. • `official`: keeps the Zyxel Device prepared with the latest AP firmware for the managed APs. • `version`: uses a specific firmware. Enter the version of the firmware to update the managed APs. For example, 7.20(.2) or 7.20(.2)-DF-2026-03-02. Valid plain text characters are [a-z A-Z 0-9 ()_-.], and the string must include a [(].
`cmd led-locator mac <mac-address> enabled {true | false}`	Sets or disables the Locator LED for the specified AP. The Locator LED will indicate the actual AP among several devices that are together.
`show apc license count`	Displays the number of APs that can be managed with the current license of this Zyxel Device.
`show state apc ap`	Displays detailed information about the APs managed by the Zyxel Device.
`show state apc wait-list`	Displays detailed information about the APs detected but not yet managed by the Zyxel Device.
`show state wlan-security-profile-wpa-psk group`	Displays the group ID and encryption method of the AP group(s).
`show config wlan-setting single-ap <mac-address> ap-smart-mesh-setting`	Displays the Smart Mesh setting on the specified AP. Smart Mesh is a WiFi network consisting of a controller for management and APs / Repeaters to extend coverage and reduce WiFi dead zones in the coverage area
`show apc firmware-update source`	Displays the firmware prepared on your Zyxel Device to update the managed APs. The default is `official`, which means the Zyxel Device keeps the latest firmware prepared for the managed APs.

35.2.1 General AP Management Command Examples

The following command shows the number of APs that can be managed with the current license of this Zyxel Device.

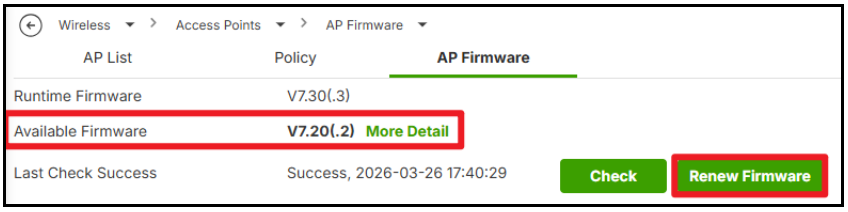
```
usgflex500h running config# show apc license count
get-apc-license-count
    count "Supports 72 AP devices."
    status Success
```

The following example shows how to update a managed AP to a specific firmware version.

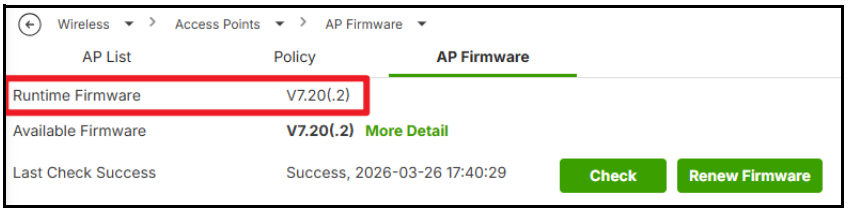
1 Specify the firmware version and check whether the configuration is successful.

```
MyUSGFLEX500H> cmd apc firmware-update source 7.20(.2)
apc-firmware-update-source
    result Success
    ..
MyUSGFLEX500H> show apc firmware-update source
show-apc-firmware-update-source
    source 7.20(.2)
    ..
```

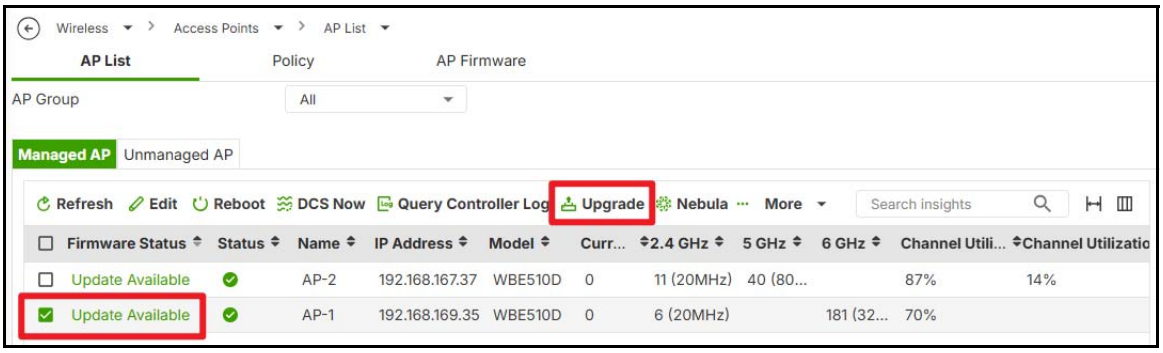
2 Log in to the Web Configuration. Go to **Wireless > Access Points > AP Firmware**. You can see the specified firmware version in the **Available Firmware** field. Click **Renew Firmware**.



3 The specified firmware version is prepared for updating the manged APs.



4 Go to **Wireless > Access Points > AP List**. Select the manged AP(s) that you want to update to the specified firmware version. Click **Upgrade**.



Note: By default, the Zyxel Device keeps the latest AP firmware prepared for managed APs. After you configure a specific AP firmware version, use the `cmd apc firmware-update source official` command to restore the default setting. This setting is also restored after the Zyxel Device reboots

35.3 Wireless Status Commands

The following table describes the commands available to view wireless traffic usage for managed APs and their clients. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 138 Command Summary: Wireless Status

LABEL	DESCRIPTION
`show topn topn-ap ranking {top5-by-usage | top10-by-usage | top5-by-sta | top10-by-sta} metric {usage | station-count} {per-day <yyyy-mm-dd> | per-days start-date <yyyy-mm-dd> end-date <yyyy-mm-dd>}`	Displays data for managed APs according to the specified sorting options and date range. You can sort and display managed AP data using the following options. Top APs sorting options: • `top5-by-usage`: Top five managed APs by traffic usage. • `top10-by-usage`: Top ten managed APs by traffic usage. • `top5-by-sta`: Top five managed APs by number of connected stations (wireless clients). • `top10-by-sta`: Top ten managed APs by number of connected stations. Data type: • `usage`: Traffic usage. • `station-count`: Number of connected stations. Date range: • `per-day` <*yyyy-mm-dd*>: Hourly data for the specified date. Enter *0000-00-00* to display data for the current day. • `per-days start-date` <*yyyy-mm-dd*> `end-date` <*yyyy-mm-dd*>: Daily data for the specified date range. Enter *0000-00-00* for both the start and end dates to display data for the most recent multiple days.
`show topn single-ap mac` <ap-mac-address> `metric {usage | station-count} {per-day` <*yyyy-mm-dd*> `| per-days start-date` <*yyyy-mm-dd*> `end-date` <*yyyy-mm-dd*>`}`	Displays data for the specified managed AP over the specified date range. `ap-mac-address`: The MAC address of the managed AP. Data type: • `usage`: Traffic usage. • `station-count`: Number of connected stations. Date range: • `per-day` <*yyyy-mm-dd*>: Hourly data for the specified date. Enter *0000-00-00* to display data for the current day. • `per-days start-date` <*yyyy-mm-dd*> `end-date` <*yyyy-mm-dd*>: Daily data for the specified date range. Enter *0000-00-00* for both the start and end dates to display data for the most recent multiple days.

Table 138 Command Summary: Wireless Status (continued)

LABEL	DESCRIPTION
`show topn topn-sta ranking {top5-by-usage | top10-by-usage} {per-day <yyyy-mm-dd> | per-days start-date <yyyy-mm-dd> end-date <yyyy-mm-dd>}`	Displays wireless traffic usage for managed AP wireless clients according to the specified sorting options and date range. You can sort and display wireless client data using the following options. Top wireless clients sorting options: • `top5-by-usage`: Top five wireless clients by traffic usage. • `top10-by-usage`: Top ten wireless clients by traffic usage. Date range: • `per-day` <*yyyy-mm-dd*>: Hourly data for the specified date. Enter *0000-00-00* to display data for the current day. • `per-days start-date` <*yyyy-mm-dd*> `end-date` <*yyyy-mm-dd*>: Daily data for the specified date range. Enter *0000-00-00* for both the start and end dates to display data for the most recent multiple days.
`show topn single-sta <station-mac-address> metric usage {per-day <yyyy-mm-dd> | per-days start-date <yyyy-mm-dd> end-date <yyyy-mm-dd>}`	Displays wireless traffic usage for the wireless client over the specified date range. `station-mac-address`: The MAC address of the wireless client. Date range: • `per-day` <*yyyy-mm-dd*>: Hourly data for the specified date. Enter *0000-00-00* to display data for the current day. • `per-days start-date` <*yyyy-mm-dd*> `end-date` <*yyyy-mm-dd*>: Daily data for the specified date range. Enter *0000-00-00* for both the start and end dates to display data for the most recent multiple days.

35.4 AP Client Commands

The following table describes the commands available for AP clients. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 139 Command Summary: AP Clients

LABEL	DESCRIPTION
`[del] wlan-setting macfilter-profile macfilter-`*<groupid>*`-`*<ssid>* `mac` *<mac-address> <mac-wildcard-mask> filter-type* `{allow | block}`	Sets or removes a MAC address filter for the specified WiFi client. You can then sets the MAC filter action on a WiFi Network (SSID) to allow or block the WiFi client from connecting to the SSID. • `groupid`: The ID of the AP group. • `ssid`: The WiFi network to which the policy applies. • `mac-address`: The MAC address of the WiFi client to allow or block. • `mac-wildcard-mask`: The MAC wildcard mask specifies which parts of the MAC address must match for a rule to apply. An F or f in the mask requires an exact match for the corresponding digit. A 0 allows any value for the corresponding digit. For example, a mask of FF:FF:FF:00:00:00 applied to a MAC address of 96:FA:95:1D:67:4A creates a MAC address range of 96:FA:95:00:00:00 to 96:FA:95:FF:FF:FF. The default value is all fs, which represents a specific MAC address. • `allow`: The WiFi client can connect to the WiFi network in the AP group. • `block`: The WiFi client cannot connect to the WiFi network in the AP group.
`show state apc station`	Displays details of the WiFi clients connected to the AP.
`show state apc policy-station`	Displays configured security policies for the AP's WiFi clients.
`show state apc ssidinfo`	Displays the WiFi networks (SSIDs) currently in use and the number of clients connected on each band.

35.5 WiFi Aid and Connection Log Commands

Use the commands in this section to check the connection issues between WiFi clients and managed AP(s) across three connection stages: Wireless, DHCP, and DNS. You can check which connection stage failed to determine the cause of a failed WiFi connection.

Note: Each client is counted as one failed connection attempt, no matter how many connection attempts were made.

Note: A failure at a specific stage indicates that the connection failed at that stage.

Note: At the time of writing, this feature is supported only on WBE530 and WBE665S with firmware version 7.35 or later, and on other models with firmware version 7.40 or later.

At the time of writing, each model supports connection history for the following number of days.

Table 140 WiFi Connection Historical Data by Model

MODEL	LAST X DAY(S)
USG FLEX 50H USG FLEX 50HP USG FLEX 100H USG FLEX 100HP USG FLEX 200H USG FLEX 200HP	1
USG FLEX 500H USG FLEX 700H	7

WiFi Connection Stages

See the three connection stages below and their potential failure causes.

1 Wireless - Client associates with the WiFi network (SSID)

Potential failure causes:

- Client entered the wrong password
- 802.1X Authentication failed
- Client is connected to another AP by functions such as load balancing
- Client is blocked by functions such as legacy client restrictions

Troubleshooting:

- Make sure the client is within transmission range of the manged AP
- Make sure the client is connecting to the correct WiFi network and has entered the correct password
- Make sure the Wi-Fi adapter on the client is functioning properly by trying to connect to another WiFi network

2 DHCP - Client gets the IP address from the network

Potential failure causes:

- DHCP server does not respond (failure/timeout)

Troubleshooting:

- Check that the DHCP server is online is reachable from the Zyxel Device and the correct info is entered on the Zyxel Device
- Increase the number of IP addresses that the DHCP server can allocate
- Shorten the DHCP lease time to free up IP addresses faster for high-turnover networks, such as cafes with guest WiFi

3 DNS - DNS server translates domain names into IP addresses

Potential Failure Causes:

- DNS server does not respond (failure/timeout)

Troubleshooting:

- Check that the DNS server is reachable from the Zyxel Device and the correct info is entered on the Zyxel Device

The following table describes the commands available to check failed WiFi client connections.

Table 141 Command Summary: WiFi Aid and Connection Log

LABEL	DESCRIPTION
`show wifiaid dashboard`	Displays the number of Wi-Fi clients with failed connection attempts by stage (Wireless, DHCP, or DNS), along with the total number of failed attempts and total connection attempts. You can add the following command to filter the displayed data: • `ap-group <ap-group-name>`: Displays data for the specified AP group. Only one AP can be specified. • `time-option <time-range>`: Displays data within the specified time range in the format yyyy-mm-ddThh:mm~yyyy-mm-ddThh:mm. Refer to Table 140 on page 282 for the number of days of historical data supported by each model. • `ssid <ssid-name>`: Displays data of the specified WiFi network (SSID). Only one WiFi network (SSID) can be specified. For example, `show wifiaid dashboard ap-group default time-option 2025-05-29T15:00~2025-05-30T15:00 ssid SSID_1`.
`show wifiaid failed-client`	Displays detailed information about WiFi connection failures to WiFi clients. • Data under `current-result` displays past failed connection attempts only for clients that have not yet successfully connected. • Data under `history-result` displays past failed connection attempts, including those of clients that have successfully connected. You can add the `ap-group`, `time-option`, and `ssid` commands to filter the displayed data. See details above.
`show wifiaid ap`	Displays detailed information about WiFi connection failures to managed APs. You can use the `ap-group`, `time-option`, and `ssid` commands to filter the displayed data. See details above.
`show wifiaid ssid`	Displays detailed information about WiFi networks (SSIDs) with failed WiFi connections. You can add the `ap-group`, `time-option`, and `ssid` commands to filter the displayed data. See details above.

Table 141 Command Summary: WiFi Aid and Connection Log (continued)

LABEL	DESCRIPTION
`show wifiaid connection-log`	Displays detailed logs of connection failure events. You can add the following command to filter the displayed data: • `ap-group <ap-group-name>`: Displays data for the specified AP group. Only one AP can be specified. • `time-option <time-range>`: Displays data within the specified time range in the format yyyy-mm-ddThh:mm~yyyy-mm-ddThh:mm. Refer to Table 140 on page 282 for the number of days of historical data supported by each model. • `ssid <ssid-name>`: Displays data of the specified WiFi network (SSID). Only one WiFi network (SSID) can be specified. • `ap <ap-mac-address>`: Displays data of specified managed AP. Only one AP can be specified. • `client <client-mac-address>`: Displays data of specified client. Only one client can be specified. • `eventtypes {wireless | dhcp | dns}`: Displays data for specified connection failure stages: Wireless, DHCP, or DNS. For example, `show wifiaid connection-log client 02:11:22:33:44:55 eventtypes wireless eventtypes dhcp`.
`show state wifiaid-client`	Displays all clients with failed WiFi connections.

35.5.1 Command Example

The following example shows how to display clients with failed WiFi connections and use the client MAC address to identify the cause by checking the '`message`'.

Figure 98 WiFi Aid Command Example

```
MyUSGFLEX500H> show wifiaid failed-client
wifi-aid-failed-client
    current-result
        client
            client-mac 02:11:22:33:44:55
            client-connection-failed 1
            client-connection-total 1
            client-connection-result wifiaid_wireless
            ap-group -APGroup_test2
            ..
        ..
    history-result
        client
            client-mac 02:11:22:33:44:55
            client-connection-failed 1
            client-connection-total 1
            client-connection-result wifiaid_wireless
            ap-group -APGroup_test2
            ..
        ..
    ..
MyUSGFLEX500H> show wifiaid connection-log client 02:11:22:33:44:55
connection-log-data
    client
        associate-time "2026-04-09 10:47:07"
        client-mac 02:11:22:33:44:55
        ap-description AP-1
        ssid SSID3
        ssid-encode SSID3
        log-status true
        event-type "Wireless connection"
        ap-group -APGroup_test2
        message "Station: 02:11:22:33:44:55 WPA-PSK auth fail."
        ..
    ..
```

35.6 AP Group Commands

The following table describes the commands available for AP groups. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 142 Command Summary: AP Group

LABEL	DESCRIPTION
`[del] wlan-setting group` *<group-name>*	Creates or removes an AP group on the Zyxel Device.
`wlan-setting group` *<group-name>* `description` *<description>*	Sets a description for this AP group. You can use up to 31 characters, spaces and underscores allowed.
`wlan-setting group` *<group-name>* `location` *<location>*	Sets the name of the place where the AP group is located.

Table 142 Command Summary: AP Group (continued)

LABEL	DESCRIPTION
`wlan-setting group <group-name> led-suppress {true | false}`	Sets or disables all LEDs for all APs in the specified AP group.
`wlan-setting group <group-name> group-port-setting port {LAN1 | LAN2 | LAN3}`	Specifies a port in the AP group to configure.
`wlan-setting group <group-name> enabled-rogue-ap enabled {true | false}`	Enables or disables a rogue AP in the AP group. A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.
`wlan-setting group-setting group-info-remind {true | false}`	Enables (`true`) or disables (`false`) display of group messages when there are more than 2 groups.
`wlan-setting group <group-name> wlan-slot {1 | 2 | 3}`	Sets the slot number for the radio profile (1 for 2.4 GHz, 2 for 5 GHz, 3 for 6 GHz in the specified AP group.
`wlan-setting group <group-name> ssids <ssid> ssid ssid-<groupid>-<ssid>`	Sets the AP group ID and SSID name for the specified AP group.
`del wlan-setting group <group-name> ssids <ssid>`	Removes the specified WiFi network (SSID) from the AP group.
`wlan-setting group <group-name> last-modified`	Displays the date and time the AP group was last configured.
`wlan-setting group <group-name> id <group-id>`	Sets the AP group ID for the specified AP group.
`wlan-setting group <group-name> group-port-setting port {LAN1 | LAN2 | LAN3} pvid {1..4094}`	Sets the port's PVID for the specified port and AP group. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
`wlan-setting group <group-name> group-port-setting port {LAN1 | LAN2 | LAN3} allowed-vlan <vlan-id>`	Sets the VLAN ID to which the port belongs. Only the network traffic from the allowed VLANs will be sent or received through this port. You can enter individual VLAN ID numbers separated by a comma or a range of VLANs by using a dash, such as 1, 3, 5–8. The setting can use '0-9,-', but must start with '1-9', and not end with '-,'. The default is 1.
`wlan-setting group <group-name> group-port-setting port {LAN1 | LAN2 | LAN3} enabled {true | false}`	Enables or disables the specified port in the specified AP group.
`wlan-setting group <group-name> group-smart-mesh-setting enabled {true | false}`	Enables or disables Smart Mesh in the specified AP group. Smart Mesh is a WiFi network consisting of a controller for management and APs / Repeaters to extend coverage and reduce WiFi dead zones in the coverage area.

Table 142 Command Summary: AP Group (continued)

LABEL	DESCRIPTION
`wlan-setting group <group-name> group-smart-mesh-setting ethernet-failover {true | false}`	Enables a wired AP connected to the Zyxel Device to change its role from mesh controller to mesh extender if the AP is unable to reach the Zyxel Device. When disabled, a wired AP connected to the Zyxel Device automatically changes its role from mesh controller to mesh extender only if the AP's uplink Ethernet cable is unplugged.
`wlan-setting group <group-name> enabled-rogue-ap {true | false}`	Enables rogue AP detection on all managed APs in the specified AP group.
`wlan-setting group <group-name> led-suppress {true | false}`	Sets or disables all LEDs for the specified AP group.
`show config wlan-setting group default [group-port-setting | group-smart-mesh-setting | load-balancing | wlan-slot | ssids | id | description | location | last-modified | led-suppress | enabled-rogue-ap]`	Displays detailed information of the specified AP group. An AP Group is a group of APs that WiFi clients can move between without losing connection or needing to re-authenticate.

35.6.1 Command Example

The following command displays smart mesh settings for the 'default' AP group. The Zyxel Device generates a unique AP Roaming Group name (`group-uuid`) to distinguish AP Groups with the same **AP Group** name (created in **Wireless > WLAN Settings > AP Group Settings**) that are connected to different Zyxel Devices in the same WiFi coverage area. In the following screen, `chutil` is the channel utility.

Figure 99 AP Group Command Example

```
MyUSGFLEX500H> show config wlan-setting group default group-smart-mesh-
setting
group-smart-mesh-setting
    group-uuid 0828903f-f908-4059-831a-5eb8aac6fa23
    enabled false
    ethernet-failover true
    wireless-bridge-enabled false
    perferred-band-mode auto
    downlink true
    mesh-pap-psk true
    eth-timeout 10
    eth-period 30
    repeater-disconnect-tolerance 120
    repeater-connect-timeout 300
    rssi-threshold-2g -80
    rssi-threshold-5g -75
    rssi-threshold-6g -85
    chutil-threshold-2g 50
    chutil-threshold-5g 80
    chutil-threshold-6g 80
    manual-uplink false
    manual-uplink-retry 4
    mesh-mlo auto
    mesh-mlo-fallback-timeout 200
    ..
MyUSGFLEX500H>
```

35.7 AP SSID Settings Commands

The following table describes the commands available for AP SSID settings. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 143 Command Summary: AP SSID Settings

LABEL	DESCRIPTION
`show config wlan-setting ssid-profile <ssid>`	Displays detailed information of the specified WiFi network (SSID).
`show config wlan-setting security-profile <profile-id>`	Displays detailed information of the specified security profile.
`show config wlan-setting l2isolation-profile l2isolation-<groupid>-<ssid>`	This shows the information of the Layer 2 isolation profile for the specified SSID. Layer 2 isolation prevents WiFi clients connected to the same SSID from communicating with each other directly.
`show config wlan-setting ssid-profile ssid-<groupid>-<ssid> override-tag`	Displays the assigned AP tags of the specified WiFi network (SSID).

Table 143 Command Summary: AP SSID Settings (continued)

LABEL	DESCRIPTION
`wlan-setting security-profile security-<groupid>-<ssid> security-mode {none| enhanced-open| wpa2| wpa2-mix| wpa3}`	• Sets the encryption and authentication method for the AP group. • *groupid*: Enter the AP group ID to set encryption and authentication method. • *ssid*: Enter the SSID to set encryption and authentication method. • none: allow any client to associate this network without any data encryption or authentication. • `enhanced-open`: allow any client to associate this network without any password but with improved data encryption. • `wpa2/wpa2-mix/wpa3`: Enter `wpa2`, `wpa2-mix`, or `wpa3` to enable WPA2/2-MIX/3 data encryption. Upon selecting WPA Personal with WPA3, APs that do not support it will revert to WPA2.
`wlan-setting security-profile security-<groupid>-<ssid> wpa-psk-shadow <pre-shared-key>`	Sets a pre-shared key of 8 to 63 case-sensitive keyboard characters for WPA2, WPA2-mix, or WPA3 data encryption. • *groupid*: Enter the AP group ID. • *ssid*: Enter the SSID.
`wlan-setting ssid-profile ssid-<groupid>-<ssid> ssid <ssid-name>`	Sets the SSID name as it appears to WiFi clients.
`wlan-setting ssid-profile ssid-<groupid>-<ssid> macfilter-action {allow | block | disable}`	Sets a MAC address filter for the specified WiFi network (SSID) in an AP group. This allows or blocks WiFi clients from connecting to the SSID based on the MAC filter profile applied to specific WiFi clients. • `groupid`: The ID of the AP group. • `ssid`: The WiFi network for which to set the policy. • `allow`: Allows WiFi clients with the policy rule 'allow' to connect to the SSID. All other clients are blocked. • `block`: Blocks WiFi clients with the policy rule 'block' from connecting to the SSID. All other clients are allowed. • `disable`: Allows all WiFi clients to connect to the SSID.
`[del] wlan-setting ssid-profile ssid-<groupid>-<ssid> override-tag <tag-name>`	Assigns or removes an AP tag for the specified WiFi network (SSID). When the tags of an SSID and an AP in the same group match, the SSID will be broadcast. If you do not assign an AP tag to an SSID, then only the AP with that SSID will broadcast the SSID.
`wlan-setting security-profile security-<groupid>-<ssid> transition-mode {true| false}`	Upon selecting `enhanced-open` or `wpa3`, transition mode generates two VAP so APs that do not support Enhanced-Open/WPA Personal With WPA3 can connect using Open/WPA Personal With WPA2 network.
`wlan-setting security-<groupid>-<ssid> mac-auth enabled {true| false}`	Sets to authenticate WiFi clients by their MAC addresses together with a user name and password.
`wlan-setting security-profile security-<groupid>-<ssid> auth-server-info type {internal| external}`	Sets how to perform 802.1X secure authentication with MAC address authentication. • `external`: use an external RADIUS server for 802.1X authentication. • `internal`: use the Zyxel Device for 802.1X authentication.
`mac-auth database mac <mac-address> description <description>`	Sets the MAC address or OUI (Organization Unique Identifier) of the WiFi client to be authenticated along with optional information to describe the client. Make sure to use the correct format for the MAC address (XX:XX:XX:XX:XX:XX) or OUI (XX:XX:XX).

Table 143 Command Summary: AP SSID Settings (continued)

LABEL	DESCRIPTION
wlan-setting security-profile security-<*groupid*>-<*ssid*> mac-auth setting {account| calling-station-id} delimiter {colon| dash| none} letter-case {upper| lower}	Sets the MAC address format used for MAC authentication in the AP group SSID profile. Sets the delimiter used in the MAC address: • colon: Uses colons (e.g., 00:11:22:33:44:55) • dash: Uses dashes (e.g., 00-11-22-33-44-55) • none: Uses no delimiter (e.g., 001122334455) Specifies whether the MAC address should use uppercase or lowercase letters: • upper: Uppercase (e.g., AA:BB:CC) • lower: Lowercase (e.g., aa:bb:cc)
wlan-setting security-profile security-<*groupid*>-<*ssid*> auth-server-info {internal| external} auth-server <*auth-server*>	Sets the authentication server for the AP group SSID profile. • *groupid*: Enter the AP group ID. • *ssid*: Enter the SSID. • external: use an external RADIUS server for 802.1X authentication. • internal: use the Zyxel Device for 802.1X authentication. • *auth-server*: enter the name of the authentication server.
wlan-setting security-profile security-<*groupid*>-<*ssid*> internal-eap-proxy {true|false}	Allows EAP packets to pass directly between the AP's clients and the RADIUS server when you use the internal authentication server for security. The Zyxel Device will only forward the packets without inspecting or modifying them.
wlan-setting security-profile security-<*groupid*>-<*ssid*> dot1x-eap {true | false}	Sets the encryption and authentication method to WPA2/WPA3-Enterprise for the AP group.
wlan-setting ssid-profile ssid-<*groupid*>-<*ssid*> selected-bands bands {2.4| 5| 6}	Specifies which frequency band(s) the SSID will use.
wlan-setting ssid-profile ssid-<*groupid*>-<*ssid*> vlan-id <vlan-id>	Sets the ID number of the VLAN to which the SSID belongs.
wlan-setting ssid-profile ssid-<*groupid*>-<*ssid*> rate-limit {downlink| uplink} speed <*speed*> unit mbps	Sets the maximum data download and upload rates in Mbps, on a per-station basis.
wlan-setting ssid-profile ssid-<*groupid*>-<*ssid*> block-intra {true | false}	Enables to prevent crossover traffic from within the same SSID. Disable to allow intraBSS traffic.
wlan-setting ssid-profile ssid-<*groupid*>-<*ssid*> band-select {true | false}	Enables band steering so that the AP steers WiFi clients to the 5 GHz band.

Table 143 Command Summary: AP SSID Settings (continued)

LABEL	DESCRIPTION
`wlan-setting ssid-profile ssid-<groupid>-<ssid> proxy-arp enabled {true | false}`	The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a MAC address. An ARP broadcast is sent to all devices on the same Ethernet network to request the MAC address of a target IP address. Enable this to allow the Zyxel Device to answer ARP requests for an IP address on behalf of a client associated with this SSID. This can reduce broadcast traffic and improve network performance.
`wlan-setting ssid-profile ssid-<groupid>-<ssid> dot11kv enabled {true| false}`	Enables IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming.
`wlan-setting security-profile security-<groupid>-<ssid> dot11r enabled {true| false}`	Turns on or off IEEE 802.11r fast roaming on the AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another, by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process. Note: This feature is not available when you enable MLO.
`wlan-setting ssid-profile ssid-<groupid>-<ssid> uapsd {true | false}`	Enables Unscheduled Automatic Power Save Delivery (U-APSD), which is also known as WMM-Power Save. This helps increase battery life for battery powered WiFi clients connected to the Zyxel Device using this SSID profile.
`[del] wlan-setting ssid-profile ssid-<groupid>-<ssid> l2isolation l2isolation-<groupid>-<ssid>`	Turns on or off layer-2 isolation. If a client device's MAC addresses is NOT listed, it is blocked from communicating with other devices in an SSID on which layer-2 isolation is enabled.
`[del] wlan-setting l2isolation-profile l2isolation-<groupid>-<ssid> mac <mac-address>`	Enter the MAC address of each client device that you want to allow to be accessed by other client devices in the SSID on which layer-2 isolation is enabled.
`wlan-setting ssid-profile ssid-<groupid>-<ssid> hide-ssid {true | false}`	Hides or shows the SSID in clients' Wi-Fi network lists. If the SSID is hidden, clients have to manually enter the SSID name to connect.

35.8 AP Radio Settings Commands

The following table describes the commands available for AP radio settings. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 144 Command Summary: AP Radio Settings

LABEL	DESCRIPTION
`show config wlan-setting radio-profile`	This shows the AP group's radio settings.
`show state country-deployment country-table`	This shows the list of supported countries and their corresponding wireless regulatory domains.

Table 144 Command Summary: AP Radio Settings (continued)

LABEL	DESCRIPTION
`wlan-setting radio-profile radio-<groupid>-<slotid> country-code <country-code>`	Sets the country where the AP is located or installed. The available channels vary depending on the country you select. Be sure to select the correct or same country for both radios on an AP and all connected APs in order to prevent roaming failure and interference with other systems. • `groupid`: the AP group's ID. • `slotid`: the slot number for the radio profile (`1` for 2.4 GHz, `2` for 5 GHz, `3` for 6 GHz). • `country-code`: the code for the country.
`wlan-setting radio-profile radio-<groupid>-<slotid> deployment-selection {single-ap| low-density| moderate-density| high-density| custom}`	Sets the following criteria according to where you deploy the AP. • `high-density`: for the lowest output power to reduce interference to the minimum in areas where you have 10 or more APs. • `moderate-density`: for moderate output power to reduce interference in areas where you have 6 to 9 APs. • `low-density`: for higher concentration of output power for less than 5 APs. • `single AP`: to maximize WiFi coverage in areas where you have just 1 AP.
`wlan-setting radio-profile radio-<groupid>-<slotid> tx-power <output power>`	Sets the transmit power level for the specified radio profile. The higher the AP output power, the greater the WiFi coverage, but the more interference there will be with nearby APs. • `groupid`: the AP group's ID. • `slotid`: the slot number for the radio profile (`1` for 2.4 GHz, `2` for 5 GHz, `3` for 6 GHz). • `output power`: the output power of the radio.
`wlan-setting radio-profile radio-<groupid>-<slotid> ch-width {20 | 40 | 80 | 160 | 320}`	Sets the WiFi channel bandwidth you want the AP to use. • `groupid`: the AP group's ID. • `slotid`: the slot number for the radio profile (`1` for 2.4 GHz, `2` for 5 GHz, `3` for 6 GHz).
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-mode-interval {true| false}`	Sets the DCS (Dynamic Channel Selection) time interval (in minutes) to regulate how often an AP surveys 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 channel with lower interference.
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-time-interval <10..1440>`	Sets the DCS (Dynamic Channel Selection) time interval (in minutes) to regulate how often an AP surveys other APs within its broadcast radius.
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-mode-schedule {true | false}`	Enable to have the AP automatically find a less-used channel within its broadcast radius at a specific time on selected days of the week.
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-schedule-stat {mon-stat | tue-stat | wed-stat | thu-stat | fri-stat | sat-stat | sun-stat} {true | false}`	Sets the day of the week to have the AP use DCS to automatically scan and find a less-used channel.
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-schedule-stat start-time <time>`	Sets the time of the day (in 24-hour format) to have the AP use DCS to automatically scan and find a less-used channel.

Table 144 Command Summary: AP Radio Settings (continued)

LABEL	DESCRIPTION
`wlan-setting radio-profile radio-<groupid>-<slotid> dcs-client-aware {true| false}`	Enable to have the AP wait until all connected clients have disconnected or currently have no traffic before switching channels.
`wlan-setting radio-profile radio-<groupid>-2 dcs-dfs-aware {true | false}`	If your APs are operating in an area known to have RADAR devices, enable this to have the selected APs choose non-DFS channels to provide a stable WiFi service.
`wlan-setting radio-profile radio-<groupid>-2 nol-channel-block {true| false}`	If your APs are operating in an area known to have RADAR devices, enable this to have the selected APs choose non-DFS channels to provide a stable WiFi service.
`wlan-setting radio-profile radio-<groupid>-1 dcs-2g-method {auto| manual | 3-channel | 4-channel}`	Sets the channel deployment for the 2.4G radio. • `3-channel`: limit channel switching to channels 1, 6, and 11, the three channels that are sufficiently separated 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. • `4-channel`: limit channel switching to four channels. If the only allowable channels in your country are 1 – 11 then the AP uses channels 1, 4, 7, 11; otherwise, the AP uses channels 1, 5, 9, 13. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum. • `auto`: allow channel-hopping across all channels to have the AP automatically select the best channel. • `manual`: specify certain individual channels that the AP can switch between.
`wlan-setting radio-profile radio-groupid-1 dcs-2g-selected-channels <channel>`	Specifies a channel for the 2.4G radio.
`wlan-setting radio-profile radio-<groupid>-2 dcs-5g-method {auto | manual}`	Sets the channel deployment for the 5G radio. • `auto`: have the AP automatically select the best channel. • `manual`: specify certain individual channels that the AP can switch between.
`wlan-setting radio-profile radio-<groupid>-2 dcs-5g-selected-channels <channel>`	Specifies a channel for the 5G radio.
`wlan-setting radio-profile radio-<groupid>-3 dcs-6g-method {auto | manual}`	Sets the channel deployment for the 6G radio. • `auto`: have the AP automatically select the best channel. • `manual`: specify certain individual channels that the AP can switch between.
`wlan-setting radio-profile radio-<groupid>-2 dcs-6g-selected-channels <channel>`	Specifies a channel for the 6G radio.
`wlan-setting radio-profile radio-<groupid>-<slotid> reject-legacy-station {true| false}`	Has the AP allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.

Table 144 Command Summary: AP Radio Settings (continued)

LABEL	DESCRIPTION
`wlan-setting radio-profile radio-<groupid>-<slotid> rssi-threshold enable {true | false}`	Enable to monitor WiFi clients and drop the connections of clients that are idle or have a low signal in order to optimize the bandwidth available for other clients. Dropped WiFi clients have may connect to an AP with a stronger signal. Additionally, dual band WiFi clients can also steer from one band to change from a busy band with many WiFi clients to a less busy band with fewer clients.
`wlan-setting radio-profile radio-<groupid>-<slotid> rssi-threshold kickout-threshold <-20..-105>`	Sets a minimum disconnect signal strength. When a WiFi client's signal strength is lower than the specified threshold, the AP disconnects the WiFi client. –20 dBm is the strongest signal you can require for automatic disconnection and –105 dBm is the weakest.
`wlan-setting radio-profile radio-<groupid>-<slotid> rssi-threshold sta-idlechk-level {high | standard | low}`	`high`, `standard` and `low` stand for different traffic rate threshold levels. The level you select here decides when the AP takes action to improve the access point's WiFi network performance. The AP will postpone the actions implemented on access points until the threshold you set here is exceeded. • `low`: has the AP to postpone the action while the access point network traffic is low. Select this if the AP is usually connected to only a few devices and there are no heavy users. • `standard`/`high`: has the AP to postpone the action only when the access point network traffic is medium to heavy. Select this if multiple users are connected at the same time and are streaming videos, using cloud services, or transferring large files.
`wlan-setting radio-profile radio-<groupid>-<slotid> country-ie {true | false}`	Enables 802.11d on the access point. 802.11d allows clients to automatically configure themselves to their local regulatory domain, ensuring compliance with country-specific rules regarding allowed frequencies, power levels, and signal bandwidth. Enabling 802.11d causes the AP to broadcast the country where it is located, which is determined by the Country setting.
`wlan-setting radio-profile radio-<groupid>-<slotid> {wlan-rate-control-2g | wlan-rate-control-5g | wlan-rate-control-6g} <rate>`	Sets the minimum data rate in Mbps that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the AP. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.

35.9 Wireless Health Settings Commands

The following table describes the commands available for wireless health settings. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 145 Command Summary: Wireless Health Settings

LABEL	DESCRIPTION
`wlan-setting wireless-health-action radio-24g-dcs-now {true| false}`	Has the AP scan and choose a radio channel that has least interference.
`wlan-setting wireless-health-action radio-5g-downgrade-cw {true | false}`	Has the AP change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other APs. If the AP wireless performance has not improved, the Zyxel Device will have the AP scan and choose a radio channel that has least interference.

Table 145 Command Summary: Wireless Health Settings (continued)

LABEL	DESCRIPTION
`wlan-setting wireless-health-action radio-6g-downgrade-cw {true| false}`	Has the AP change the channel bandwidth to reduce the radio interference with other APs. • For WiFi 7 APs, the channel bandwidth changes from 320 MHz to 80 MHz. • For WiFi 6E APs, the channel bandwidth changes from 160 MHz to 80 MHz. If the AP wireless performance has not improved, the Zyxel Device will have the AP scan and choose a radio channel that has least interference.
`wlan-setting wireless-health-action client-kick-sta {true| false}`	Has the AP try to steer wireless clients with poor signal strength to an AP or SSID with a strong signal every 30 minutes.
`wlan-setting wireless-health-action aggressiveness-enabled {true| false}`	Enables the AP takes action to improve the access point's WiFi network performance. • `true`: has the Zyxel Device take action according to the aggressiveness level specified in the next command (`low, standard, high`.) • `false`: triggers immediately without checking the idle state; client devices may experience disconnection.
`wlan-setting wireless-health-action aggressiveness-level {low | standard | high}`	`high`, `standard` and `low` stand for different traffic rate threshold levels. The level you select here decides when the Zyxel Device takes actions to improve the APs wireless network performance. The Zyxel Device will postpone the actions implemented on APs until your network is less busy if the threshold is exceeded. Type a suitable traffic rate threshold level for your network. • `high`: has the Zyxel Device postpone the action set when the AP network traffic is heavy. • `standard`: has the Zyxel Device postpone the action set when the AP network traffic is medium. • `low`: has the Zyxel Device postpone the action set when the AP network traffic is low.

35.10 AP Controller Settings Commands

The following table describes the commands available for AP controller (APC) settings. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 146 Command Summary: APC Settings

LABEL	DESCRIPTION
`apc-setting apc-admin password-shadow "password"`	Sets the password for accounts with the username "admin" on managed APs. You can use 4 to 63 alphanumeric characters. The following special characters are allowed: ~!@#$%^&*()_-+={}\|;:<>,./" Uses the `password-shadow` command followed by the password in plain text, to encrypt this password in a saved configuration file. Valid plain text characters are [0-9][a-z][A-Z]['(){}<>^`+/:!*#@&=$.~%|;-"] The password requires: • From 6 to 63 characters • At least 1 upper case letter • At least 1 digit • At least 1 special character.
`apc-setting apc-service {true | false}`	Allows change of the password for accounts with the username "admin" on managed APs.

Table 146 Command Summary: APC Settings (continued)

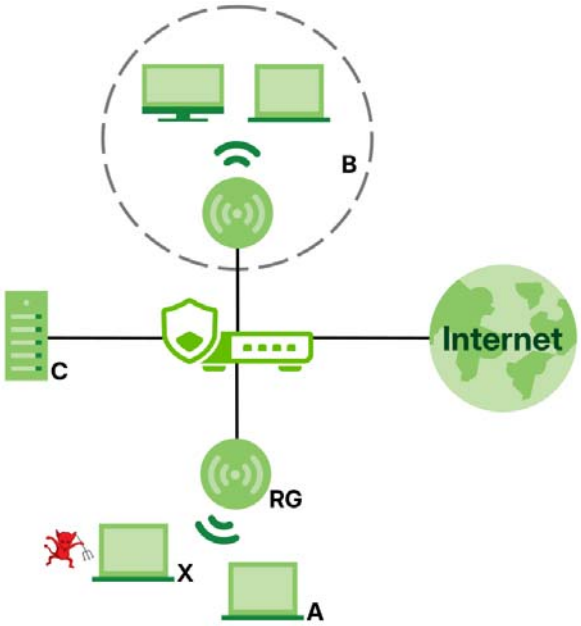
LABEL	DESCRIPTION
`apc-setting ac-ip force {true | false}`	Lets the Zyxel Device change the AP controller's IP address on managed AP(s) to match the configuration on the Zyxel Device.
`apc-setting ac-ip auto {true | false}`	Lets managed AP(s) automatically send broadcast packets to find any other AP controllers.
`apc-setting ac-ip primary <ip-address>`	Specifies the IP address of the primary AP controller.
`apc-setting ac-ip secondary <ip-address>`	Specifies the IP address of the secondary AP controller.
`apc-setting fallback enable {true | false}`	Lets the primary AP controller manage AP(s) again if the primary AP controller is temporarily unavailable.
`apc-setting fallback interval`	Sets how often managed AP(s) check whether the primary AP controller is available (30 to 86400 seconds).
`apc-setting last-config enable {true | false}`	Returns the managed AP to the last saved configuration.
`apc-setting internal-auth-server cert <certificate-name>`	Specifies the certificate used when wireless clients on managed APs perform 802.1X authentication against the Zyxel Device's internal authentication server. By default, the Zyxel Device uses the "default" certificate for AP management.
`show state apc-admin`	Displays the password for accounts with the username "admin" on managed APs.
`show apc-ccm apc-admin-cli`	Displays encrypted password configuration for "admin".

35.11 Rogue AP Detection Commands

A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

In the following example, 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 WiFi network (**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. The attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Figure 100 Rogue AP Example



The following table describes the commands available for Rogue AP Detection. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 147 Command Summary: Rogue AP Detection

LABEL	DESCRIPTION
`cmd rogue-ap detect now`	Scans for rogue APs in the network.
`wlan-setting rogue-ap weak-security {true | false}`	Determines an AP as a suspected rogue AP if it is using an SSID with weak security (Open, WEP, WPA-PSK).
`wlan-setting rogue-ap unmanaged-ap {true | false}`	Determines an AP as a suspected rogue AP if it is not managed by the Zyxel Device.
`wlan-setting rogue-ap hidden-ssid {true | false}`	Determines an AP as suspected rogue AP if it broadcasts hidden SSIDs for wireless clients.
`wlan-setting rogue-ap ssid-keyword enabled {true | false}`	Determines an AP as a suspected rogue AP if it broadcasts an SSID containing a specified keyword.
`[del] wlan-setting rogue-ap ssid-keyword keyword <`*`string`*`>`	Adds or removes a suspect rogue AP keyword contained in the SSID name as a detection rule. Use up to 32 characters [0-9a-zA-Z`~!@#$%^&*()-_=+,<.>/?;:'"[{]} |]. Note: You can add up to ten keywords.
`show state rogue-ap wlan-setting`	Displays the WLAN settings of a suspected rogue AP.
`show state rogue-ap detection info`	Displays the rogue AP scanning results.
`show state rogue-ap detection monitoring`	Displays details of suspected rogue APs.

35.11.1 Rogue AP Detection Command Examples

The following command shows how to check the current rogue AP detection rules and remove configured SSID keywords.

```
MyUSGFLEX500H running config# show state rogue-ap wlan-setting
wlan-setting
    weak-security true
    unmanaged-ap true
    hidden-ssid true
    ssid-keyword
        enabled true
        keyword-list 1
            keyword SSID_TW
            ..
        keyword-list 2
            keyword 1234
            ..
        ..
    ..
MyUSGFLEX500H running config# del wlan-setting rogue-ap ssid-keyword  keyword 12
34
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# show state rogue-ap wlan-setting
wlan-setting
    weak-security true
    unmanaged-ap true
    hidden-ssid true
    ssid-keyword
        enabled true
        keyword-list 1
            keyword SSID_TW
            ..
        ..
    ..
```

CHAPTER 36
System

36.1 System Overview

Use these commands to configure general Zyxel Device information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which Zyxel Device zones (if any) from which computers.

36.2 Host Name Commands

The following table describes the commands available for the hostname. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 148 Host Name Commands

COMMAND	DESCRIPTION
`system hostname <hostname>`	Sets a descriptive name to identify your Zyxel Device. You can use up to 30 single-byte characters, dashes (-) and underscores (_). Spaces are not allowed.
`show state system hostname`	Displays the name to identify your Zyxel Device.
`show state system timezone-auto-sync`	Displays the Zyxel Device timezone settings.

36.3 Time and Date

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

36.3.1 Date/Time Commands

The following table describes the commands available for date and time setup.

Table 149 Date/Time General Commands

COMMAND	DESCRIPTION
`cmd datetime date <yyyy-mm-dd> time <hh:mm:ss>`	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
`system timezone-auto-sync {true| false}`	Allows the Zyxel Device to automatically update its time zone from the time server. The `false` command disables the Zyxel Device from automatically updating its time zone from the time server.
`system timezone <timezone>`	Sets the timezone of your location manually. This will set the time difference between your timezone and Greenwich Mean Time (GMT).
`show config system timezone-auto-sync`	Displays if the Zyxel Device is allowed to automatically update its time zone from the cloud server.
`show state system timzone`	Displays the Zyxel Device timezone.

36.3.2 NTP Service Commands

The following table describes the commands available for configuring the NTP service. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 150 NTP Service Commands

COMMAND	DESCRIPTION
`vrf main ntp enabled {true| false}`	Has the Zyxel Device get the time and date from the time server you set. Uses the `false` command to have the Zyxel Device use the time and date settings you configured manually.
`vrf main ntp ntp-source-address <IP address>`	Sets the IP address of the NTP time server for your Zyxel Device to get the time and date. Check that the IP address is available.

Table 150 NTP Service Commands

COMMAND	DESCRIPTION
vrf main ntp time-sources server {IP address| FQDN} {version *<version>* | *<association-type>* *<association-type>* | iburst {true | false}| prefer {true | false} | auth-key-id <id>}	Sets the IP address or Fully-Qualified Domain Name of your NTP time server. version: Enter the version of NTP to be used for time synchronization. association-type: Enter the desired association type between the NTP time server and your Zyxel Device. • PEER: Has both the NTP time server and the Zyxel Device provide time synchronization services to each other. • POOL: Has the ZD get the time and date from a pool of NTP servers determined by a DNS name. The ZD acts as an NTP client, and only gets the time from the NTP server. • SERVER: Has the ZD get the time and date from a single NTP server. The ZD acts as an NTP client, and only gets the time from the NTP server iburst: Has the Zyxel Device send multiple time queries at the beginning of the synchronization to obtain more accurate time information. prefer: Prioritizes synchronization with this time server, when the Zyxel Device synchronizes with multiple NTP servers. auth-key-id: Sets the authentication key ID for authenticating NTP messages between the Zyxel Device and the NTP time server.
vrf main ntp server-subnet *<priority>* {allow| deny}{CIDR subnet| all}	Sets the Zyxel Device as an NTP server and allows or blocks access to specific subnets, or to all subnets. priority: Enter the priority for this rule. The lower the number, the higher the priority. 1 is the highest. CIDR subnet: Enter IP subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> all: Applies the allow or block rule to all subnets.
vrf main server-subnet	Sets the subnet of your NTP time server.
vrf main ntp auth-key	Sets the key used to authenticate between the Zyxel Device and the NTP time server.
show ntp clients	Displays the status of NTP clients synchronizing with the Zyxel Device.
cmd ntp update execute	Gets the time and date from the NTP time server you set.
cmd ntp update get-result	Displays if the Zyxel Device has successfully gotten the time and date from the NTP time server.

36.4 System Monitor Commands

The following table describes the commands available for monitoring CPU, memory, storage, and temperature utilization.

A system log will be generated as a reminder when the Zyxel Device's memory utilization reaches the threshold. You can also set up an email notification. For details on sending email notification, see Mail Server and Alerts Commands on page 314. The following table shows the default thresholds for each model at the time of writing.

Table 151 Default Memory Usage Threshold

MODEL	THRESHOLD
USG FLEX 50H USG FLEX 50HP USG FLEX 100H USG FLEX 100HP	90%
USG FLEX 200H USG FLEX 200HP USG FLEX 500H USG FLEX 700H	80%

You must use the `edit running` command to enter configuration mode before using these commands.

Table 152 System Monitor Commands

COMMAND	DESCRIPTION
`system monitor {cpu | mem | storage | temperature} enabled {true | false}`	Enables or disables CPU, memory, storage, and temperature monitoring.
`system monitor {cpu | mem | storage | temperature} time-window` *`<1...60>`*	Sets the time period (in minutes) used to calculate the average utilization. The usage percentage is based on data collected during this period.
`system monitor {cpu | mem | storage | temperature} threshold` *`<1...100>`*	`cpu`, `mem`, `storage`: Sets a threshold for the percentage of CPU, memory, and storage. `temperature`: Sets a threshold for the Zyxel Device's hardware temperature in degree centigrade or Celsius.
`system monitor mem cleanup-db-threshold` *`<1...100>`*	Sets a threshold for the memory utilization percentage that triggers a memory database cleanup. When the Zyxel Device's memory utilization reaches the specified threshold, it starts cleaning up its memory database (for example, live sessions and NAT).
`show state system monitor`	Displays the configuration details for CPU, memory, storage, and temperature monitoring.

Table 152 System Monitor Commands (continued)

COMMAND	DESCRIPTION
`show system history type cpu {average | sys-average | fp-average} period {1hr | 24hrs | 7days}`	Displays the CPU usage over a historical period. • `average`: The average overall CPU usage. • `sys-average`: The average CPU usage for system processes. • `fp-average`: The average CPU usage for fastpath processes.
`show system history type {mem | fp-mem | session | port <port-number> | interface <interface-name>} period {1hr | 24hrs | 7days}`	Displays the system usage over a historical period. • `mem`: The system memory usage in percent. • `fp-mem`: The fastpath memory usage in percent. • `session`: The number of sessions, both established and non-established, passing through or within the Zyxel Device. • `port`: The number of bytes per second received and transmitted on the specified port. • `interface`: The number of bytes per second received and transmitted on the specified interface. • `1hr, 24hrs, 7days`: The time range for displaying the specified system usage.

36.5 Device HA

Device HA lets a passive (secondary) Zyxel Device automatically take over if the active (primary) Zyxel Device fails. Both Zyxel Devices must be the same model with the same firmware version. Device HA pairing occurs when Device HA is set up successfully on both Zyxel Devices.

The primary Zyxel Device is the license controller. Existing licenses on the secondary Zyxel Device are appended to the licenses on the primary Zyxel Device after pairing occurs. When updating licenses, update them on the primary Zyxel Device.

The following features can be transferred to the secondary Zyxel Device when it becomes active using Device HA:

- Start-up and Running Configuration
- Signatures
- Device Insight
- External Block List
- DHCP Leasing Entries
- Two-factor Authentication
- Certificates
- Licenses including NCC if applicable
- Zyxel Device Time

36.5.1 Heartbeat

Device HA uses a dedicated heartbeat link between an active and a passive device for status syncing and to trigger failover and backup to the passive device if the active device becomes unresponsive. On the passive device, all ports are disabled except for the port with the heartbeat link.

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

Figure 101 Device HA Backup Taking Over for the Master

Note: Make sure that the heartbeat port is not already in an interface that is already configured for other features such as VLAN, Bridge.

Note: The dedicated heartbeat link port must be the highest-numbered copper Ethernet port on each Zyxel Device for Device HA to work. At the time of writing, these are the models that support HA with associated heartbeat link ports.

Table 153 Device HA Heartbeat Ports

MODEL	HEARTBEAT PORT
USG FLEX 200H / 200 HP	8
USG FLEX 500H / 700 H	12

Failover from the active Zyxel Device to the passive Zyxel Device occurs when:

- A monitored interface is down on the active Zyxel Device.
- The connectivity check on the heartbeat link exceeds the failure tolerance.

After failover, the initially active Zyxel Device becomes the passive Zyxel Device.

36.5.2 Firmware Upgrade on Paired Zyxel Devices

1. First, upgrade the firmware to the passive device.
2. After upgrade, the passive device becomes the active device and handles all traffic during the firmware upgrade.
3. Firmware is then upgraded to the passive primary device.
4. After the firmware upgrade is complete on both Zyxel Devices, the primary device becomes the active device again.

36.5.3 Preparing to Deploy Device HA

1. Make sure the passive Zyxel Device is offline, then enable Device HA in the active Zyxel Device.
2. The management IP addresses for both the active and passive Zyxel Devices must be in the same subnet.
3. Make sure the SSH service is enabled on both Zyxel Devices. SFTP (Secure File Transfer Protocol) is used to transfer files from the active to the passive Zyxel Device.
4. Connect the passive Zyxel Device to the active Zyxel Device using the heartbeat ports. These are the highest-numbered copper Ethernet ports on the Zyxel Devices - see Table 153 on page 304.
5. If both Zyxel Devices are turned on at the same time with Device HA enabled, then they may send the heartbeat at the same time. In this case, the Zyxel Device with the **Primary (License Controller)** role becomes the active Zyxel Device.

36.5.4 Using NCC To Manage Device HA

You must register both Zyxel Devices on NCC, that is they must both belong to an organization. The passive Zyxel Device will be registered automatically in NCC if it is not already registered in NCC.

Both Zyxel Devices must be in the same organization and be registered to the same account.

The passive Zyxel Device is removed from the NCC site after Device HA pairing is complete, as a site in NCC can only have one Zyxel Device firewall (at the time of writing).

NCC automatically sends an email to notify users when Zyxel Devices are paired with licenses transferred.

36.6 Device HA Configuration Commands

This table lists the Device HA configuration commands.

Table 154 Device HA Configuration Commands

COMMAND	DESCRIPTION
`device-ha enabled {true | false}`	Enables or disables Device HA. You must enable Device HA on both the active and passive Zyxel Devices. Make sure the passive Zyxel Device is offline when you enable Device HA on the active Zyxel Device. Then turn on the secondary Zyxel Device and connect both Zyxel Devices using an Ethernet cable connected to the heartbeat ports. Wait for the secondary Zyxel Device to respond.
`cmd device-ha auto-provision enabled {true | false}`	Enables or disables automatic synchronization of the primary Zyxel Device to the secondary Zyxel Device.
`vrf main device-ha virtual-mac enabled {true | false}`	Enables or disables a virtual MAC address which the active Zyxel Device automatically generates. It has priority over the physical MAC address. With a virtual MAC address, you can hot swap the active Zyxel Device without reconfiguring Device HA. At the time of writing, the virtual MAC address begins with “X6”, (X6:XX:XX:XX:XX:XX).

Table 154 Device HA Configuration Commands (continued)

COMMAND	DESCRIPTION
device-ha management-ip active *<ipv4-address>*	Sets the management IP address of the active Zyxel Device. Management IP addresses allow you to manage whichever is the active Zyxel Device when Device HA is paired. You must configure management IP addresses for both the active and passive Zyxel Devices and they must have the same subnet mask. Type the IPv4 address of the highest-numbered copper Ethernet port on the active Zyxel Device (the heartbeat dedicated link port).
device-ha management-ip passive *<ipv4-address>*	Sets the management IP address of the passive Zyxel Device. Type the IPv4 address of the highest-numbered copper Ethernet port on the active Zyxel Device (the heartbeat dedicated link port).
device-ha management-ip netmask *<subnet-mask>*	Active and passive Zyxel Devices must use the same subnet mask. Enter a subnet mask such as 255.255.255.0 of the management IP address.
device-ha monitor-interface interface *<interface-name>*	Member interface types can be Ethernet, VLAN, or Bridge. Select an interface to be monitored by Device HA to determine if a passive Zyxel Device should become active.
device-ha linkdown-monitor enabled {true | false}	Has the passive Zyxel Device become the active Zyxel Device when a selected monitored interface is down. This is on by default (true).
device-ha conn-check-monitor enabled {true | false}	Has the passive Zyxel Device become the active Zyxel Device when a connectivity ping check fails on a selected monitored interface. This is off by default (false).
device-ha failover pause-count <5..50>	Sets the maximum number of failovers allowed where the passive Zyxel Device becomes the active Zyxel Device. A failover may happen due to a monitored interface being down, a connectivity ping check fails or the Ethernet heartbeat connection is down.
cmd device-ha failover pause-count {clear | enable | disable>	Removes, enables or disables the failover pause count. Disabling the failover pause count means there is no limit on the number of failovers allowed
device-ha failover pause-count-reset-period <1..30>	Sets the time period in days to reset the failover count. The default is that the failover count is reset every 5 days.
device-ha failover conn-check-hold-period <60..86400>	Sets a minimum time period between failovers to mitigate failover flapping. Failover flapping occurs when the active and passive devices keep switching due to a connectivity ping check failure. The default is 300 seconds.
device-ha heartbeat interval <2..10>	Sets the number of seconds (2-10) allowed for absence of a heartbeat signal. The default is 2 seconds.
device-ha heartbeat lost-tolerance-count <2..10>	Sets the number of heartbeat failures allowed before failover is activated on the passive Zyxel Device. The default is 2 seconds.
vrf main device-ha pause enabled {true | false}	Temporarily stops Device HA without unpairing the active and passive Zyxel Devices. You may do this to troubleshoot the active Zyxel Device for example. Note: Before you save (commit) this command, make sure to turn off or disconnect ALL cables from the passive Zyxel Device! After successfully troubleshooting, remember to set this command to false, then turn on and reconnect ALL cables on the passive Zyxel Device.

36.7 Device HA Show Commands

This table lists the show commands for device HA.

Table 155 device-ha Show Commands

COMMAND	DESCRIPTION
`show state vrf main device-ha status`	Displays whether or not Device HA is activated, the pairing status, the health link and the role (primary or secondary). The primary is the license controller.
`show state vrf main device-ha summary`	Displays • the last time (epoch) and reason failover occurred • the last time (epoch) synchronization occurred and the current status • the number of times failover occurred • the first time (epoch) failover occurred epoch is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT)
`show state vrf main device-ha status sync-service-port`	Displays the SSH port Device HA uses (49058) for file synchronization between the active and passive Zyxel Devices. You cannot change this port number.
`show state vrf main device-ha status {active | passive | enabled | initial-role | pairing-state | pairing-msg | ha-health-state | local-state | local-role | sync-service-port}`	Displays all or each item individually. See the example below. • Role refers to which Zyxel Device is the license controller (primary). • Status refers to Device HA pairing status. • Health refers to the state of the heartbeat link on the monitored port. • The local Zyxel Device is the Zyxel Device that you are currently logged into.
`show state vrf main device-ha file-sync-consistency entry {full | dhcp-lease-file | ip-reputation-sig | startup-config | ssl-inspection-ca | app-patrol-sig | ips-sig | ebl-sig | device-insight | 2fa-google-auth | geoip-sig | sps-sig | timezone}`	Displays whether the specified entry is the same on the passive and active Zyxel Devices.
`show state vrf main device-ha log {local | peer}`	Displays logs for the local and peer Zyxel Device. The local Zyxel Device is the Zyxel Device that you're logged into and could be passive or active.
`cmd device-ha ha-log clear`	Removes all Device HA logs from both the active and passive Zyxel Devices. This command is only available on the active Zyxel Device.

36.7.1 Device HA Show Command Examples

The following are some example Device HA show commands. This command shows the current status.

```
Router# show state vrf main device-ha status
status
    enabled false
    initial-role secondary
    pairing-state none
    pairing-msg ""
    ha-health-state none
    local-state none
    local-role none
    active
        role none
        sn unknown
        icon-color off
        ..
    passive
        role none
        sn unknown
        icon-color off
        ..
    sync-service-port 49058
    ..
```

This command shows details on failovers.

```
Router# show state vrf main device-ha summary
    last-failover-epoch 0
    last-failover-reason ""
    last-sync-epoch 0
    last-sync-status ""
    failover-count 0
    first-failover-epoch 0
    ..
```

The following shows some different log messages you may see for the local Zyxel Device (the Zyxel Device that you are logged into).

```
Router# show state vrf main device-ha log local
op-state Active
    msg " Change to passive state : forced change "
    epoch 1730268017
   ..
Router# show state vrf main device-ha log local
op-state Passive
    msg "Enter Passive state."
    epoch 1730268020
    ..
Router# show state vrf main device-ha log local
op-state Passive
    msg "Change to active state : heartbeats missed"
    epoch 1730268032
```

36.8 Device HA Synch Commands

This table lists the Device HA synchronization commands. These commands synchronize the latest information from the active Zyxel Device with the passive Zyxel Device.

Table 156 device-ha Synch Commands

COMMAND	DESCRIPTION
`cmd device-ha manual-failover`	Triggers Device HA failover causing the active Zyxel Device become the passive Zyxel Device. This command is only available for the currently active Zyxel Device.
`cmd device-ha force-sync full`	Transfers all the latest signatures to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync dhcp-lease-file`	Transfers the latest IP address leasing data to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync startup-config`	Transfers the current configuration of the active Zyxel Device to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync ssl-inspection-ca`	Transfers the latest SSL inspection trusted certificates to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync app-patrol-sig`	Transfers the latest application patrol signatures to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync ips-sig`	Transfers the latest IPS signatures to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync ebl-sig`	Transfers the latest External Block List signatures to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync ip-reputation-sig`	Transfers the latest IP reputation signatures to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync device-insight`	Transfers the latest Device Insight data to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync 2fa-google-auth`	Transfers the latest Two-Factor authentication data to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync geoip-sig`	Transfers the latest Geo-IP data to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync timezone`	Transfers the latest time zone to the passive Zyxel Device. This command is only available for the active Zyxel Device.
`cmd device-ha force-sync sps-sig`	Transfers the latest System Protection Signatures to the passive Zyxel Device. System protection signatures protect the Zyxel Device configuration system such as the web configurator GUI.

36.9 Device HA Debug Commands

This table lists a Device HA command you may use for debugging.

Table 157 device-ha Debug Commands

COMMAND	DESCRIPTION
`cmd device-ha debug-log collect`	Only execute this command if requested by customer support. Allows advanced Device HA debug log collection on the Zyxel Device.

36.10 Device Insight Overview

Use Device Insight to collect status and basic information of the clients connected to the Zyxel Device internal interface or IPSec VPN. The clients shown may include clients connected to the Zyxel Device:

- Using wired connections.
- Through access points (APs) using wired connections.
- Through access points (APs) using WiFi connections.
- Through built-in access points using WiFi connections.
- Using SecuExtender (IPSec VPN clients).

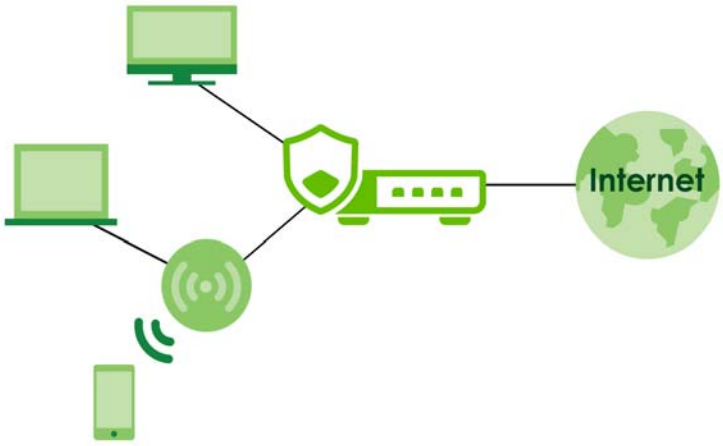
Device Insight collects client information including:

- Hostname
- IP address and MAC address
- Operating system
- Category, such as mobile phones or computers
- Connected interface

Note: To collect clients' information using Device Insight, the clients must be in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly as traffic must pass through another router or a layer-3 switch to the Zyxel Device.

In the graphic below, **A** is a client connected to the Zyxel Device using a wired connection. **B** is a client connected to the Zyxel Device through an AP using a wired connection. **C** is a client connected to the Zyxel Device through an AP using a WiFi connection. **D** is a client connected to the Zyxel Device through an IPSec VPN tunnel using SecuExtender.

Figure 102 Clients' Device Insight Example



36.10.1 Device Insight Commands

The following table describes the commands available for Device Insight. You must use the `edit running` commands to enter the configuration mode before you can use the configuration commands.

Table 158 Device Insight Commands

COMMAND	DESCRIPTION
`vrf main device-insight enabled {true| false}`	Enable Device Insight to collect status and basic information of the clients connected to the Zyxel Device internal interfaces or IPSec VPN.
`vrf main device-insight block-list enabled {true| false} mac <mac-address> logging {no| log| log-alert}`	Enable Device Insight block list to block a client device by the client device's MAC address. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when the blocked client device tries to connect to the Zyxel Device.
`vrf main device-insight mac <mac-address> description <description>`	Creates an entry for the specified client device MAC address. This also sets a description for this entry. You can use up to 63 single-byte characters, including 0-9a-zA-Z\\-'()+.,\\/@_
`vrf main device-insight bypass-interface <interface>`	Sets an internal interface that will not be detected by Device Insight. Device Insight detects all clients connected to the Zyxel Device internal interfaces by default.
`cmd device-insight flush all`	Clears all clients status and information Device Insight collected.
`cmd device-insight remove <mac-address>`	Removes a client that's no longer connected to your network. For example, guest A visited your company over a month ago. Guest A used his cellphone to connect to your Zyxel Device networks. His cellphone was identified by Device Insight. Guest A has left for over a month and you're sure he will not return in the near future. You can remove his device using this command. Guest A's device will be identified again if he connects to your Zyxel Device networks in the future. Please note that clients that are blocked cannot be removed. Make sure to unblock clients before you remove them.
`cmd device-insight feedback mac <mac-address> category <category> os <operating-system> type <type>`	Specify a MAC address to report on the client that is wrongly identified regarding its category, operating system or type.

36.11 DNS Overview

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

36.11.1 Domain Zone Forwarder

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

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

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

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

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

36.11.2 DNS Commands

The following table describes the commands available for DNS. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 159 DNS Commands

COMMAND	DESCRIPTION
`vrf main dns proxy forward {local| dns-server` *`ip-address`*`}`	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s).
`vrf main dns zone <`*`domain`*`> ip <`*`ip-address`*`> ttl <`*`0...2147483647`*`>`	Sets how many seconds to keep the record of the mapping between a fully qualified domain name (FQDN) and an IP address.
`vrf main dns zone <`*`domain`*`> a-record`	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address.
`vrf main dns zone <`*`domain`*`> cname-record`	A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. Type a Fully-Qualified Domain Name (FQDN) of a server. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
`vrf main dns zone <`*`domain`*`> mx-record`	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain.
`vrf main dns security-options default recursion {true| false} additional-from-cache {true| false}`	Selects to use the default security option. Enables recursion to allow the Zyxel Device to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule. Enables additional info from cacher to allow the Zyxel Device to cacher Resource Records (RR) obtained from previous DNS queries.

Table 159 DNS Commands (continued)

COMMAND	DESCRIPTION
vrf main dns security-options customize {recursion {true| false} additional-from cache {true| false} address-object-group <*CIDR*>	Configures and selects to use the customize security option. Enables recursion to allow the Zyxel Device to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule. Enables additional info from cacher to allow the Zyxel Device to cacher Resource Records (RR) obtained from previous DNS queries. Sets the address object to apply it to the security option.
show config vrf main dns	Displays the DNS settings, such as the DNS server IP address and security options settings.
show state vrf main dns	Displays the DNS settings status, such as the DNS server IP address and if the proxy server is enabled.

36.11.3 DNS Command Examples

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns zone abc.com a-record 1 hostname www
210.17.2.13 ptr true
usgflex200hp running config# commit
Configuration committed.
```

This command displays security options configured for the customized and default rules.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns security-options customize recursion true
additional-from-cache true address-object-group 10.0.0.0/8 address-object-group
172.16.0.0/12 address-object-group 192.168.0.0/16
usgflex200hp running config# vrf main dns security-options default recursion true
additional-from-cache true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main dns security-options
security-options customize
    recursion true
    additional-from-cache true
    address-object-group 10.0.0.0/8
    address-object-group 172.16.0.0/12
    address-object-group 192.168.0.0/16
    ..
security-options default
    recursion true
    additional-from-cache true
```

36.12 Notification

The notification commands allow you to configure the Zyxel Device to send you event notifications by email.

You can also configure where to email the alerts when they're generated. Alerts are used for events that require more serious attention, such as system errors and attacks.

36.12.1 Mail Server and Alerts Commands

Use the commands listed below to configure the mail server and mail alerts settings.

Table 160 Mail Server and Alerts Commands

COMMAND	DESCRIPTION
`notification mail tls enabled {true| false}`	Sets the mail server to use or not use (`false` command) Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
`notification mail tls start-tls {true| false}`	The mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device. This command turns off STARTTLS and uses the TLS protocol. The `false` command enables the default STARTTLS protocol (SSL) for encrypted communications between the mail server and the Zyxel Device.
`notification mail tls authenticate-server {true| false}`	Sets the Zyxel Device to authenticates the mail server in the TLS handshake or not (`false` command).
`notification mail server-address <server-address>`	Sets the SMTP mail server IP address or domain name.
`notification mail server-port <1...65535>`	Sets the SMTP port. The default value is 25.
`notification mail from <sender-address>`	Sets the default email address from which the outgoing email is delivered. This address is used in replies. The value should be an email address. It can be up to 83 characters. The valid characters are [a-z][A-Z][/=?^_.{|}~w-!#$%*+].
`notification mail to <recipient-address>`	Sets the email address of the recipient to whom the outgoing email is sent. This is the address that will receive the email. It can be up to 83 characters. The valid characters are [a-z][A-Z][/=?^_.{|}~w-!#$%*+].
`notification mail smtp-authentication {true| false}`	Enables SMTP authentication.
`notification mail user <username> password <password>`	Sets the username and password for SMTP authentication. You can use 4 to 63 single-byte characters for the password, including 0-9a-zA-Z'!@#$%^&*()_+={|}\:;"<>'/
`notification mail user <username> password-shadow <password>`	Uses the `password-shadow` command followed by the password in plain text, to encrypt this password in a saved configuration file. Valid plain text characters are [0-9][a-z][A-Z]['(){}<>^`+/ :!*#@&=$.~%|;-"] The password requires: • From 6 to 63 characters • At least 1 upper case letter • At least 1 digit • At least 1 special character.

Table 160 Mail Server and Alerts Commands

COMMAND	DESCRIPTION
`notification mail auth-type {without-auth | basic-auth | microsoft-oauth2}`	Sets how to authenticate with the SMTP mail server. • `without-auth`: Use this if the SMTP mail server used for the sender email does not require login credentials. • `basic-auth`: Use this if the SMTP mail server used for the sender email requires username and password login credentials. • `microsoft-oauth2`: Use this if the SMTP mail server used for the sender email uses a Microsoft 365 email address. The Microsoft 365 application is built into Microsoft Azure, a cloud computing platform, that uses Microsoft products locally and in the cloud.
`notification mail client-id`	Required when you select `microsoft-oauth2` authentication and generated when you register your application in Azure to uniquely identify your application. To see your `client-id` (at the time of writing), go to the Azure portal, and locate your application in the **App registrations** overview page.
`notification mail tenant-id`	Required when you select `microsoft-oauth2` authentication. This identifies your specific Azure Active Directory (Azure AD) instance (directory ID). To see it (at the time of writing), go to the Azure Active Directory, and select **Properties**.
`notification mailalert <profile-name> enabled {true| false}`	Sends log messages and alert to the email address you specify.
`notification mailalert <profile-name> source {all| source-list source}`	Specifies the types of alerts to be mailed when they're generated.
`notification mailalert <profile-name> from <email-address>`	Enters the email address from which the outgoing email is delivered. The address is used in replies.
`notification mailalert <profile-name> send-alerts-to <email-address>`	Enters the mail address to which alerts are delivered. You can configure up to 5 email addresses.
`notification mailalert <profile-name> mail-subject <subject>`	Sets the email subject.
`notification profile <profile-name> enabled {true| false}`	Creates a log or sends an email notification when the specified type(s) of event occur.
`notification profile [profile name] event {new-firmware | device-shutdown | device-reboot | factory-reset | port-link-down | port-link-up | cpu-usage-over-threshold | mem-usage-over-threshold | storage-usage-over-threshold | temperature-over-threshold | admin-login| admin-login-fail | user-login | user-login-fail | user-lockout | usb-full-warning | usb-full-alert | device-ha-failover]`	Sets the event type(s) to log or send an email notification. You can specify multiple event types by adding the word `'event'` before each type.
`notification profile <profile-name> description <description>`	Sets a description of this event profile to identify it. You can use up to 512 single-byte characters, special characters and spaces are allowed.

Table 160 Mail Server and Alerts Commands

COMMAND	DESCRIPTION
`notification profile <profile-name> inhibition enabled {true|false}`	Temporarily stops receiving notifications for CPU usage over threshold, memory usage over threshold, temperature too high (CPU, Switch, Board), USB disk full alert, USB disk full warning, and storage usage over the threshold. Other event types will not be affected.
`notification profile <profile-name> inhibition period <5...1440>`	Sets how long to stop receiving the above notifications if inhibition is enabled. The range is from 5 to 1440 minutes. The default is 60 minutes.
`notification profile <profile-name> action-type {send-mail | log-only} subject title <email-subject> to <recipient-email>`	Sets the action to take when specified type(s) of event in the specified profile occur: • `send-mail`: Creates a log and sends an email notification when the selected type(s) of event occur. • `log-only`: Creates a log when the selected type(s) of event occur. • `email-subject`: Sets the email subject. • `recipient-email`: Sets the mail address to which notifications are delivered. You can configure up to 5 email addresses.
`show config notification mail`	Displays mail server settings.
`show config notification mailalert`	Displays mail alert settings.
`show notification status mail`	Displays mail server settings such as server-address, server-port, password, auth-type, client-id, tenant-id, tls.
`show notification status mailalert`	Displays all mail alert profiles settings.

36.13 Language Commands

Use the language command to set the language the web configurator is using. You must use the `edit running` command to enter the configuration mode before you can use the command.

Table 161 Command Summary: Language

COMMAND	DESCRIPTION
`gui system language <language>`	Specifies the language used in the web configurator screens.

36.14 Process Tuning Commands

Use the process tuning command to adjust the Zyxel Device's process priorities to optimize performance.

Table 162 Command Summary: Process Tuning

COMMAND	DESCRIPTION
`system process-tuning logging nice-value <1...19>`	Specifies the priority for the Zyxel Device to process logs. Higher nice values indicate lower priority. Setting a higher value allows the Zyxel Device to process logs as less urgent, giving more CPU time to other processes. The default value is `10`.
`system process-tuning cpu-affinity-bit <1...3>`	Specifies which CPU core(s) are used to process logs. • `1` = core 1 • `2` = core 2 • `3` = core 1 + core 2 (default)

36.15 Statistics Commands

Use the statistics commands to allow statistics to be gathered on a port or interface. You must use the `edit running` command to enter the configuration mode before you can use the commands.

Table 163 Command Summary: Statistic

COMMAND	DESCRIPTION
`gui system statistics port <p1 | p2 | p3 | p4 | p5 | p6 | p7 | p8 | p9 | p10 | p11 | p12 | p13 | p14>`	Specifies the port on which you want to gather statistics. You may select up to 4 ports, separated by a space. For example, `gui system statistics port p1 p2 p3 p4`
`del gui system statistics port <p1 | p2 | p3 | p4 | p5 | p6 | p7 | p8 | p9 | p10 | p11 | p12 | p13 | p14>`	Stops the specified port from gathering statistics. You may select up to 4 ports, separated by a space. For example, `del gui system statistics port p1 p2 p3 p4`
`gui system statistics interface <ge1 | ge2 | ge3 | ge4 | cat | DMZ | vti_custom_1009>`	Specifies the interface on which you want to gather statistics. You may select up to 4 ports, separated by a space. For example, `gui system statistics interface ge1 ge2 ge3 ge4`
`del gui system statistics interface <ge1 | ge2 | ge3 | ge4 | cat | DMZ | vti_custom_1009>`	Stops the specified interface from gathering statistics. You may select up to 4 ports, separated by a space. For example, `del gui system statistics interface ge1 ge2 ge3 ge4`

36.16 ARP Commands

An ARP table maps IP addresses to MAC addresses. When those mappings become incorrect or outdated, problems can occur. Mappings may be incorrect if a device changes its MAC address (new network card), or if two devices accidentally share the same IP address, or there were network changes such as when a device changes VLANs, moves between switches or there are new routing or firewall rules. Instead of waiting for ARP entries to expire, clearing the ARP table forces immediate re-learning. However, in large

networks, clearing ARP tables can cause a temporary spike in broadcast traffic (ARP requests). So, rather than clearing the whole table, clear a specific ARP entry when the problem is isolated to one IP/MAC mapping and the rest of the network is working normally.

Table 164 Command Summary: ARP

COMMAND	DESCRIPTION
`cmd arp-table clear ip <ip-address>`	Removes a specific IP - MAC address mapping.
`cmd arp-table flush`	Removes all IP - MAC address mappings in the ARP table.
`show arp-table`	Displays he ARP table.

The following are some example clearing and flushing ARP commands. Use the show command to see the results of running a command.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# show arp-table
Address                 HWtype  HWaddress           Flags Mask            Iface
172.21.56.3              ether   c0:3f:d5:ba:9e:b7   C                     ge1
192.168.167.47           ether   78:c5:7d:45:27:47   C                     ge3
172.21.57.22             ether   24:4b:fe:e9:e6:c8   C                     ge1
192.168.169.33                   (incomplete)                              ge4
192.168.169.35           ether   14:36:0e:c8:59:b1   C                     ge4
172.21.59.254            ether   00:00:5e:00:01:04   C                     ge1
192.168.167.37           ether   14:36:0e:c8:59:e7   C                     ge3
192.168.167.33                   (incomplete)                              ge3
172.21.57.27             ether   f4:a8:0d:6c:c4:3f   C                     ge1
172.21.57.14             ether   a0:ad:9f:99:d1:ab   C                     ge1

MyUSGFLEX500H running config# cmd arp-table clear ip 172.21.56.3
OK.
MyUSGFLEX500H running config# show arp-table
Address                 HWtype  HWaddress           Flags Mask            Iface
192.168.167.47           ether   78:c5:7d:45:27:47   C                     ge3
172.21.57.22             ether   24:4b:fe:e9:e6:c8   C                     ge1
192.168.169.33                   (incomplete)                              ge4
192.168.169.35           ether   14:36:0e:c8:59:b1   C                     ge4
172.21.59.254            ether   00:00:5e:00:01:04   C                     ge1
192.168.167.37           ether   14:36:0e:c8:59:e7   C                     ge3
192.168.167.33                   (incomplete)                              ge3
172.21.57.27             ether   f4:a8:0d:6c:c4:3f   C                     ge1
172.21.57.14             ether   a0:ad:9f:99:d1:ab   C                     ge1
MyUSGFLEX500H running config# cmd arp-table flush
OK.
MyUSGFLEX500H running config# show arp-table
Address                 HWtype  HWaddress           Flags Mask            Iface
172.21.57.22             ether   24:4b:fe:e9:e6:c8   C                     ge1
172.21.59.254            ether   00:00:5e:00:01:04   C                     ge1
172.21.57.14             ether   a0:ad:9f:99:d1:ab   C                     ge1
172.21.57.27             ether   f4:a8:0d:6c:c4:3f   C                     ge1
```

36.16.1 ARP Spoofing

Use these ARP command to enable or disable ARP spoofing prevention.

ARP spoofing prevention verifies the ARP responses from client devices. If the IP and MAC addresses do not match the ARP table on the Zyxel Device, the Zyxel Device will refresh the ARP table to remove the falsified MAC mappings and create a log.

Table 165 Command Summary: ARP Spoofing

COMMAND	DESCRIPTION
`system network-stack arp-seal enabled {true| false}`	Refreshes the ARP table to remove the falsified MAC mappings and creates a log on the Zyxel Device when there is an ARP message that fails the ARP verification.
`show state system network-stack arp-seal`	Displays if the ARP spoofing prevention feature is enabled.

CHAPTER 37 System Remote Management

37.1 Remote Management Overview

This chapter shows you how to determine which services/protocols can access which Zyxel Device zones (if any) from which computers.

Note: To access the Zyxel Device from a specified computer using a service, make sure no service control rules or to-Zyxel Device firewall rules block that traffic.

You may manage your Zyxel Device from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

37.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the Zyxel Device will disconnect the session immediately.
3. There is a firewall rule that blocks it.

37.1.2 System Timeout

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

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

37.2 Common System Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 166 Input Values for General System Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the Zyxel Device model supports.
zone_object	The name of the zone. Ue up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

37.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 167 HTTP/HTTPS Commands

COMMAND	DESCRIPTION
`vrf main http-server server enabled {true| false}`	Enables HTTP access to the Zyxel Device web configurator. The `false` command disables HTTP access to the Zyxel Device web configurator.
`vrf main http-server server port <1...65535>`	Sets the HTTP service port number. The default port is 80.
`vrf main http-server server content-compression {true| false}`	Has the Zyxel Device compress data size before sending data to the clients.
`vrf main http-server server max-connection-per-ip <0...255>`	Sets the numbers of HTTP connections an IP address is allowed to access the Zyxel Device.
`vrf main http-server secure-server enabled {true| false}`	Enables HTTPS access to the Zyxel Device web configurator. The `false` command disables HTTPS access to the Zyxel Device web configurator.
`vrf main http-server secure-server customized exclude-protocol {TLSv1.3| TLSv1.2| TLSv1.1| TLSv1}`	Disables the specified TLS support in the HTTPS server.
`vrf main http-server secure-server customized exclude-ciphers {AES| CHACHA20| 3DES| DES| RC4}`	Has the Zyxel Device not use the specified encryption algorithm for the SSL in HTTPS connections.
`vrf main http-server secure-server port <1...65535>`	Sets the HTTPS service port number. The default port is 443.
`vrf main http-server secure-server force-https {true| false}`	Redirects all HTTP connection requests to a HTTPS URL. The `false` command disables forwarding HTTP connection requests to a HTTPS URL.

Table 167 HTTP/HTTPS Commands (continued)

COMMAND	DESCRIPTION
`vrf main http-server secure-server auth-client {true| false}`	Sets the client to authenticate itself to the HTTPS server. The `false` command sets the client not to authenticate itself to the HTTPS server.
`vrf main http-server secure-server certificate <certificate>`	Specifies a certificate used by the HTTPS server. The client will be required to send a certificate to create a secure connection with the Zyxel Device. Use up to 30 single-byte characters for the certificate name, including 0-9a-zA-Z;'~!@#$%^&()_+[]{}',.=-
`vrf main http-server secure-server compatibility {modern| intermediate| old}`	Sets the compatibility level of the HTTPS server. `modern`: This supports the least types of encryption algorithms. Select this to better protect your network. `old`: This supports the most types of encryption algorithms. Select this if your browser version is old.
`vrf main http-server security-options <security-options> {true| false}`	Sets the security methods for HTTP connections.
`vrf main http-server auth-server <1...2>`	Sets the web configurator login authentication using local account or external server according to the index order.
`vrf main http-server secure-server dhe-algo {true | false}`	Sets the DHE (Diffie-Hellman Ephemeral) key exchange algorithm that uses temporary Diffie-Hellman keys for each connection, so that new connections use a different key to old ones. DHE is disabled by default. If your client requires DHE, then use this command to enable it.
`show config vrf main http-server`	Displays the HTTP and HTTPS settings.
`show state vrf main http-server`	Displays the status of HTTP and HTTPS.

37.3.1 HTTP/HTTPS Command Examples

This following example shows how to:

- Set HTTPS certificate as a certificate named Test.
- Redirect all HTTP connection to use HTTPS connections.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main http-server secure-server certificate Test
usgflex200hp running config# vrf main http-server secure-server force-https true
usgflex200hp running config# commit
Configuration committed.
```

37.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

37.4.1 SSH Implementation on the Zyxel Device

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

37.4.2 Requirements for Using SSH

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

37.4.3 SSH Commands

The following table describes the commands available for SSH. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 168 SSH Commands

COMMAND	DESCRIPTION
`vrf main ssh-server enabled {true| false}`	Allows access to the Zyxel Device using SSH connections
`vrf main ssh-server address <`*`ip-address`*`>`	Sets the IPv4 address or domain of an SSH client.
`vrf main ssh-server port <`*`1...65535`*`>`	Sets the SSH service port number. The default port is 22.
`vrf main ssh-server certificate <`*`certificate`*`>`	Specifies a certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections.
`vrf main ssh-server dhe-algo {true | false}`	Sets the DHE (Diffie-Hellman Ephemeral) key exchange algorithm that uses temporary Diffie-Hellman keys for each connection, so that new connections use a different key to old ones. DHE is disabled by default. If your client requires DHE, then use this command to enable it.
`show config vrf main ssh-server`	Displays the SSH settings.
`show state vrf main ssh-server`	Displays: • If users are allowed to access the Zyxel Device using SSH connections • The SSH service port number • The IPv4 address or domain of the SSH clients.

37.5 FTP

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

37.5.1 FTP Commands

The following table describes the commands available for FTP. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 169 FTP Commands

COMMAND	DESCRIPTION
`vrf main ftp-server enabled {true| false}`	Allows access to the Zyxel Device using FTP connections.
`vrf main ftp-server port <1...65535>`	Sets the FTP service port number. The default port is 21.
`vrf main ftp-server tls-required {true| false}`	Allows FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and servers.
`vrf main ftp-server certficate <certificate>`	Specifies a certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections.
`vrf main ftp-server dhe_algo {true | false}`	Sets the DHE (Diffie-Hellman Ephemeral) key exchange algorithm that uses temporary Diffie-Hellman keys for each connection, so that new connections use a different key to old ones. DHE is disabled by default. If your client requires DHE, then use this command to enable it.
`show config vrf main ftp-server`	Displays the FTP settings.
`show state vrf main ftp-server`	Displays: • If users are allowed to access the Zyxel Device using FTP connections • The FTP service port number • The IPv4 address or domain of the FTP clients.

37.6 SNMP

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

SNMP v3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

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

37.6.1 Supported MIBs

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

37.6.2 SNMP Traps

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

Table 170 SNMP Traps

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

37.6.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 171 Command Summary: SNMP

COMMAND	DESCRIPTION
`vrf main snmp listen protocols <protocol> port <1...65535>`	Sets the SNMP listening port and protocol.
`vrf main snmp static-info location <location>`	Sets the geographic location (of up to 60 characters) for the Zyxel Device.
`vrf main snmp static-info contact <contact>`	Sets the contact information (of up to 60 characters) for the person in charge of the Zyxel Device.
`vrf main snmp static-info name <name>`	Specifies the username of a login account on the Zyxel Device.
`vrf main snmp community <community-name> authorization {read-only | read-write}`	Specifies the access right for the SNMP community. • `read-only`: Allows the manager to retrieve device data for monitoring, but prevents any configuration changes. • `read-write`: Allows the manager to retrieve and modify device data. Note: The Zyxel Device supports two SNMP communities, which can be either read-only or read-write. Managed APs with firmware version 7.20 or lower support only one read-only and one read-write SNMP community. Ensure that the firmware versions of both your Zyxel Device and managed APs are up to date.

37.6.4 System Advanced Commands

The following table describes the advanced commands for system. You must use the `edit running` command to enter the configuration mode before you can use these commands.

37.6.4.1 SecuManager

SecuManager is a management system that uses the NETCONF protocol (port 4335) to send commands to the Zyxel Devices for management and monitoring.

SecuManager features include:

- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Backup and restore device configuration

To allow SecuManager management of your Zyxel Device:

- You must have a SecuManager server URL or IP address.
- The Zyxel Device must be able to communicate with the SecuManager server.

When you enable SecuManager, you allow SecuManager to send and run commands (CLI scripts) on the Zyxel Device.

Note: If you enable SecuManager, NCC is automatically disabled and cannot manage the Zyxel Device.

Table 172 Command Summary: System Advanced

COMMAND	DESCRIPTION
`system drop-invalid-tcp-flags enabled {true | false}`	Allows the Zyxel Device to inspect TCP packets and drop any with invalid flags, such as FIN + SYN, FIN + RST, and SYN + RST flag combinations.
`system drop-invalid-tcp-flags logging {no | log | log-alert}`	Generates a log (`log`), log and alert (`log-alert`) or not (`no`) when the Zyxel Device detects an invalid TCP flag.
`system drop-syn-with-data enabled {true | false}`	When setting up a TCP connection, a SYN packet is used during the initial handshake to establish connection between two network devices, and typically does not carry any data payload. A SYN packet with a payload may indicate a potential attack, such as a SYN flood. Enable this to allow your Zyxel Device to drop SYN packets with a payload.
`system drop-syn-with-data logging {no | log | log-alert}`	Generates a log (`log`), log and alert (`log-alert`) or not (`no`) when there is a SYN packet with payload detected by the Zyxel Device.
`system drop-syn-with-data dst-port <0..65535>`	Drops SYN packets with a payload sent to the specified port. If set to 0, SYN packets with a payload sent to any port will be dropped.
`system drop-syn-with-data payload-size <1..65535>`	Drops SYN packets with a payload equal to or larger than the specified size (in bytes)
`system category-query-failopen enabled {true | false}`	A category server classifies IP addresses and URLs to different categories, such as anonymizers, browser exploits, and malicious downloads. Allows traffic to bypass checking (`true`) if the Zyxel Device cannot access the category server.

Table 172 Command Summary: System Advanced (continued)

COMMAND	DESCRIPTION
`system category-query-failopen log {no | log}`	Generates a log (`log`)or not (`no`) if the query to the category server fails.
`show config system drop-invalid-tcp-flags`	Displays the drop invalid TCP flags settings.
`show config system drop-syn-with-data`	Displays the drop sync with data settings.
`show config system category-query-failopen`	Displays the category query failopen settings when the Zyxel Device cannot access the category settings.
`secumanager enabled {true | false}`	Activates or deactivates SecuManager to manage the Zyxel Device. Note: If you enable SecuManager, NCC is automatically disabled and cannot manage the Zyxel Device.
`secumanager server {{`*`ip-address`*`| `*`fqdn`*`}}`	Sets the SecuManager server address. This should be an IPv4 address or a FQDN (Fully Qualified Domain Name), such as server01.corp.zyxel.com.
`secumanager server-ca <default |` *`certificate`*`>`	Sets the certificate the Zyxel Device uses to authenticate itself with the SecuManager.
`secumanager port <`*`port-number`*`>`	Sets the TCP port to communicate with SecuManager. Port 4335 (NETCONF) is the default. Note: Make sure port 4335 is not blocked by a security policy on the Zyxel Device.

37.6.5 System External Integrations Commands

Use these commands to integrate the Zyxel Device with other (third-party) cloud-based security platforms. At the time of writing, the Zyxel Device supports the Avast Business Hub, a cloud-based security platform where you can manage the endpoint devices to display:

- License information
- Device Insight details
- Security policy synchronization

The Avast Business Hub can also protect your endpoints, applications, and networks from:

- Ransomware (malware that encrypts your files preventing you from accessing them
- Phishing (fraudulent emails and messages seeking private information)
- Antivirus
- Web attacks.

You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 173 Command Summary: System External Integrations Commands

COMMAND	DESCRIPTION
`third-party-service avast client-id <client-id>`	Sets the `client-id` for authentication and authorization of the Zyxel Device with Avast. Avast API settings are the configurations within the Avast Business Hub for integrating the Zyxel Device with Avast. After you create your Avast account, go to the Avast Business Hub portal, then find **Integration** to see your **Client ID**.
`third-party-service avast client-secret <client-secret>`	Sets the `client-secret` for authentication and authorization of the Zyxel Device with Avast. Avast API settings are the configurations within the Avast Business Hub for integrating the Zyxel Device with Avast. After you create your Avast account, go to the Avast Business Hub portal, then find **Integration** to see your **Client Secret**.
`third-party-service avast client-secret-shadow <client-secret>`	Uses the *`client-secret-shadow`* command followed by the `client-secret` in plain text, to encrypt this `client-secret` in a saved configuration file. Valid plain text characters are [0-9][a-z][A-Z]['(){}<>^`+/ :!*#@&=$.~%|;-"] The password requires: • From 6 to 63 characters • At least 1 upper case letter • At least 1 digit • At least 1 special character.
`show third-party-service avast status`	Displays the Avast service status, such as client ID, client secret, last-sync, synch result, company ID, company name.

CHAPTER 38
File Manager

38.1 Configuration Files Overview

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include.

You can edit configuration files in a text editor and upload them to the Zyxel Device. Configuration files use a '.conf' extension.

38.1.1 Zyxel Device Configuration File Details

You can store multiple configuration files on the Zyxel Device. You can also have the Zyxel Device use a different configuration file without the Zyxel Device restarting.

- When you first receive the Zyxel Device, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the Zyxel Device creates a **startup-config.conf** file of the current configuration.
- The Zyxel Device checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the Zyxel Device copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.
- When the Zyxel Device reboots, if the **startup-config.conf** file passes the error check, the Zyxel Device keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

38.1.2 Configuration File Flow at Restart

You can manually restart the Zyxel Device through a management interface or by physically turning the power off and back on.

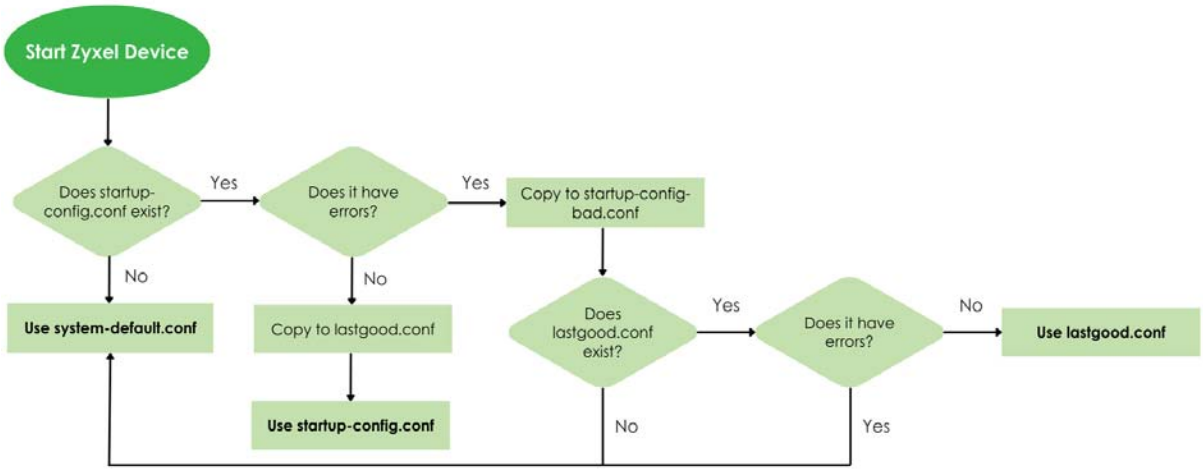
The Zyxel Device restarts automatically when you upload new firmware.

The Zyxel Device always checks for errors in any configuration file when rebooting. The Zyxel Device generates a log for any errors.

- If there is not a **startup-config.conf** when you restart the Zyxel Device, the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings. The Zyxel Device will apply the **system-default.conf** when it boots without a **startup-config.conf**, even if you have a **lastgood.conf**.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it if there are no errors. The Zyxel Device also copies it to the **lastgood.conf** configuration file as a back up file.
- If there is an error in **startup-config.conf**, the Zyxel Device generates a log and copies **startup-config.conf** to **startup-config-bad.conf** and then tries the existing **lastgood.conf** configuration file.

- If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.

Figure 103 Zyxel Device Start-up Flow



38.1.3 Recovery Manager

Use this to create a complete recovery backup file of the Zyxel Device that can be used if the Zyxel Device needs to be replaced or you want to sell it to someone else. You should save a backup or recovery file to your computer each time you make a configuration change. The recovery file can then be restored on a replacement Zyxel Device. You must set a password for the recovery file. The password must be 8 to 128 characters long, and can contain [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,.?]. Write this password down in a safe place as it will be required if you want to restore this configuration on a replacement Zyxel Device later.

Note: Use the Web Configurator (**Recovery Manager** in **Maintenance > Firmware/File Manager > Configuration File**) to create a recovery file with a '.rbf' extension first.

The recovery file includes the following:

Configuration files

Contains all configuration files.

Certificates

- My Certificates (Site-to-Site VPN, Remote access VPN)
- SSL VPN Certificates
- Trusted Certificates: Certificates that you have set the Zyxel Device to accept as trusted.

Google Authenticator File

Contains two-factor authentication (2FA) information. Google Authenticator adds an extra layer of security for local users accessing the Zyxel Device or a secured network behind the Zyxel Device through a VPN tunnel.

38.1.3.1 Downloading the Complete Recovery File

At the time of writing, there is no CLI command to download the recovery backup file to your computer. Go to **Recovery Manager** in **Maintenance > Firmware/File Manager > Configuration File** the Web Configurator to create a recovery file. You can also download the recovery file using the Web Configurator to your computer. See the USG FLEX H Series User Guide to explain how to use the Web Configurator to do these. After you've created a recovery file in the Web Configurator, you can also use FTP to download it to your computer.

Steps to Download Using FTP:

1 Find the Recovery File Name

Use the command `show system backup status` to find the name of the recovery file on the Zyxel Device. The file name should be in the following format: Hostname_Recovery_YYYY-MM-DD.rbf', where YYYY-MM-DD is the date created, and host name is the name you gave this Zyxel Device. This is an example file name: 'MyUSGFLEX500H_Recovery_2025-07-28.rbf'

2 Download the Recovery File

Run an FTP client to download the recovery file from the Zyxel Device at: /tmp/ Hostname_Recovery_YYYY-MM-DD.rbf.

Example FTP Commands:

```
open 192.168.168.1
Name: xxxx
Password: xxxx
ftp> get /tmp/Hostname_Recovery_YYYY-MM-DD.rbf
```

3 Restore the Recovery File on the Replacement Zyxel Device

Go to the **Maintenance** > **Firmware/File Manager** > **Configuration File** on the Web Configurator of the replacement Zyxel Device to upload the saved recovery file, such as 'MyUSGFLEX500H_Recovery_2025-07-28.rbf'. To restore the recovery file you must use the password that you configured when you downloaded the file in **Recovery Manager** in **Maintenance > Firmware/File Manager > Configuration File** the Web Configurator.

38.2 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

Table 174 File Manager Command Input Values

LABEL	DESCRIPTION
file-name	The name of a file. Use up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.

38.3 File Manager Commands Summary

The following table lists the commands that you can use for file management. You must use the `edit running` command before you can use these commands.

Table 175 File Manager Commands Summary

COMMAND	DESCRIPTION
`cmd config-copy from <file-name> to <file-name>`	Saves a duplicate of a file on the Zyxel Device from the source file name to the target file name. Specify the file name of the file that you want to copy and the file name to use for the duplicate. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-rename from <file-name> to <file-name>`	Changes the name of a file. Specify the file name of the file that you want to rename. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-delete <file-name>`	Removes a file. Specify the file name of the file that you want to delete. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-mail send-now <file-name>`	Has the Zyxel Device sends the specified configuration file to the configured email addresses. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-apply <file-name>`	Has the Zyxel Device use a specific configuration file. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-apply system-default.conf`	Returns the Zyxel Device to the default configuration using the system-default.conf file. All configuration files including those you saved on the Zyxel Device will be deleted. The Login password returns to the password on the back label or 1234, and the LAN IP address returns to 192.168.168.1. License registration bindings, IPSec certificates, remote access VPN certificates, trusted certificates and two-factor authentication (2FA) information are retained.
`cmd config-apply option {dry-run | ignore-error | copy-reboot} <file-name>`	Has the Zyxel Device check or apply a specific configuration file to the Zyxel Device. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf. • `dry-run`: Check the specified configuration file without applying any changes to the Zyxel Device. • `ignore-error`: Apply the specified configuration file to the Zyxel Device even if errors occur. This allows the Zyxel Device to apply the correct parts of the configuration. This is not recommended. • `copy-reboot`: Use the specified configuration file as the startup configuration file and reboot the Zyxel Device.
`cmd config-apply-status`	Shows the result of the `dry-run` check.

Table 175 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
`gui system standby-firmware-display {true| false}`	By default, the web configurator displays the current active partition. When enabled, the Zyxel Device also displays the standby partition in the web configurator.
`show dir config-file-standby`	Displays the details of the configuration files stored on the standby partition on the Zyxel Device. • File name: This is the name of the configuration file. • Size: This is the size of the configuration file. • Modified time: This is the date and time that the configuration file was created.

38.4 File Manager Backup Commands Summary

The following table lists the commands that you can use to back up configuration files.

Table 176 File Manager Backup Commands Summary

COMMAND	DESCRIPTION
`configuration auto-backup enabled {true| false}`	Backs up the configuration file at a user defined schedule. Note: After the first backup, the back up only occurs if the configuration file is different from the previous backed up configuration file.
`configuration auto-backup schedule daily time <hh:mm>`	Has the Zyxel Device back up its configuration file once a day at the specified hour and minute.
`configuration auto-backup schedule weekly week-day <week-day> time <hh:mm>`	Has the Zyxel Device back up its configuration file once a week on the specified day, at the specified hour and minute.
`configuration auto-backup schedule monthly month-day <month-date> time <hh:mm>`	Has the Zyxel Device back up its configuration file once a month on the specified day, at the a specified hour and minute. Note: If the date you select is greater than the number of days in a month, the Zyxel Device automatically backs up its configuration file on the last day of the month. For example, if you select 31 and the month is February, the Zyxel Device backs up its configuration file on day 28 or 29.
`configuration auto-backup send-email-enabled {true| false}`	Has the Zyxel Device send an email when it automatically backs up its configuration file.
`configuration email recipient <email-address>`	Sets the email address of the receiver(s). Use a valid email address of up to 83 characters for each email address. You can send the configuration file to a maximum of five email addresses.
`configuration email subject <subject>`	Sets an email subject for the emailed configuration file. Use 1 to 60 letters, numbers, and the following special characters: ‘()+,./:=?;!*#@$%-
`configuration email content <content>`	Sets the email body text for the emailed configuration file. Use 1 to 251 single-byte characters, including 0-9a-zA-Z!"#$%&’()*+,-./:;<=>@[\]^_‘{|} and spaces are allowed. ? is not allowed.

Table 176 File Manager Backup Commands Summary (continued)

COMMAND	DESCRIPTION
`configuration email encryption-key <key>`	Sets an unzip password for the emailed configuration file. The recipient must use this password to unzip the configuration file. Use up to 128 characters. Valid characters are [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,./]. If you do not set a password here, then none is needed to unzip the configuration file.
`configuration email encryption-key-shadow <key>`	Sets a shadow key for the unzip configuration file password. A shadow key can change the encryption key into a random sequence of letters and numbers and also change those back to the actual encryption key. Use up to 128 characters. Valid characters are [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,./].
`configuration auto-backup backup-rotation <1 - 50>`	Sets a newer backup to replace the oldest backup when the number you enter here is reached. Enter a number from 1 to 50. For example, if you use 50, then the 51st backup configuration file will replace the first configuration file. You will always have a maximum of 50 backup configuration files.
`cmd config-mail send-now file-name <file-name> recipient <email-address> content <content> subject <subject> encryption-key <key>`	Immediately emails the specified configuration file to the recipient with optional content, subject and encryption key. Put the content and subject in single quotes. • *file-name:* (Required) This is name of the configuration file on the Zyxel Device. Use up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf. • *email-address:* (Required) Use a valid email address of up to 83 characters. • *content:* (Optional) Use 1 to 251 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;<=>@[\]^_'{|} and spaces are allowed. ? is not allowed. • *subject:* (Optional) Use 1 to 60 letters, numbers, and the following special characters: '()+,./:=?;!*#@$%- • *key:* (Optional) Use up to 128 characters. Valid characters are [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,./]
`cmd config-copy from {start|running} to usb`	Has the Zyxel Device save the starting or running configuration file to your USB stick in the modelname_dir/conf folder. The saved configuration file is displayed as startup-yyyy-mm-dd-hh-mm.conf or running yyyy-mm-dd-hh-mm.conf. • `start`: startup-config.conf • `running`: the running configuration file on your Zyxel Device You must choose FAT32 as the USB file system. If no USB stick is connected to your Zyxel Device, this command will fail.
`cmd system backup password <password>`	Sets a password for the configuration backup ZIP file. You will need this password to upload the configuration file to the Zyxel Device. The password can contain 8 to 128 single-byte characters. Valid characters are [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,.?].
`show system backup status`	Displays the status of the file backup. • `Done`: The ZIP file has been successfully saved to the Zyxel Device. • `None`: Displays after a success recovery or the ZD still didn't send the backup command yet. • `Failed`: Displays when the last backup attempt failed. You can check the details of the failure in the web configurator log page or use the "show logging" command.

38.4.1 Email Configuration Command Example

The following command example sends the lastgood.conf configuration file to the recipient with email content as 'This is a test', email subject as "Test from ZyWALL' and an unzip key of 1234.

```
usgflex500h running config# cmd config-mail send-now file-name lastgood.conf
recipient john@zyxel.com.tw content 'This is a test' subject 'Test from ZyWALL'
encryption-key 1234
configuration-email
    ok
        message OK
        ..
    ..
usgflex500h running config#
```

38.5 Cloud Helper Commands

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

Note: Go to myZyxel, create an account and register your Zyxel Device first. Then you will be able to get notifications on new firmware available when you log into the Zyxel Device web configurator.

Table 177 Cloud Helper Commands

COMMAND	DESCRIPTION
`cloud-helper firmware auto-update {true| false}`	Lets the Zyxel Device automatically check for and download new firmware at the time and day specified.
`cloud-helper firmware auto-reboot {true| false}`	Lets the Zyxel Device automatically reboot when new firmware is downloaded to the Zyxel Device.
`cloud-helper firmware update-schedule daily <0...23>`	Has the Zyxel Device check for new firmware every day at the specified time. The time format is the 24 hour clock, so '0' means midnight, 01 means 1AM and so on. Set `cloud-helper firmware auto-reboot` to `yes` to have the Zyxel Device automatically restart when new firmware is downloaded to the Zyxel Device.
`cloud-helper firmware update-schedule weekly <week-day> time <0...23>`	Has the Zyxel Device check for new firmware once a week on the day and at the time specified. The time format is the 24 hour clock, so '0' means midnight, 01 means 1AM and so on. Set `cloud-helper firmware auto-reboot` to `yes` to have the Zyxel Device automatically restart when new firmware is downloaded to the Zyxel Device. If you configure both weekly and daily commands, then the command that takes effect is the last one configured.
`cmd cloud-helper get firmware <1..2>`	Downloads the latest firmware on the Cloud Helper server to the specified system space on the Zyxel Device.
`cmd cloud-helper pause-download firmware <1..2>`	Temporarily stops a firmware being downloaded to the specified system space on the Zyxel Device.

Table 177 Cloud Helper Commands (continued)

COMMAND	DESCRIPTION
`cmd cloud-helper clean-download firmware <1..2>`	Stops and removes a firmware being downloaded to the Zyxel Device.
`show cloud-helper firmware download-status`	Displays the download status of the firmware that is downloaded to the Zyxel Device from the Cloud Helper server.

38.6 Firmware Commands

You must use the `edit running` command before you can use these commands.

Table 178 Firmware Commands

COMMAND	DESCRIPTION
`cmd firmware upgrade-1 image <file-name>`	Uploads the specified firmware image to boot partition 1.
`cmd firmware upgrade-2 image <file-name>`	Uploads the specified firmware image to boot partition 2.
`cmd firmware boot-number <1 | 2>.`	Specifies which boot partition firmware image, 1 or 2, to use when the Zyxel Device reboots.
`cmd firmware boot-option <0 | 1>.`	Specifies whether to reboot the Zyxel Device after a successful firmware upgrade. Specify `0` to reboot, `1` to not reboot.
`cmd firmware remove-backup boot-number <1 | 2>`	Removes the option of which boot partition firmware image, 1 or 2, to use when the Zyxel Device reboots.
`cmd firmware remove-backup boot-option <0 | 1>`	Removes the option to reboot the Zyxel Device, (`0` to reboot, `1` to not reboot), after a successful firmware upgrade.
`gui system standby-firmware-display <true | false>`	By default the web configurator does not show the running and standby boot partitions. Use `true` to display both boot partitions and display the option to reboot in the web configurator when uploading new firmware. Selecting reboot will make the uploaded firmware the running firmware after the Zyxel Device restarts. Use `false` to return to the default and not have the web configurator show the running and standby boot partitions nor display a reboot option. The Zyxel Device restarts automatically in this case, making the uploaded firmware the running firmware after the Zyxel Device restarts.
`show firmware <boot-option | boot-number>`	Displays the configured Zyxel Device firmware boot option or boot number as configured above.
`show gui dashboard boot-status`	Displays when the Zyxel Device was last updated with new firmware. For example, 'status OK'. detail "Firmware update at 2024-02-02 09:31"

CHAPTER 39
Packet Flow Explore

39.1 Packet Flow Explore

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

39.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the Zyxel Device display routing and SNAT related settings. Use these commands to display routing and NAT flows through the Zyxel Device.

Table 179 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`cmd debug network packet-flow-explore routing vpn`	Displays where packets are forwarded according to the criteria set in IPSec Site-to-Site VPN commands. See Section 16.2.1 on page 143 for more information about IPSec Site-to-Site VPN commands.
`cmd debug network packet-flow-explore routing direct-route`	Displays packets sent to directly connected subnets.
`cmd debug network packet-flow-explore routing policy-route`	Displays where packets are forwarded according to the criteria set in Policy Route commands. See Section 8.3 on page 97 for more information about Policy Route commands.
`cmd debug network packet-flow-explore routing nat`	Displays how an internal private IP address is mapped to a single external public IP address for outbound traffic.
`cmd debug network packet-flow-explore routing static-route`	Displays where packets are forwarded according to the criteria set in Static Route commands. See Section 8.5 on page 101 for more information about Static Route commands.
`cmd debug network packet-flow-explore routing nebula-static-route`	Displays the static route created when you are using Nebula VPN.
`cmd debug network packet-flow-explore routing wan-trunk`	Displays packets forwarded to the active interface in a WAN trunk and then onto the destination IP address.
`cmd debug network packet-flow-explore routing main-route`	Displays the default routing table of the Zyxel Device system kernel where packets are forwarded onto the destination IP address.
`cmd debug network packet-flow-explore snat site-to-site-vpn`	Displays how SNAT for policy-based Site-to-Site IPsec VPN maps all internal private IP addresses of a site to a single IP address for outbound traffic.
`cmd debug network packet-flow-explore snat policy-route`	Displays where packets are forwarded according to the criteria set in Policy Route commands, with the private source IP address of the sender replaced with a public IP address for outbound traffic. See Section 8.3 on page 97 for more information about Policy Route commands.

Table 179 Packet Flow Explore Commands (continued)

COMMAND	DESCRIPTION
`cmd debug network packet-flow-explore snat nat`	Displays how 1-1 SNAT maps an internal private IP address to a single external public IP address for outbound traffic.
`cmd debug network packet-flow-explore snat nat-loopback`	Displays how loopback SNAT maps an internal private IP address to the public IP address of an internal server.
`cmd debug network packet-flow-explore snat default-snat`	Displays how SNAT maps internal private IP addresses to a single external public IP address for outbound traffic.

CHAPTER 40
Logs

40.1 Logs Overview

This chapter provides information about the Zyxel Device's logs. When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the Zyxel Device.

40.2 Log Command Input Values

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

Table 180 Log Command Input Values

LABEL	DESCRIPTION
interface	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. Virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 Bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. Virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE interfaces your Zyxel Device model supports.
source	The name of the category. The `default` category includes debugging messages generated by open source software. The `all` category includes all messages in all categories.
protocol	The name of a protocol such as TCP, UDP, ICMP.

40.2.1 Log General Commands

This table lists the log general commands.

Table 181 Log General Commands

COMMAND	DESCRIPTION
`logging log-statistic enabled {true| false}`	Has the Zyxel Device count how many logs there are in different categories.
`show logging last-boot entries`	Displays the log entries saved before the Zyxel Device reboots.
`show logging status`	Displays the Zyxel Device log settings status.
`show logging _source mapping`	Displays the mapping between the log categories and the associated IDs.
`show logging log-statistics`	Displays the number of logs in different categories.
`show logging log-drop-count`	Displays the number of dropped logs in different categories.
`system process-tuning logging nice-value <1...19>`	Specifies the priority for the Zyxel Device to process logs. Higher nice values indicate lower priority. A higher nice means 'be nicer' to other processes (use the CPU last). Setting a higher value allows the Zyxel Device to process logs as less urgent, giving more CPU time to other processes. The default value is `10`.
`system process-tuning cpu-affinity-bit <1...3>`	Specifies which CPU core(s) are used to process logs. If logging traffic is not very high, you can use one core and free up the other core for applications other than logging. • `1` = core 1 • `2` = core 2 • `3` = core 1 + core 2 (default)

40.2.2 Log Entries Commands

This table lists the commands to look at log entries.

Table 182 Log Entries Commands

COMMAND	DESCRIPTION
`show logging entries {details idkey id| priority priority| source source| srcip ipv4| src-geoip country| sport source-port| dstip ipv4| dst-geoip country| dport destination-port| srciface interface| dstiface interface| protocol protocol| keyword keyword| line-range begin number end number}`	Displays the specified entries in the system log. `keyword`: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields.

40.2.3 System Log Commands

This table lists the current `source` categories.

Table 183 Source Categories

default	secure-policy	anti-malware	tailscale
content-filter	ip-reputation	external-block-list	connectivity-check
user	ssl-inspection	built-in-service	license
pki	dos-prevention	policy-route	cloud-helper
system	ips	static-route	interface-statistics
system-monitoring	url-threat-filter	dhcp	traffic-log
session-monitor	ip-exception	ike	secureporter
app-patrol	dns-threat-filter	ssl-vpn	daily-report
device-insight	sandboxsandbox-statistics	session-control	bwm
traffic-statistics	fqdn-object	spoofing-prevention	captive-portal
device-ha	cdr	igmp	

This table lists the commands for the system log settings.

Table 184 System Log Commands

COMMAND	DESCRIPTION
`logging system-log source {all | source-list <source>} level {disable | normal | all)`	Specifies what kind of information, if any, is logged in the system log for the specified category. Use `all` to select all categories. `level` indicates the type of system logs to log for the specified source. `normal`: logs info, notice, warning, error, critical, alert, and emergency logs for the specified source. `all`: logs normal and debug logs for the specified source `disable`: no logging for the specified source
`logging system-log suppression enabled {true| false}`	Enables log consolidation in the system log.
`logging system-log suppression interval <10...600>`	Sets the log consolidation interval for the system log. The default value is 10.

40.2.3.1 System Log Command Examples

The following command displays the current status of the system log.

```
usgflex200hp> edit running
usgflex200hp running config# show logging status system-log
show-zylog-status-system-log
    ok
        events-logged 13
        suppression-active false
        suppression-interval 10
        source-list default
            level all
            ..
        source-list content-filter
            level normal
            ..
        source-list forward-web-sites
            level normal
            ..
        source-list blocked-web-sites
            level normal
            ..
        source-list warning-web-sites
            level normal
            ..
        source-list user
            level normal
            ..
        source-list pki
            level normal
```

40.2.4 Debug Log Commands

This table lists the commands for the debug log settings.

Table 185 Debug Log Commands

COMMAND	DESCRIPTION
`show logging debug entries {details idkey` ***`id`*** `| priority` ***`priority`*** `| source` ***`source`*** `| srcip` ***`ipv4`*** `| dstip` ***`ipv4`*** `| srciface` ***`interface`*** `| dstiface` ***`interface`*** `| protocol` ***`protocol`*** `| keyword` ***`keyword`*** `| line-range begin` ***`number`*** `end` ***`number`*** `}`	Displays the specified entries in the debug log.

40.2.5 Remote Syslog Server Commands

This table lists the commands for the remote syslog server settings.

Table 186 Remote Syslog Server Commands

COMMAND	DESCRIPTION
`logging syslog remote-server <1...4> source {all| source-list source}`	Specifies what kind of information, if any, is logged in the specified syslog remote server for the specified category. Uses `all` to select all categories.
`logging syslog remote-server <1...4> enabled {true| false}`	Enable the specified remote server.
`logging syslog remote-server <1...4> server-address <ipv4-address>`	Sets the IPv4 address of the specified remote server.
`logging syslog remote-server <1...4> server-port <port-number>`	Sets the port of the specified remote server.
`logging syslog remote-server <1...4> log-format {cef| syslog}`	Sets the format of the log information. `cef`: Common Event Format, syslog-compatible format. `syslog`: syslog format.
`logging syslog remote-server <1...4> facility {local_1| local_2| local_3| local_4| local_5| local_6|local_7}`	Sets the log facility for the specified remote server.

40.3 USB Storage Commands

The Zyxel Device can use a connected USB device to store system logs, diagnostic information and firmware.

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

For Zyxel Devices that have more than one USB port, these commands only apply to the first USB storage device that is attached to the Zyxel Device.

Use these commands to configure settings that apply to the USB storage device connected to the Zyxel Device.

You must use `edit running` to be in configuration mode to use the indented commands shown below.

Table 187 USB Storage Commands

COMMAND	DESCRIPTION
`logging usb-storage enabled {true| false}`	Enable or disable the connected USB storage service.
`logging usb-storage keep-duration enabled {true| false} duration <1...365>`	Sets a number of days that the Zyxel Device keeps the log.

Table 187 USB Storage Commands (continued)

COMMAND	DESCRIPTION
`logging usb-storage source {all| source-list source}`	Sets the logging settings for the specified category for the connected USB storage device. Uses `all` to select all categories.
`logging usb-storage flush-threshold <1...100>`	Sets the maximum number of logs the Zyxel Device can store. When the number of logs exceeds the threshold you set, new logs will be stored in the connected USB storage device.
`logging usb-storage log-rotate enabled {true| false}`	Maximizes the size of a file containing logs on the USB drive/stick. Any number of files, each up to the maximum size, can be saved to the USB drive/stick daily. For example, 2024-09-19.log.1 and 2024-09-19.log.2. can be saved to the USB drive/stick in one day.
`logging usb-storage log-rotate size <1...1000>`	Sets the maximum size of a file containing logs on the USB drive/stick. For example, if you set this to 100MB, and the 2024-09-19.log file exceeds 100MB, then the contents of 2024-09-19.log is moved to 2024-09-19.log.1, so that logs can be added to 2024-09-19.log again. If the 2024-09-19.log.1 already exists, then 2024-09-19.log.1 is renamed to 2024-09-19.log.2, and its content is then moved from 2024-09-19.log to 2024-09-19.log.1.
`logging usb-storage log-rotate compress {true| false}`	Enables gzip to compress log files to reduce size. You will be able to save more log files to the USB drive/stick, but you will have to have to unzip them first to perform analysis of the logs. Rotated compressed log files, for example, 2024-09-19.log.1.gz, 2024-09-19.log.2.gz etc., are saved on the USB drive/stick.
`logging usb-storage log-rotate check-period <1...360>`	Sets how often to check log file sizes on the USB drive/stick. The range is from 1 to 360 minutes. The default is 5 minutes.
`logging usb-storage disk-full-warning enabled {true| false}`	Enable to create a log when the available space on the USB drive/stick connected to the Zyxel Device is below the specified threshold. One log of type warning is sent every 24 hours if the USB drive/stick is not full, but the remaining space is less than the specified threshold. One log of type alert (with email) is sent every 4 hours if the USB drive/stick is full, that is, there is no available space left. For example, say the USB Disk full Threshold is 200 MB. • If the space available on the USB drive/stick is 300 MB, then no log is sent. • If the space available on the USB drive/stick is 199 MB, then a log of type warning is sent to notify that there is available space, but it is less than threshold. • If the space available on the USB drive/stick is 0 MB, then a log of type alert and an email is sent to notify that there is no available space left on USB drive/stick.
`logging usb-storage disk-full-warning threshold <100..9999>`	Sets the minimum size needed to save logs to the connected USB drive/stick (100 to 9999) in MB. When the available space on the USB drive/stick is below this value, a log will be created.
`logging usb-storage disk-full-warning purge-oldest-file {true| false}`	If the available space on the USB drive/stick is below the specified threshold, the oldest log files will be removed until the available space is above the threshold. Removes the oldest logs (`true`) when the available space is below the threshold. Then, the new logs can be saved to the USB drive/stick. If the USB drive/stick has just one log file (no older log files), then purge file will fail.

Table 187 USB Storage Commands (continued)

COMMAND	DESCRIPTION
`show-usb-storage`	Displays information about the USB storage device connected to the Zyxel Device: • USB storage device name • Used space (in MB or GB), available space (in MB or GB), and the percentage of used space • File system • Supported USB standard and connection speed • Connection status
`cmd usb-storage unmount`	Disconnects the USB storage device from the Zyxel Device.
`cmd usb-storage mount`	If you use `cmd usb-storage unmount` to disconnect the USB storage device from the Zyxel Device, you can then use `cmd usb-storage mount` to reconnect the USB storage device.

40.3.1 USB Storage Command Example

The following example shows information about the USB storage device connected to the Zyxel Device.

```
usgflex500h> edit running
usgflex500h> show usb-storage
    ok
        device-description "SMI USB DISK"
        usage "156.7MB / 3.9GB"
        usage-percent 3.9
        filesystem FAT32
        speed "USB 2.0 480Mbps"
        status Connected
        result ""
        ..
    ..
```

40.4 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

Table 188 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
email-address	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the Zyxel Device send various statistics reports every day. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 189 Email Daily Report Commands

COMMAND	DESCRIPTION
`system daily-report enabled {true| false}`	Enable to send reports by email every day.
`system daily-report report-items {cpu-usage| mem-usage| port-usage| session-usage| interface-usage| app-patrol| content-filter| anti-malware| ip-reputation| ips| dhcp| stationCount| txStatistics| rxStatistics} {true| false}`	Specifies the information to include in the report. `port-usage` includes data for all ports. `interface-usage` includes only the interface data specified by the statistics commands. See Section 36.15 on page 317 for more information.
`system daily-report mail to <email-address>`	Sets the email address (or addresses) to which the outgoing email is delivered.
`system daily-report mail subject append-system-name {true| false}`	Determines whether the system name will be appended to the subject of the report e-mails.
`system daily-report mail subject append-date-time {true| false}`	Determines whether the sending date and time will be appended at subject of the report e-mails.
`system daily-report mail subject set <mail-subject>`	Sets the subject line for outgoing email from the Zyxel Device. You can use up to 60 single-byte characters, including 0-9a-zA-Z'()+,./:=?;!#@$_%-
`system daily-report schedule <hh:mm>`	Sets the time of the day the report is emailed.
`system daily-report reset-counter {true| false}`	Determines whether or not to start all of the report statistics data counters over at zero every 24 hours.
`cmd system daily-report send now`	Sends the daily e-mail report immediately.

40.4.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Enables reporting.
- Sets the subject of the report e-mails to test.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as my-email@example.com.
- Sets the sender as receiver@example.com.
- Sets the Zyxel Device to send the report at 1:57 PM.
- Has the Zyxel Device not reset the counters after sending the report.

- Has the report include CPU, memory, and session usage.

```
usgflex200hp> edit running
usgflex200hp running config# system daily-report enabled true
usgflex200hp running config# system daily-report mail subject set test
usgflex200hp running config# system daily-report mail subject append-system-name
false
usgflex200hp running config# system daily-report mail subject append-date-time true
usgflex200hp running config# system daily-report mail from my-email@example.com
usgflex200hp running config# system daily-report mail to receiver@example.com
usgflex200hp running config# system daily-report schedule 13:57
usgflex200hp running config# system daily-report reset-counter false
usgflex200hp running config# system daily-report report-items cpu-usage true
usgflex200hp running config# system daily-report report-items mem-usage true
usgflex200hp running config# system daily-report report-items session-usage true
usgflex200hp running config# commit
Configuration committed.
```

40.5 Log Setting Commands

Use these commands to control log messages.

- WTP (Wireless Terminal Point) logs relate to logs for WiFi clients such as APs, extenders, laptops, and mobile phones.
- APC (Access Point Controller) logs relate to logs for the AP Controller.

Table 190 Log Setting Commands

COMMAND	DESCRIPTION
`wtp-logging system-log source <all | source-list source enabled {true | false}`	Specifies selected types of system WTP logs to retrieve. Specific sources are for troubleshooting by qualified technicians only.
`wtp-logging syslog remote-server {1..4}`	Specifies a syslog server to configure on the managed WTP. You may specify log types for up to 4 syslog servers. See Section 40.2.5 on page 343 for remote server configurations
`wtp-logging syslog remote-server {1..4} source <all | source-list source enabled {true | false}`	Sends selected types of logs to the specified syslog server.
`cmd wtp-logging query-log <mac-address>`	Has the Zyxel Device retrieve logs from the WTP specified by MAC address.
`cmd logging clear wtp-logging ap-mac <mac-address>`	Deletes the WTP log cache on Zyxel Device and flushes zylogs on the the WTP with the given MAC address.
`show wtp-logging entries priority <emergency | alert | critical | error | warning | notice | info | debug>`	Displays WTP logs with equal or higher priority than the indicated priority. Priorities are listed here from highest to lowest.
`show wtp-logging entries source source`	Displays WTP logs from the specified source.
`show wtp-logging entries keyword <keyword>`	Displays WTP logs containing the specified keyword.
`show wtp-logging entries line-range begin <num> end <num>`	Displays the specified number of WTP log entries.

Table 190 Log Setting Commands (continued)

COMMAND	DESCRIPTION
show wtp-logging result-status	Displays WTP log status such as AP info, current query status, last time queried and log file status.
apc-logging system-log source <all | source-list *source* enabled {true | false}	Specifies selected types of system APC logs to retrieve. Specific sources are for troubleshooting by qualified technicians only.
apc-logging usb-storage source all level <disable | normal | all>	Specifies selected levels of APC logs to send to USB storage.
apc-logging usb-storage source source-list *source*	Specifies selected types of APC logs to send to USB storage. Specific sources are for troubleshooting by qualified technicians only.
apc-logging syslog remote-server <*num*> source <all | source-list *source* enabled {true | false}	Specifies selected types of APC logs to send to a specified syslog server.
show logging apc	Displays all AP Controller (APC) logs.
show logging lastboot apc	Displays AP Controller (APC) logs since the last time the APC booted..
show logging apc _source mapping	Displays AP Controller (APC) logs by category.
show logging apc keyword <*keyword*>	Displays AP Controller (APC) logs containing the keyword.

40.5.1 Log Setting Command Examples

This example shows the WTP log settings for system logs.

```
usgflex500h> edit running
usgflex500h running config# wtp-logging system-log source all enabled true
usgflex500h running config# commit
usgflex500h running config# copy running startup
```

This example shows the WTP log settings for remote syslog server 1.

```
usgflex500h> edit running
usgflex500h running config# wtp-logging syslog remote-server 1 source all enabled
false
usgflex500h running config# wtp-logging syslog remote-server 1 source source-list
user enabled true
usgflex500h running config# wtp-logging syslog remote-server 1 source source-list
pki enabled true
usgflex500h running config# wtp-logging syslog remote-server 1 source source-list
dhcp enabled true
usgflex500h running config# commit
usgflex500h running config# copy running startup
```

CHAPTER 41
SecuReporter

41.1 SecuReporter Overview

SecuReporter is a security analytics portal accessible, that collects and analyzes logs from SecuReporter-licensed Zyxel Devices in order to identify anomalies, alert on potential internal / external threats, and report on network usage.

You need to buy a SecuReporter license for your Zyxel Device and register it at myZyxel using your myZyxel account. The SecuReporter license must be activated on each Zyxel Device. The Zyxel Device must be able to communicate with the myZyxel server.

41.1.1 SecuReporter Commands

SecuReporter stores logs in a temporary file for uploading to the SecuReporter portal for security analysis. How often to upload is determined by the upload interval (default every 600 seconds) or upload file size (default is when the temporary log file reaches 10 MB). More frequent uploads provides better real-time log analysis, but uses more network bandwidth and Zyxel Device CPU processing power.

You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 191 SecuReporter Commands

COMMAND	DESCRIPTION
`vrf main secureporter enabled {true| false}`	Sends security-related logs to the SecuReporter portal. Uses `false` to disable SecuReporter logging. SecuReporter must be enabled to collect and analyze logs from this Zyxel Device. • You must read and accept the General Data Protection Regulation (GDPR) privacy policy by enabling SecuReporter in the Web Configurator before you can enable it by using the CLI. • SecuReporter is enabled by default if you have activated a SecuReporter Standard license, • SecuReporter is disabled by default if you have a SecuReporter Trial license. • You cannot enable SecuReporter if you do not have a SecuReporter license.
`vrf main secureporter upload-filesize <1...10>`	A temporary log file is uploaded to the SecuReporter security analytics portal when it meets the size set here (in megabytes) or the interval defined in the following field. 10 MB is the default. Set it to a smaller number for more frequent uploads.
`vrf main secureporter upload-interval <60...600>`	A temporary log file is uploaded to the SecuReporter security analytics portal at the interval defined here or when it meets the size set in the previous field. 600 seconds is the default. Set it to a smaller number for more frequent uploads.
`vrf main secureporter app-patrol enabled {true| false}`	The `true` command will have the Zyxel Device send application patrol logs to SecuReporter for analysis and trend spotting.

Table 191 SecuReporter Commands (continued)

COMMAND	DESCRIPTION
`vrf main secureporter anti-malware enabled {true| false}`	The `true` command will have the Zyxel Device send anti-malware logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter threat-protection enabled {true| false}`	The `true` command will have the Zyxel Device send IPS and DoS prevention logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter content-filter enabled {true| false}`	The `true` command will have the Zyxel Device send content filtering logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter reputation-filter enabled {true| false}`	The `true` command will have the Zyxel Device send IP reputation and URL Threat filter logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter traffic-log enabled {true| false}`	The `true` command will have the Zyxel Device send traffic logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter traffic-log client-info enabled {true| false}`	The `true` command will have the Zyxel Device send traffic logs along with the client information to SecuReporter for analysis and trend spotting.
`vrf main secureporter interface-statistics enabled {true| false}`	The `true` command will have the Zyxel Device send logs of interface statistics to SecuReporter for analysis and trend spotting.
`vrf main secureporter app-statistics enabled {true| false}`	The `true` command will have the Zyxel Device send app traffic logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter sandboxing enabled {true| false}`	The `true` command will have the Zyxel Device send sandbox traffic logs to SecuReporter for analysis and trend spotting.
`vrf main secureporter ike enabled {true| false}`	The `true` command will have the Zyxel Device send VPN logs to SecuReporter for analysis and trend spotting.
`cmd securpt-claim-device device-name <name> organization <organization-name> organization_id <organization-id> gdpr {none| partial| fully}`	Enter the name of the Zyxel Device. Add it to an existing organization by entering the organization name and ID. Enter the name of the Zyxel Device. Add it to a new organization by entering a name for the organization you want to create. `none`: Has your personal data, such as user names, MAC addresses, email addresses and host names to be identifiable in downloaded logs. `partial`: Has your personal data, such as user names, MAC addresses, email addresses and host names to be replaced with artificial identifiers in downloaded logs. `fully`: Has your personal data, such as user names, MAC addresses, email addresses and host names to be replaced with anonymized information in downloaded logs.
`show securpt-claim-status`	Displays: • If the Zyxel Device is claimed by an organization. • The names and IDs of all organizations.

41.1.2 SecuReporter Commands Example

The following example shows SecuReporter configurations. Set the upload file size to 5 MB. Set the upload interval to 100 seconds.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main secureporter enabled true
usgflex200hp running config# vrf main secureporter upload-filesize 5
usgflex200hp running config# vrf main secureporter upload-interval 100
usgflex200hp running config# vrf main secureporter anti-malware enabled true
usgflex200hp running config# vrf main secureporter threat-protection enabled true
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 42
Diagnostics and Maintenance Tools

42.1 Diagnostics Overview

The diagnostics feature provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

42.1.1 Diagnostic Commands

The following table lists the commands that you can use to have the Zyxel Device collect diagnostics information. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 192 Diagnostic Commands

COMMAND	DESCRIPTION
`diagnostics diaginfo ac categories <1...2047>`	Collects information on the AP controller (the Zyxel Device) according to the category you set. For example, set the category number to 2 to collect AAA related information. Set the category number to 128 to collect VPN related information. Uses this command with the assistance of the customer support.
`diagnostics diaginfo copy-to-usb {true | false}`	Has the Zyxel Device create a copy of the diagnostic file to a connected USB storage device.
`diagnostics diaginfo copy-conf {true | false}`	Includes the configuration file currently used by the Zyxel Device in the generated diagnostic file.
`cmd diagnostics diaginfo collect ac {start| stop}`	Starts collecting or stops collecting information on the AP controller (the Zyxel Device).
`show diagnostics mem status all`	Displays the current DRAM memory utilization percentage for each application used on the Zyxel Device and each application's running time in hours - minutes - seconds.
`show diagnostics cpu average`	Displays the current percentage usage of each CPU in the Zyxel Device as a percentage of total processing power and the current CPU utilization percentage for each application used on the Zyxel Device.
`show diagnostics cpu status average`	Displays the Zyxel Device average CPU utilization.
`show diagnostics cpu all`	Displays all the Zyxel Device CPU utilization.

Table 192 Diagnostic Commands (continued)

COMMAND	DESCRIPTION
`show diagnostics diaginfo collect status`	Displays whether the Zyxel Device is collecting diagnostics information (Standby) or the Zyxel Device has finished collecting diagnostics information (Busy on device).
`show dir diagnostics-file`	Displays the details of the latest diagnostics files on the Zyxel Device. • File name: This is the name of the diagnostic file. • Size: This is the size of the diagnostic file. • Modified time: This is the date and time that the diagnostic file was created.
`show dir diagnostics-file-standby`	Displays the details of the latest diagnostics files stored on the standby partition on the Zyxel Device. • File name: This is the name of the diagnostic file. • Size: This is the size of the diagnostic file. • Modified time: This is the date and time that the diagnostic file was created.
`cmd delete type diagnostics-file <file-name>`	Removes a diagnostics file from the Zyxel Device. The file name must end with .log.
`cmd nebula connection-test`	Starts the connection test from the Zyxel Device to the Nebula Control Center (NCC).
`show gui nebula connection-test status`	Returns the result of the connection test from the Zyxel Device to the Nebula Control Center (NCC).
`cmd nebula connection-test [force {restart | stop}]`	Forcibly restarts or stops diagnosing the connection from the Zyxel Device to the Nebula Control Center in the event that the connection test hangs.
`show gui nebula status`	Displays the connection status between the Zyxel Device and the Nebula Control Center (NCC). • Connected: The Zyxel Device has an Internet connection with the NCC. • Disconnected: The Zyxel Device does not have an Internet connection with the NCC. • Unknown: The Zyxel Device was unable to receive a timely response from the Nebula server when checking the Internet connection with the NCC. • No Site Assignment: The Zyxel Device is registered with the NCC, but is not assigned to a site. • Disabled: The Internet connection from the Zyxel Device to the NCC was disabled using the Command Line Interface (CLI).
`show gui nebula info`	Displays the organization and site the Zyxel Device belongs to in Nebula.

42.1.2 Diagnosis Commands Examples

The following example shows you how to check all the Zyxel Device CPU utilization.

```
usgflex200hp running config# show diagnostics cpu all
cpu-all-diagnostics
    ok
        cpu_core_list 0
            cpu-utilization "11.9 %"
            cpu-utilization-for-1-min "12.3 %"
            cpu-utilization-for-5-min "12.8 %"
            ..
        cpu_core_list 1
            cpu-utilization "5.9 %"
            cpu-utilization-for-1-min "8.7 %"
            cpu-utilization-for-5-min "7.5 %"
            ..
        cpu_core_list 2
            cpu-utilization "100.0 %"
            cpu-utilization-for-1-min "100.0 %"
            cpu-utilization-for-5-min "100.0 %"
            ..
        cpu_core_list 3
            cpu-utilization "100.0 %"
            cpu-utilization-for-1-min "100.0 %"
            cpu-utilization-for-5-min "100.0 %"
            ..
```

The following commands show how to start the connection test from the Zyxel Device to Nebula, the result, and how to forcibly stop the connection test (if the connection test hangs).

```
usgflex500h> edit running
usgflex500h running config# cmd nebula connection-test
nebula-connection-test
    status in-progress
    ..
usgflex500h running config# show gui nebula connection-test status
show-nebula-connection-test-status
    status success
    log "Testing internet connection to Google DNS server (8.8.8.8)
ping 8.8.8.8, timeout: 1 second
ping-result: 45.10 ms


Testing DNS name resolve for d2.nebula.zyxel.com
Resolved IP address: 52.16.x.y


Testing Nebula connection
TCP ping to d2.nebula.zyxel.com:4335, timeout: 1 second
TCP ping successful, time taken: 294.14 ms
"
    ..
usgflex500h running config# cmd nebula connection-test force
restart    stop
usgflex500h running config# cmd nebula connection-test force stop
nebula-connection-test
    status standby
    ..
usgflex500h running config#
```

42.1.3 Packet Capture Commands

Use the packet capture commands to capture network traffic going through the Zyxel Device's interfaces. Studying these packet captures may help you identify network problems.

Table 193 Packet Capture Commands

COMMAND	DESCRIPTION
`cmd diagnostics packet-capture enabled {true| false}`	Enable packet capture on the Zyxel Device.
`cmd diagnostics packet-capture config ftp {server` ***`ip-address`*** `| port` ***`port-number`*** `| username` ***`name`*** `| password` ***`password`*** `}`	Sets the FTP server for which to capture packets.
`cmd diagnostics packet-capture config ip-version {ip| ip6| any}`	Sets whether to capture IPv4 or IPv6 traffic. `any` means to capture packets for all types of traffic.
`cmd diagnostics packet-capture config proto-type {icmp| icmp6| igmp| igrp| plm| ah| esp| vrrp| udp| tcp| any}`	Sets the protocol of traffic for which to capture packets. `any` means to capture packets for all types of traffic.
`cmd diagnostics packet-capture config host-ip {`***`ip-address`***`| any}`	Sets a host IP address for which to capture packets. `any` means to capture packets for all hosts.

Table 193 Packet Capture Commands (continued)

COMMAND	DESCRIPTION
cmd diagnostics packet-capture config host-object <*profile-name*>	Sets a host IP address object for which to capture packets.
cmd diagnostics packet-capture config host-port <*0...65535*>	If you set the IP type to any, tcp, or udp using the proto-type command, you can specify the port number of traffic to capture.
cmd diagnostics packet-capture config files-size <*1...1000000000*>	Specifies a maximum size limit in megabytes for the total combined size of all the capture files on the ZyWALL, including any existing capture files and any new capture files you generate. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the duration command above) expires.
cmd diagnostics packet-capture config split-size <*1...2048*>	Specifies a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
cmd diagnostics packet-capture config ring-buffer {true| false}	Enable or disable the ring buffer used as a temporary storage.
cmd diagnostics packet-capture config storage {internal| usbstorage| ftpserver}	Has the Zyxel Device only store packet capture entries on the Zyxel Device (internal) or on a USB storage or on a FTP server connected to the Zyxel Device.
cmd diagnostics packet-capture config duration <*0...300*>	Sets a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command. 0 means there is no time limit.
cmd diagnostics packet-capture config file-suffix <*profile-name*>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is “interface name-file suffix.cap”, for example “vlan2-packet-capture.cap”.
cmd diagnostics packet-capture config snaplen <*0...1514*>	Specifies the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
cmd diagnostics packet-capture config iface {add| del} <*interface-name*>	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
show diagnostics packet-capture config	Displays the packet capture settings.
show diagnostics packet-capture status	Displays whether the packet capture is ongoing.

42.1.4 Ping Commands

Use the commands listed below to ping a specified IP address.

Table 194 Ping Commands

COMMAND	DESCRIPTION
`show diagnostics ping`	Displays the ping command result.
`cmd diagnostics ping {ip ipv4-or-domainname | ip ipv6-or-domainname} <ip-or-domain name>`	Sends an ICMP ECHO_REQUEST to test the reachability of the specified host and measures the round-trip time for a message sent from the originating host to the destination computer.
`cmd diagnostics ping interface <interface>`	Pings `the interface that you entered.`
`cmd diagnostics ping {ip ipv4-or-domainname | ip ipv6-or-domainname} <ip-or-domain name> Extension-Option 'c <count> - s <size> -w <wait-time>'`	Sets the following extension options when running ping to the specified host. Enclose the Extension-Options in single quotes. -c *count:* Number of ping requests to send. -s *size:* N umber of bytes of data to send in each ping. -w *wait-time:* Maximum number of seconds for the entire ping operation to run.
`cmd diagnostics ping Extension-Option <extension-option>`	Enter the extension options as listed above as a single string to apply to all ping commands. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters. Enclose the Extension-Option string in single quotes. For example, '-c <count> -s <size> -w <wait-time>'.
`cmd diagnostics ping stop {true| false}`	Stops or continues to run ping.
`show diagnostics ping status`	Displays if ping is running on the Zyxel Device.

The following example shows you how to use the extension options when running ping to 8.8.8.8. It will send 4 ping requests, each with a maximum size of 100 bytes and it will wait 10 seconds for a ping reply.

```
usgflex500h running config# cmd diagnostics ping ip ipv4-or-domainname 8.8.8.8
Extension-Option '-c 4 -s 100 -w 10'
ping-diagnostics
    ok
        result ok
        ..
    ..
usgflex500h running config#
```

42.1.5 Trace Route Commands

Use the trace route commands to identify where packets are dropped for troubleshooting.

Table 195 Trace Route Commands

COMMAND	DESCRIPTION
cmd diagnostics traceroute {ip ipv4-or-domainname | ip ipv6-or-domainname} <*ip-or-domain name*>	Displays the route packets take to the IP address or domain name that you specify. Use Ctrl+C to return to the prompt.
cmd diagnostics traceroute interface <*interface*>	Specifies a network interface from which to send outgoing probe packets.
cmd diagnostics traceroute {ip ipv4-or-domainname | ip ipv6-or-domainname} <*ip-or-domain name*> Extension-Option '-m <max_ttl> - *s* <*src_addr*> <*packet length*> -F'	Sets the following extension options when running traceroute to the specified host. Enclose the Extension-Options in single quotes. -m: *max_ttl* is the maximum number of hops allowed. The default is 30. -s: *src_addr* is the source IP address for outgoing traceroute packets. <*packet length*> is the maximum packet length to send. -F: Disables the fragment flag in packet.
cmd diagnostics traceroute Extension-Option <*extension-option*>	Enter the extension options as listed above as a single string to apply to all traceroute commands. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters. Enclose the Extension-Option string in single quotes. For example, '-m <*max_ttl*> -s <*src_addr*>'.
cmd diagnostics traceroute stop {true| false}	Stops or continues to run traceroute to the specified host name or IP address
show diagnostics traceroute	Displays the traceroute command result.

The following example shows you how to use the extension options when running traceroute to 8.8.8.8. The maximum number of hops is 10 and the source address to send traceroute from is 192.168.168.1. In the second command, the maximum packet length is 1,500 bytes with the fragment flag disabled.

```
usgflex500h running config#cmd diagnostics traceroute ip ipv4-or-domainname
8.8.8.8 Extension-Option '-m 10 -s 192.168.168.1'

cmd diagnostics traceroute ip ipv4-or-domainname 8.8.8.8 Extension-Option '1500 -
F'
usgflex500h running config#
```

42.1.6 NSLOOKUP Commands

Use the NSLOOKUP commands to perform name server lookup for querying the Domain Name System (DNS) to get the domain name or IP address mapping.

Table 196 NSLOOKUP Commands

COMMAND	DESCRIPTION
`cmd diagnostics nslookup Query-Server <ip-address>`	Enter the IP address of a server to which the Zyxel Device sends queries for NSLOOKUP.
`cmd diagnostics nslookup Extension-Option <extended-option>`	Enter the extended option if you want to use an extended NSLOOKUP command. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
`cmd diagnostics nslookup domain-name-or-ip {domain-name domain-name| ipv4 ipv4| ipv6 ipv6}`	Performs name server lookup for querying a DNS server to get the domain name or IPv4/IPv6 address mapping.

42.1.7 Route Traces Commands

Use the route trace commands to configure traceroute to identify where packets are dropped for troubleshooting.

Table 197 Route Traces Commands

COMMAND	DESCRIPTION
`cmd debug zyinetpkt set host [ip {any|ipv4}] [port {any|<1..65535>}]`	Sets the IP address and port number of a specific source or destination host whose traffic you want to trace.
`cmd debug zyinetpkt set source[ip {any|ipv4}] [port {any|<1..65535>}]`	Sets the source IP address and port number of traffic that you want to trace.
`cmd debug zyinetpkt set destination [ip {any|ipv4}] [port {any|<1..65535>}]`	Sets the destination IP address and port number of traffic that you want to trace.
`cmd debug zyinetpkt set trace {both | slow-path | fast-path}`	Sets the path to use for traces. Fast-path traces bypass the kernel, so speeds up traffic such as NAT, IPSec VPN, and Security policies through the Zyxel Device.
`cmd debug zyinetpkt set duration <1..120>`	Sets the time interval in seconds for renewing a route trace.
`cmd debug zyinetpkt set protocol {any | <0..255>}`	Sets the protocol of traffic that you want to trace. `any` means any protocol.
`cmd debug zyinetpkt set enable {true | false}`	Captures packets that match configured conditions until the duration is reached.
`cmd debug zyinetpkt set buffer-size <1000..100000>`	Sets the trace buffer size. The trace buffers contain the trace data. You determine the size of your trace buffers based on the number of trace entries you want to create, and the size of the trace entries.
`cmd debug zyinetpkt set log-level {simple | complex}`	Sets the level of log details for route trace commands.

42.2 AP Diagnostics Overview

The AP diagnostics feature provides an easy way to generate a file containing diagnostic information from the Zyxel Device's managed APs. You may need to generate this file and send it to customer support during troubleshooting.

42.2.1 AP Diagnostics Commands

The following table lists the commands that you can use to have the Zyxel Device collect configuration and diagnostic information of managed APs. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 198 AP Diagnostics Commands

COMMAND	DESCRIPTION
`cmd diagnostics ap-diaginfo config ap {<ap-mac-address> | empty}`	Specifies the managed AP whose diagnostic information you want to collect. You can specify up to five APs for collecting, but only one AP per command. Use `empty` to remove all specified APs from the current configuration. Note: Diagnostic data from each AP is stored in an individual AP diagnostic file.
`cmd diagnostics ap-diaginfo config storage {usb | onboard}`	Specifies where to store diagnostic files. • `usb`: stores diagnostic files on the USB storage device connected to the Zyxel Device if the Zyxel Device allows this. • `onboard`: stores diagnostic files on the Zyxel Device.
`cmd diagnostics ap-diaginfo collect {start | stop}`	Starts or stops the collection.
`show diagnostics ap-diaginfo status`	Displays the current status of collection. • `Status` displays `Standby` when no collection is in progress and `Collecting` during collection. • `Progress` displays the number of APs specified for collection and the number of APs that have completed the collection. For example, `2/3` means that three APs are being collected and two of them have finished.

42.2.2 AP Diagnostics Commands Examples

The following example shows you how to generate AP configuration and diagnostic files.

```
MyUSGFLEX500H running config# cmd diagnostics ap-diaginfo
config ap 02:AA:BB:CC:DD:EE
config-ap-setting
    success
        result ok
        ..
MyUSGFLEX500H running config# cmd diagnostics ap-diaginfo
config ap 02:11:22:33:44:55
config-ap-setting
    success
        result ok
        ..
    ..
MyUSGFLEX500H running config# cmd diagnostics ap-diaginfo
collect start
collect-ap-start
    success
        result ok
        ..
    ..
MyUSGFLEX500H running config# show diagnostics ap-diaginfo
status
show-ap-status
    success
        status Collecting
        progress 0/2
        storage Onboard
        ap-list
            mac-address 02:AA:BB:CC:DD:EE
            ..
        ap-list
            mac-address 02:11:22:33:44:55
            ..
        ..
    ..
MyUSGFLEX500H running config# show diagnostics ap-diaginfo
status
show-ap-status
    success
        status Standby
        progress 2/2
        storage Onboard
        ap-list
            mac-address 02:AA:BB:CC:DD:EE
            ..
        ap-list
            mac-address 02:11:22:33:44:55
            ..
        ..
    ..
```

42.2.3 AP Packet Capture Commands

The following table lists the commands that you can use to capture specific traffic of the managed APs' WiFi network. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 199 AP Packet Capture Commands

COMMAND	DESCRIPTION
`cmd diagnostics ap-packet-capture config ap-group <group-name>`	Specifies the AP group the managed APs whose packets you want to capture belongs to.
`cmd diagnostics ap-packet-capture config ap {<ap-mac-address> | empty}`	Specifies the managed AP whose packets you want to capture. You can specify multiple APs for packet capture, but only one AP per command. Use `empty` to remove all specified APs from the current capture configuration before starting a new capture.
`cmd diagnostics ap-packet-capture config interface {<ap-interface> | empty}`	Specifies the interfaces for which to capture packets passing through the specified managed AP(s). You can specify multiple interfaces for packet capture, but only one interface per command. See the `AP-interface` commands below for packet capture: • `SSID Name(xGHz)`: WiFi packets on a specific WiFi network (SSID) or a specific frequency band. x indicates the frequency band. For example, `SSID2(5GHz)`. • `WIRELESS(xGHz)`: WiFi packets transmitted and received by client devices on a specific frequency band. x indicates the frequency band. For example, `WIRELESS(2.4GHz)`. • `WDS-x-9`: WiFi packets transmit through the downlink AP using a specific radio profile. x indicates the radio profile number 1, 2, or 3. For example, `WDS-2-9`. • `WDS-x-10`: WiFi packets transmit through the uplink AP using a specific radio profile. x indicates the radio profile number 1, 2, or 3. For example, `WDS-1-10`. • `UPLINK`: Packets transmitted and received through the uplink port. • `LANx`: Packets passing through a specific LAN port of the managed AP. x indicates the LAN port number. For example, `LAN2`. • `Br0`: Packets transmitted and received through the AP's virtual bridge, connecting uplink and downlink interfaces. Use `empty` to remove all specified interfaces from the current capture configuration before starting a new capture.
`cmd diagnostics ap-packet-capture config ip-version {ip | ip6 | any}`	Specifies the packets with a specific IP version that you want to capture. `any` means to capture packets for all IP versions of traffic.
`cmd diagnostics ap-packet-capture config proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any}`	Specifies the protocol of traffic for which to capture packets. `any` means to capture packets for all types of traffic.
`cmd diagnostics ap-packet-capture config host-ip {<ip-address> | any}`	Specifies a host IP address for which to capture packets. `any` means to capture packets for all hosts.
`cmd diagnostics ap-packet-capture config host-port <0...65535>`	Specifies the port number of traffic to capture if you specify the protocol type to `any`, `tcp`, or `udp` using the `proto-type` command above.

Table 199 AP Packet Capture Commands (continued)

COMMAND	DESCRIPTION
`cmd diagnostics ap-packet-capture config file-suffix <string>`	Specifies text to add to the end of the capture file name (before the dot and filename extension) to help you identify the files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is “interface name-file suffix.cap”, for example “wlan-1-2-packet-capture.cap”.
`cmd diagnostics ap-packet-capture config snaplen <0...1514>`	Specifies the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
`cmd diagnostics ap-packet-capture config duration <0...300>`	Sets a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command below. 0 means there is no time limit.
`cmd diagnostics ap-packet-capture config files-size <1...10>`	Specifies a maximum size limit in megabytes (MB) for the total combined size of all the capture files from each AP. The valid range is 1 to 10 MB. The Zyxel Device stops capturing when the size limit is reached.
`cmd diagnostics ap-packet-capture config storage {internal | usbstorage}`	Specifies where to store packet capture files. • `internal`: stores packet capture files on the Zyxel Device. • `usbstorage`: stores packet capture files on the USB storage device connected to the Zyxel Device if the Zyxel Device allows this.
`cmd diagnostics ap-packet-capture enabled {true | false}`	Starts or stops packet capture based on the current capture configuration.
`show state diagnostics ap-packet-capture ap-group`	Displays details of all AP groups.
`show state diagnostics ap-packet-capture config`	Displays the current capture configuration for review before starting a capture.
`show state diagnostics ap-packet-capture status`	Displays the capture status. `Idle` displays when no packet capture is in progress. `Preparing` displays when the AP retrieves capture requirements, and `Capturing` displays when packet capture is active.

42.2.4 AP Packet Capture Commands Examples

The following example shows you how to configure an AP packet capture configuration.

```
MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config ap-group -APGroup_test2
ap-packet-capture-diagnostics-configuration
    success
        result ok
        ..
    ..

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config ap 02:AA:BB:CC:DD:EE
ap-packet-capture-diagnostics-configuration
    success
        result ok
        ..
    ..

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config interface br0
ap-packet-capture-diagnostics-configuration
    success
        result ok

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config interface wds-1-9
ap-packet-capture-diagnostics-configuration
    success
        result ok

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config interface SSID2(5GHz)
ap-packet-capture-diagnostics-configuration
    success
        result ok

MyUSGFLEX500H running config# show state diagnostics ap-
packet-capture config
config
    ap-group -APGroup_test2
    ap 02:AA:BB:CC:DD:EE
    interface br0
    interface wds-1-9
    interface SSID2(5GHz)
    ip-version any
    proto-type any
    host-ip any
    host-port 0
    files-size 10
    storage internal
    duration 0
    file-suffix -packet-capture
    snaplen 1500
    debug false
    ..
```

The following example shows how to start and stop AP packet capture and check the capture status.

```
MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture enabled true
ap-packet-capture-diagnostics-set-active
    success
        result ok
        ..
    ..

MyUSGFLEX500H running config# show state diagnostics ap-
packet-capture status
status
    capture-status Preparing
    ap
        index 1
        ap-mac 02:AA:BB:CC:DD:EE
        ap-status config
        ap-msg ""
        ..
    ..

MyUSGFLEX500H running config# show state diagnostics ap-
packet-capture status
status
    capture-status Capturing
    ap
        index 1
        ap-mac 02:AA:BB:CC:DD:EE
        ap-status on
        ap-msg ""
        ..

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture enabled false
ap-packet-capture-diagnostics-set-active
    success
        result ok
        ..
    ..
MyUSGFLEX500H running config# show state diagnostics ap-
packet-capture status
status
    capture-status Idle
    ap
        index 1
        ap-mac 02:AA:BB:CC:DD:EE
        ap-status off
        ap-msg ""
        ..
```

To start a new capture, you must remove the currently configured APs and interfaces from the capture configuration and set up a new configuration. The following example shows how to clear the current AP packet capture configuration before starting a new capture.

```
MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config ap empty
ap-packet-capture-diagnostics-configuration
    success
        result ok
        ..
    ..

MyUSGFLEX500H running config# cmd diagnostics ap-packet-
capture config interface empty
ap-packet-capture-diagnostics-configuration
    success
        result ok
        ..
```

42.2.5 Remote Capture Commands

Use the remote capture feature to capture wireless traffic passing through a managed AP and output the captured packets to a packet analyzer (also known as network or protocol analyzer), such as Wireshark. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 200 Packet Capture Commands

COMMAND	DESCRIPTION
`show remote-capture query ap-mac <ap-mac-address>`	Queries the managed AP that is connected to the device used for capturing wireless packets. This AP will act as the monitor AP.
`show remote-capture status`	Displays the queried monitor AP and the status of the remote capture query.

CHAPTER 43
Shutdown/Reboot

Use these commands to turn off or restart the Zyxel Device. Use `copy running startup` to save your current configurations as the startup configurations before you reboot or shutdown the Zyxel Device. The Zyxel Device uses the startup configurations the next time you turn on the Zyxel Device.

Note: You cannot shut down or reboot the Zyxel Device if you did not save your current configurations as the startup configurations. Use the `force` command to shut down or reboot the Zyxel Device without saving the current configurations as the startup configurations. The configurations you made using the CLI will be lost.

Table 201 Shutdown/Reboot Commands

COMMAND	DESCRIPTION
`cmd reboot {force| delay| cancel}`	`force`: Reboots the Zyxel Device immediately without turning the power off. Your current configurations are not saved. Make sure to back up your current configurations before rebooting the Zyxel Device. `delay`: Sets the number of seconds the Zyxel Device waits before rebooting. The default value is 3. `cancel`: Stops the Zyxel Device from rebooting.
`cmd poweroff {force| delay| cancel}`	Wait for the **PWR/SYS** LED to turn off before you remove the Zyxel Device power cable. `force`: Turns off the Zyxel Device immediately. Your current configurations are not saved. Make sure to back up your current configurations before turning off the Zyxel Device. `delay`: Sets the number of seconds the Zyxel Device waits before turning off. The default value is 3. `cancel`: Stops the Zyxel Device from turning off.

List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.