

Handbook

USG FLEX H Series

USG FLEX 50H / USG FLEX 50HP

USG FLEX 100H / USG 100HP / USG FLEX 200H /

USG FLEX 200HP / USG FLEX 500H / USG FLEX 700H

Firmware Version: uOS 1.35

Aug. 2025

Table of Content

Chapter 1- VPN	5
How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address	5
How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address	17
How to Configure IPSec Site to Site VPN while one Site is behind a NAT router	23
How to Configure Remote Access VPN with Zyxel VPN Client	35
How to Configure Site-to-site IPSec VPN between ZLD and uOS device	54
How to Configure Route-Based VPN	65
How to Use Tailscale.....	77
How to use Ext-group user to connect Remote Access VPN.....	88
Chapter 2- Security Service	91
How to Block HTTPS Websites Using Content Filtering and SSL Inspection	91
How to Configure Content Filter with HTTPs Domain Filter	100
How to Block Facebook Using a Content Filter Block List	105
How to block YouTube access by Schedule	109
How to Control Access to Google Drive	118
How to Block the Spotify Music Streaming Service	126
How does Anti-Malware Work	129
How to Detect and Prevent TCP Port Scanning with DoS Prevention	132
How to block the client from accessing to certain country using Geo IP?	136
How to Use Sandbox to Detect Unknown Malware?	141
How to Configure Reputation Filter- IP Reputation.....	144
How to Configure Reputation Filter- URL Threat Filter.....	149
How to Configure Reputation Filter- DNS Threat Filter	153

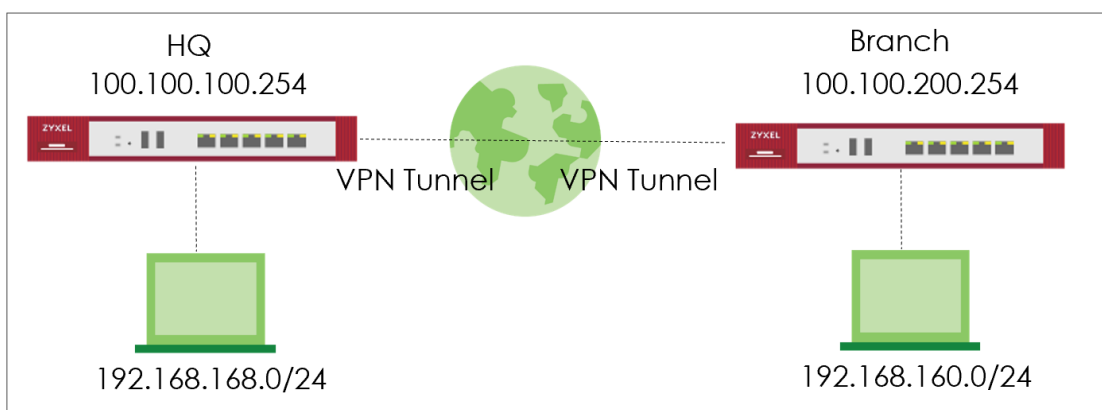
How to Configure DNS Content Filter	157
External Block List for Reputation Filter	162
How to set up DNS SafeSearch?	167
Chapter 3- Authentication	175
How to Use Two Factor with Google Authenticator for Admin Access	175
How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN	182
How to set up AD authentication with Microsoft AD	192
How to Set Up Captive Portal?	197
Chapter 4- Maintenance	205
How to Manage Configuration Files	205
How to Manage Firmware	209
How to set up configuration file backup rotation	211
Chapter 5- Others	215
How to Setup and Configure Daily Report	215
How to Setup and Send Logs to a Syslog Server	220
How to Setup and Send logs to the USB storage	223
How to Perform and Use the Packet Capture Feature	225
How to Allow Public Access to a Server Behind USG FLEX H.....	229
How to Configure DHCP Option 60 – Vendor Class Identifier	233
How to Configure Session Control	235
How to Configure Bandwidth Management for FTP Traffic	238
How to Configure WAN trunk for Spillover and Least Load First	243
How Does SIP ALG Function Work on USG FLEX H?	249
How to Deploy Device HA	253
How to check Packet Flow Explorer	266
How to set up a Link Aggregation Group (LAG) interface	272

How to Set Up AP Control Service for Zyxel APs	278
How to set up SMTP with Microsoft OAuth2.0?.....	283
Chapter 6- Nebula	296
How to Set Up Nebula site-to-site VPN on the USG FLEX H?.....	296
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)?.....	300
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)?	304
How to Onboard Firewall to Nebula within Initial Setup Wizard	308

Chapter 1- VPN

How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address

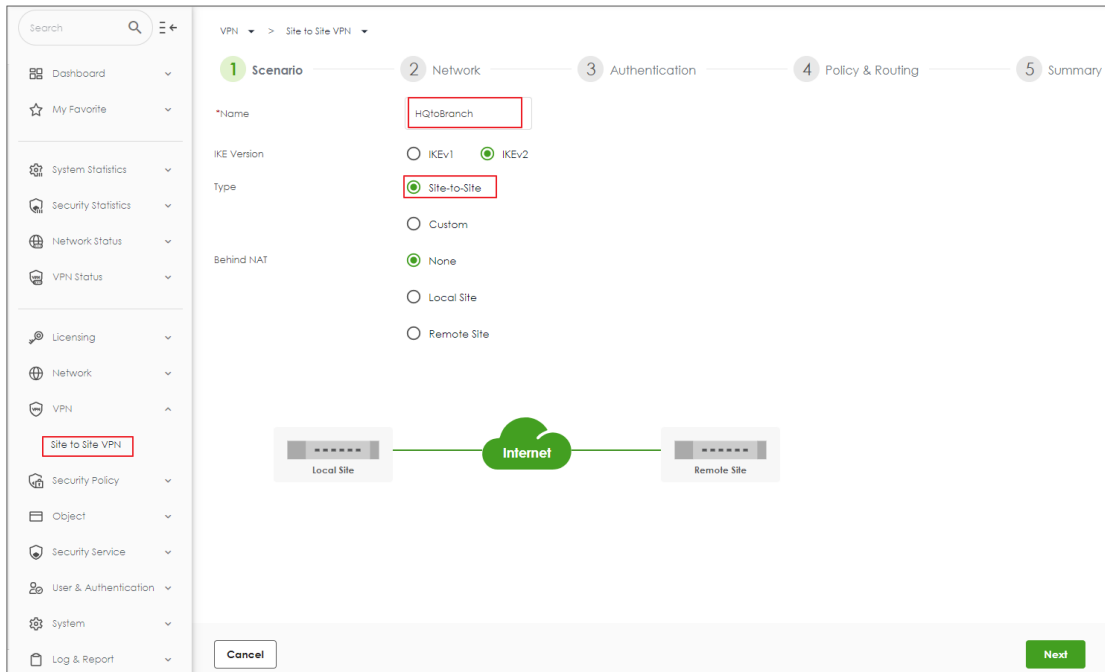
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



The screenshot shows the ZyXel VPN configuration interface. On the left is a sidebar menu with options: Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted with a red box), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the 'VPN > Site to Site VPN' configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. In the 'Scenario' step, the following fields are visible:

- *Name: HQtoBranch (highlighted with a red box)
- IKE Version: ☐ IKEv1, ☒ IKEv2
- Type: ☒ Site-to-Site (highlighted with a red box), ☐ Custom
- Behind NAT: ☒ None, ☐ Local Site, ☐ Remote Site

 Below the form is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is then connected to a 'Remote Site'. At the bottom of the interface are 'Cancel' and 'Next' buttons.

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN > Site to Site VPN >

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address

Domain Name / IP

100.100.100.254

Peer Gateway Address

Domain Name / IP

100.100.200.254

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

VPN > Site to Site VPN

✓ Scenario

✓ Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.

VPN > Site to Site VPN >

Scenario
Network
Authentication
4 Policy & Routing
5 Summary

Type
☐ Route-Based
☒ Policy-Based

Local Subnet
192.168.168.0/24

Remote Subnet
192.168.160.0/24

192.168.168.0/24

Local Site
100.100.100.254

Internet

Remote Site
100.100.200.254

192.168.160.0/24

Cancel
Back
Finish

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

VPN > Site to Site VPN

✓ Scenario
✓ Network
✓ Authentication
✓ Policy & Routing
5 Summary

Configuration

Name	HQtoBranch
IKE Version	2
Scenario	wizard
Type	Policy

Edit

Network

Local Site	100.100.100.254
Remote Site	100.100.200.254

Authentication

Authentication	pre-shared-key	*****
----------------	----------------	-------

Policy & Routing

Local Subnet	192.168.168.0/24
Remote Subnet	192.168.160.0/24

Close

Set up IPsec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.

The screenshot shows the ZyXel VPN configuration interface. On the left is a sidebar menu with options: Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted with a red box), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the 'VPN > Site to Site VPN' configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. It contains the following fields and options:

- *Name: BranchtoHQ (highlighted with a red box)
- IKE Version: ☐ IKEv1, ☒ IKEv2
- Type: ☒ Site-to-Site (highlighted with a red box), ☐ Custom
- Behind NAT: ☒ None, ☐ Local Site, ☐ Remote Site

Below the configuration fields is a diagram showing a 'Local Site' (represented by a server icon) connected to an 'Internet' cloud, which is then connected to a 'Remote Site' (represented by a server icon). At the bottom of the configuration area are 'Cancel' and 'Next' buttons. The 'Next' button is highlighted in green.

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN > Site to Site VPN >

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address

Domain Name / IP

100.100.200.254

Peer Gateway Address

Domain Name / IP

100.100.100.254

Local Site

100.100.200.254

Internet

Remote Site

100.100.100.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**.

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.

VPN > Site to Site VPN >

✓ Scenario
✓ Network
✓ Authentication
4 Policy & Routing
5 Summary

Type

☐ Route-Based
☒ Policy-Based

Local Subnet

192.168.160.0/24

Remote Subnet

192.168.168.0/24

192.168.160.0/24

Local Site

100.100.200.254

Internet

Remote Site

100.100.100.254

192.168.168.0/24

Cancel

Back

Finish

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

VPN > Site to Site VPN

✓ Scenario
✓ Network
✓ Authentication
✓ Policy & Routing
5 Summary

Configuration

Name	BranchtoHQ	
IKE Version	2	
Scenario	wizard	
Type	Policy	

Edit

Network

Local Site	100.100.200.254	
Remote Site	100.100.100.254	

Authentication

Authentication	pre-shared-key	*****
----------------	----------------	-------

Policy & Routing

Local Subnet	192.168.160.0/24	
Remote Subnet	192.168.168.0/24	

Close

Test IPsec VPN Tunnel

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

Network Connection Details

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect...
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 2023
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

Administrator: Command Prompt

```

Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

VPN Status > IPsec VPN

Verify the IPsec VPN status and do the Connectivity Check

VPN Status > IPsec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh **Connectivity Check**

#	Name	Policy Route	Remote Gateway	My Address
1	HQtoBranch	192.168.168.0/24 <-> 192.168.160.0/24	100.100.200.254	100.100.100.254

Connectivity Check

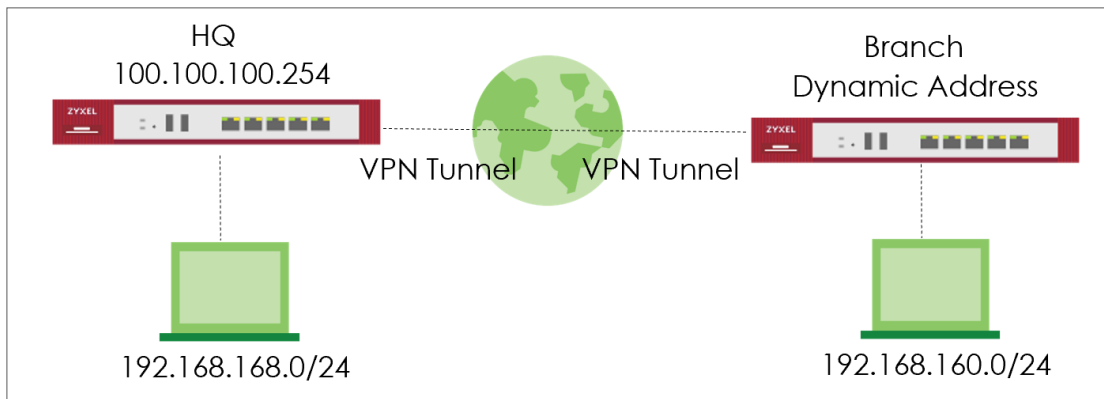
IP Address: 192.168.160.1 Test

Result
ICMP Connectivity Check PASS on sec_policy1_HQtoBranch

OK

How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address

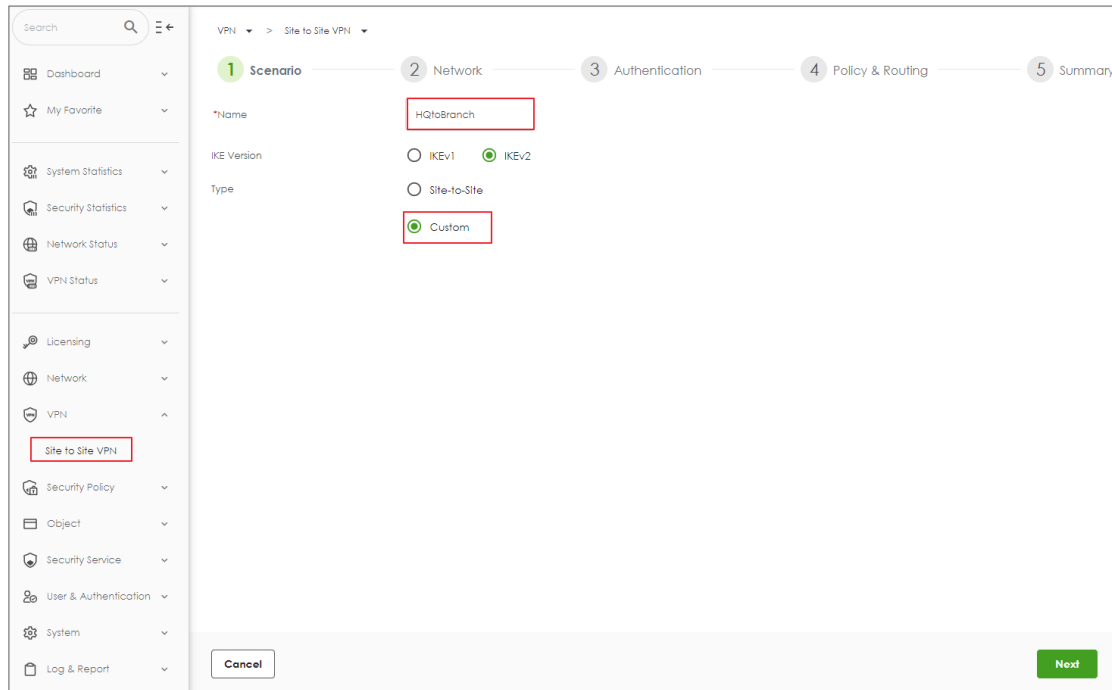
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

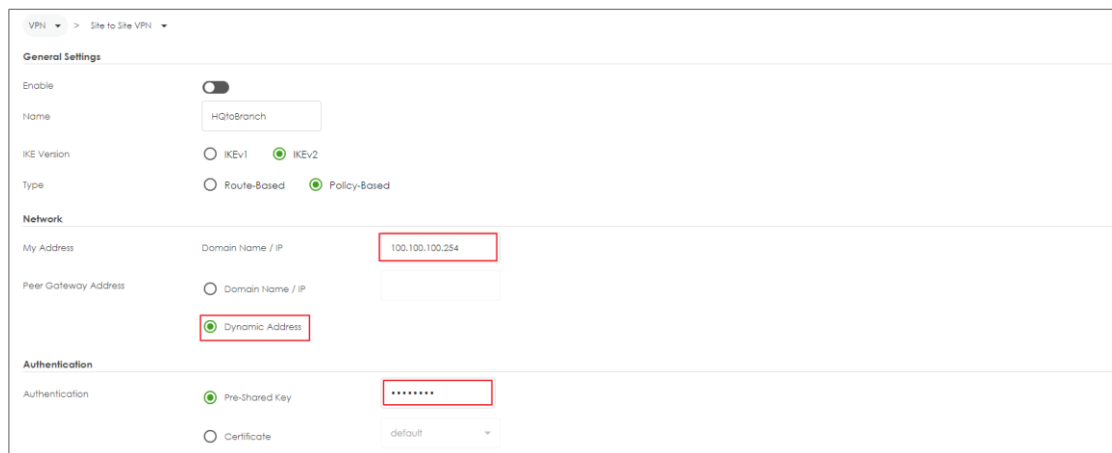
VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Custom. Click **Next**.



VPN > Site to Site VPN

Type My Address and select Peer Gateway Address as Dynamic Address. Type a secure Pre-shared key.



Scroll down to find the Phase2 setting. Type Local and Remote Subnet and select Responder Only. Then click save change.

Phase 2 Settings

Initiation

☐ Auto
☐ Nalled-up
☒ Responder Only

Policy

+ Add

Edit

Remove

Local

Remote

Protocol

Active Protocol

Encapsulation

192.168.168.0/24	192.168.160.0/24	Any	ESP	Tunnel	✓	✕
------------------	------------------	-----	-----	--------	---	---

Rows per page: 50 1 of 1 < 1 >

SA Life Time

28800

(180 - 3000000 Seconds)

Proposal

+ Add

Edit

Remove

Encryption

Authentication

aes128-cbc	hmac-sha1
------------	-----------

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups

DH2

✕

▼

Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Custom. Click **Next**.

VPN > Site to Site VPN

1 Scenario 2 Network 3 Authentication 4 Policy & Routing 5 Summary

*Name: BranchtoHQ

IKE Version: ☐ IKEv1 ☒ IKEv2

Type: ☐ Site-to-Site ☒ Custom

Cancel Next

VPN > Site to Site VPN

Type My Address as 0.0.0.0 and type Peer Gateway Address. Type a secure Pre-shared key.

VPN > Site to Site VPN

General Settings

Enable: ☒

Name: BranchtoHQ

IKE Version: ☐ IKEv1 ☒ IKEv2

Type: ☐ Route-Based ☒ Policy-Based

Network

My Address: Domain Name / IP: 0.0.0.0

Peer Gateway Address: ☒ Domain Name / IP: 100.100.100.254 ☐ Dynamic Address

Authentication

Authentication: ☒ Pre-Shared Key: ☐ Certificate: default

Scroll down to find the Phase2 setting, type Local and Remote Subnet. Then click save change.

Phase 2 Settings

Initiation

☒ Auto
 ☐ Nailed-up
 ☐ Responder Only

Policy

+ Add
 Edit
 Remove

Local	Remote	Protocol	Active Protocol	Encapsulation		
192.168.160.0/24	192.168.168.0/24	Any	ESP	Tunnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rows per page: 50 1 of 1 < 1 >

SA Life Time

(180 - 3000000 Seconds)

Proposal

+ Add
 Edit
 Remove

Encryption	Authentication
<input type="checkbox"/> aes128-cbc	hmac-sha1

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups

Test IPSec VPN Tunnel

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

Network Connection Details

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect...
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 2023
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

Administrator: Command Prompt

```

Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check

VPN Status > IPSec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh **Connectivity Check**

#	Name	Policy Route	Remote Gateway	My Address
1	HQtoBranch	192.168.168.0/24 <> 192.168.160.0/24	100.100.200.254	100.100.100.254

Connectivity Check

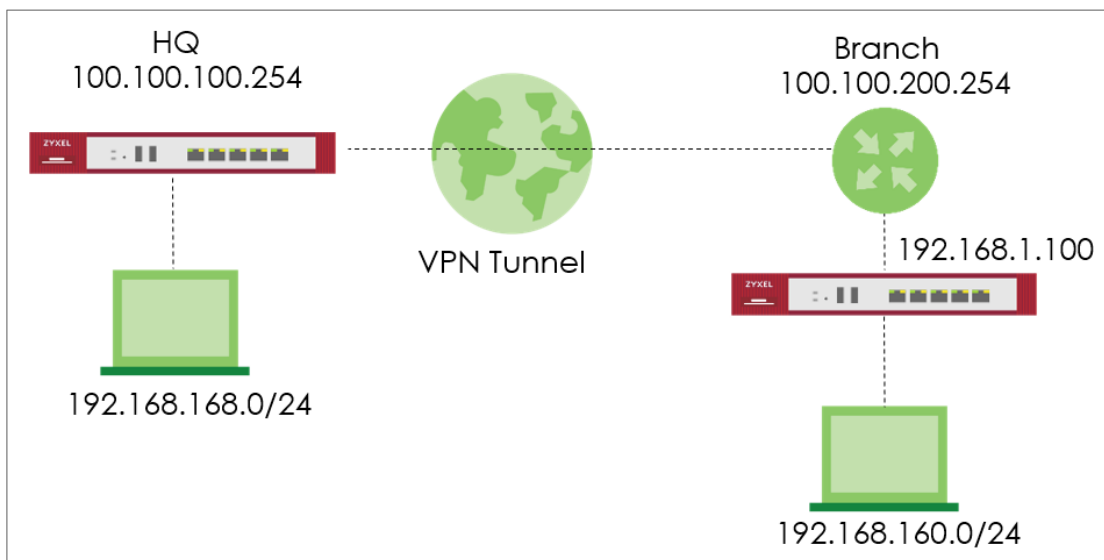
IP Address: 192.168.160.1 Test


Result
ICMP Connectivity Check PASS on sec_policy1_HQtoBranch

OK

How to Configure IPSec Site to Site VPN while one Site is behind a NAT router

This example shows how to use the VPN Setup Wizard to create a IPSec Site to Site VPN tunnel between USG FLEX H devices. The example instructs how to configure the VPN tunnel between each site while one Site is behind a NAT router. When the IPSec Site to Site VPN tunnel is configured, each site can be accessed securely.



 Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.

Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Remote Site. Click **Next**.

Search

VPN > Site to Site VPN

1 Scenario 2 Network 3 Authentication 4 Policy & Routing 5 Summary

Name: HQtoBranch

IKE Version: ☐ IKEv1 ☒ IKEv2

Config Type: ☒ Wizard ☐ Custom

Behind NAT: ☐ None ☐ Local Site ☒ Remote Site

Local Site Internet Router Remote Site

Cancel Next

VPN > Site to Site VPN > Scenario > Network

Configure My Address. Click **Next**.

VPN

>

Site to Site VPN

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address

Domain Name / IP

100.100.100.254

Peer Gateway Address

Dynamic Address

Local Site

100.100.100.254

Internet

Router

Remote Site

Dynamic Address

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

VPN > Site to Site VPN

Scenario

Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate Beta

.....

default

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.

VPN
>
Site to Site VPN

Scenario

Network

Authentication

4
Policy & Routing

5
Summary

Type

Route-Based

Policy-Based

Local Subnet

192.168.168.0/24

Remote Subnet

192.168.160.0/24

192.168.168.0/24

Local Site
100.100.100.254

Internet

Router

Remote Site
Dynamic Address

192.168.160.0/24

Cancel

Back

Finish

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing >

Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

←
VPN > Site to Site VPN >

✓ Scenario
 ✓ Network
 ✓ Authentication
 ✓ Policy & Routing
 5 Summary

Configuration

Name	HQtoBranch
IKE Version	2
Type	Policy-based

Proposal

▼

Edit

Network

Local Site	100.100.100.254
Remote Site	

Authentication

Authentication	pre-shared-key	*****
----------------	----------------	-------

Policy & Routing

Local Subnet	192.168.168.0/24
--------------	------------------

Close

Set up IPsec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Local Site. Click **Next**.

Search

VPN > Site to Site VPN

1 Scenario 2 Network 3 Authentication 4 Policy & Routing 5 Summary

Name BranchtoHQ

IKE Version ☐ IKEv1 ☒ IKEv2

Config Type ☒ Wizard ☐ Custom

Behind NAT ☐ None ☒ Local Site ☐ Remote Site

Local Site Router Internet Remote Site

Cancel Next

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN

>

Site to Site VPN

>

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address	Domain Name / IP	192.168.1.100
Peer Gateway Address	Domain Name / IP	100.100.100.254

Local Site

192.168.1.100

Router

Internet

Remote Site

100.100.100.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.

The screenshot shows the 'Policy & Routing' configuration page for a Site-to-Site VPN. The breadcrumb trail at the top is 'VPN > Site to Site VPN'. Below the breadcrumb is a progress bar with five steps: 'Scenario' (checked), 'Network' (checked), 'Authentication' (checked), 'Policy & Routing' (active, highlighted with a green circle and the number 4), and 'Summary' (disabled, highlighted with a grey circle and the number 5).

Under the 'Type' section, there are two radio buttons: 'Route-Based' (unselected) and 'Policy-Based' (selected, indicated by a green dot).

The 'Local Subnet' field contains the value '192.168.160.0/24' and is highlighted with a red rectangular border. The 'Remote Subnet' field contains the value '192.168.168.0/24' and is also highlighted with a red rectangular border.

Below the input fields is a network diagram illustrating the setup. On the left, a computer icon is connected to a 'Local Site' box (containing a server icon) with the IP address '192.168.160.0/24' below it. The 'Local Site' is connected to a 'Router' icon. The 'Router' is connected to a green cloud labeled 'Internet'. The 'Internet' cloud is connected to a 'Remote Site' box (containing a server icon) with the IP address '100.100.100.254' below it. The 'Remote Site' is connected to another computer icon. The IP address '192.168.168.0/24' is also shown below the 'Remote Site' box.

At the bottom of the page, there are three buttons: 'Cancel' on the left, 'Back' in the middle, and 'Finish' on the right (highlighted in green).

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

← VPN > Site to Site VPN

✓ Scenario

✓ Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate **Beta**

.....

default

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

←
VPN > Site to Site VPN >

✓ Scenario
 ✓ Network
 ✓ Authentication
 ✓ Policy & Routing
 5 Summary

Configuration

Name	BranchtoHQ		
IKE Version	2		
Type	Policy-based		
Proposal	<div>▼</div>		

Edit

Network

Local Site	192.168.1.100		
Remote Site	100.100.100.254		

Authentication

Authentication	pre-shared-key	<div> <div>.....</div> <div>🗐</div> </div>
----------------	----------------	--

Policy & Routing

Local Subnet	192.168.160.0/24		
--------------	------------------	--	--

Close

Test IPSec VPN Tunnel

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

Network Connection Details

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect...
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 2023
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

Administrator: Command Prompt

```

Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check

VPN Status > IPSec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh **Connectivity Check**

#	Name	Policy Route	Remote Gateway	My Address
1	HQtoBranch	192.168.168.0/24 <-> 192.168.160.0/24	100.100.200.254	100.100.100.254

Connectivity Check

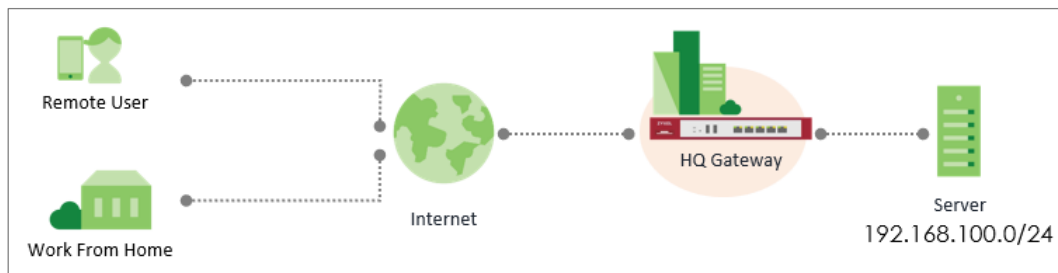
IP Address: 192.168.160.1 Test

Result
ICMP Connectivity Check PASS on sec_policy1_HQtoBranch

OK

How to Configure Remote Access VPN with Zyxel VPN Client

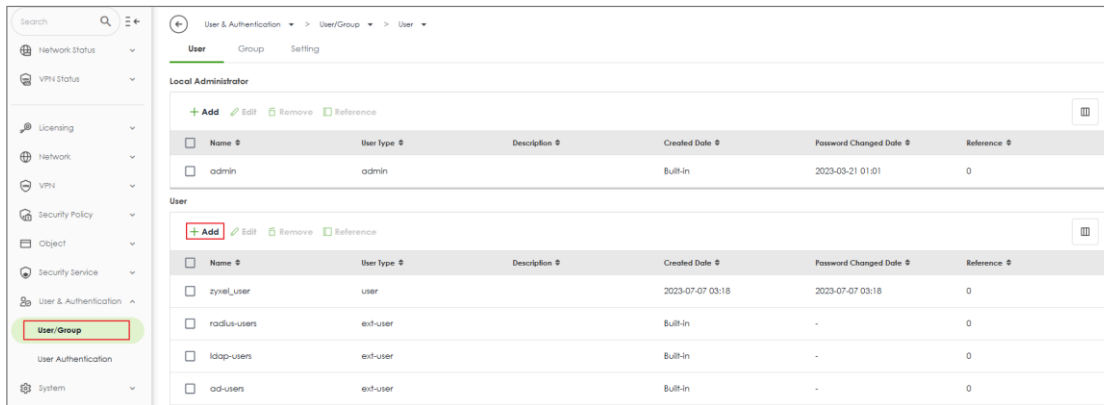
This example shows how to setup Remote Access VPN on USG FLEX H and Zyxel VPN Client. The example instructs how to implement Remote Access VPN by SSLVPN and IPSec VPN.



Before Begin

User & Authentication > User/Group > User

Create local user for remote access authentication.



Search []

Network Status [] VPN Status [] Licensing [] Network [] VPN [] Security Policy [] Object [] Security Service [] User & Authentication [] **User/Group** [] System []

User & Authentication > User/Group > User

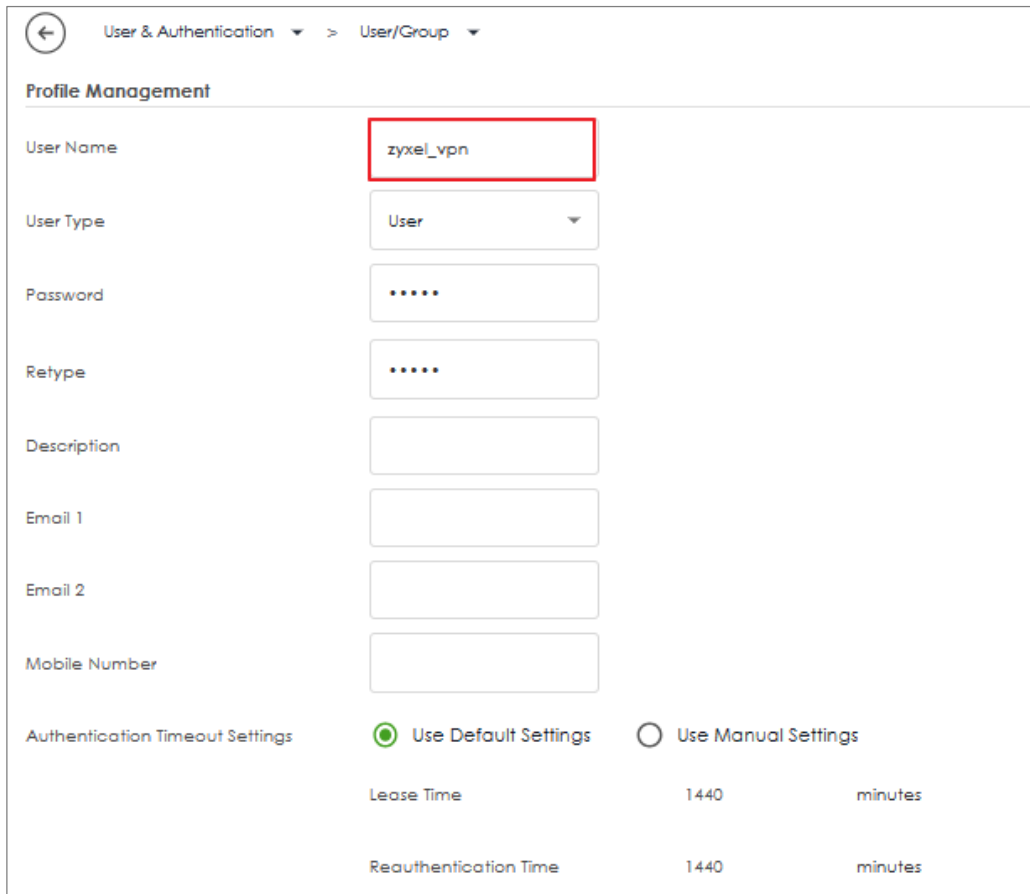
User Group Setting

Local Administrator

Name	User Type	Description	Created Date	Password Changed Date	Reference
admin	admin		Built-in	2023-03-21 01:01	0

User

Name	User Type	Description	Created Date	Password Changed Date	Reference
zyxel_user	user		2023-07-07 03:18	2023-07-07 03:18	0
radius-users	ext-user		Built-in	-	0
ldap-users	ext-user		Built-in	-	0
ad-users	ext-user		Built-in	-	0



User & Authentication > User/Group

Profile Management

User Name: **zyxel_vpn**

User Type: User

Password: []

Retype: []

Description: []

Email 1: []

Email 2: []

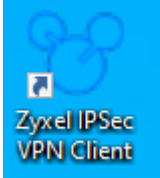
Mobile Number: []

Authentication Timeout Settings: ☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Download and install the new TGB Client

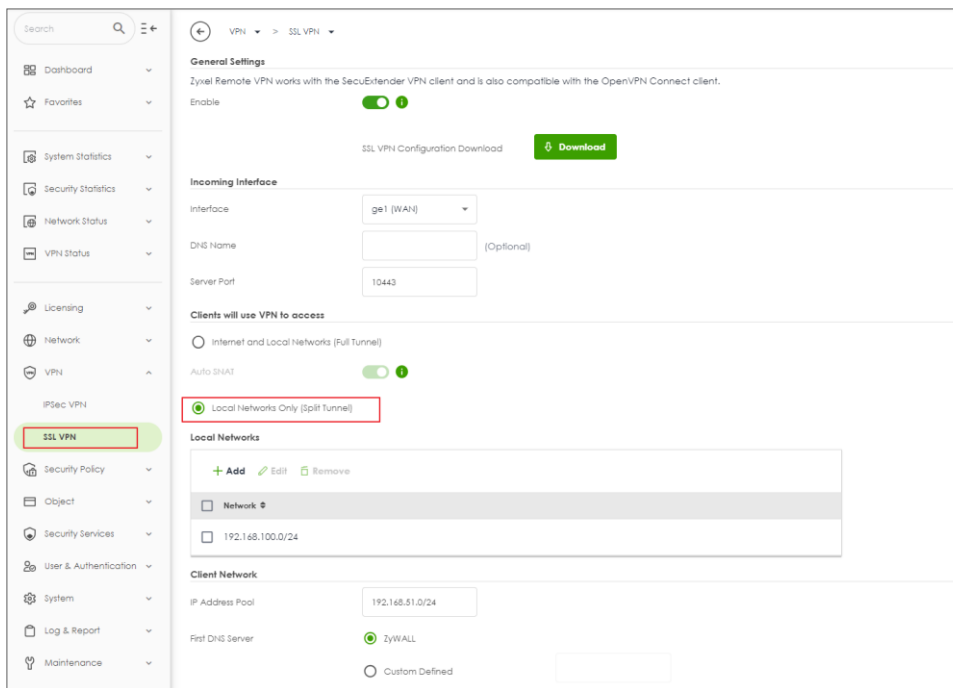


Set up SSL VPN

VPN > SSL VPN

Select the incoming interface, the default port is 10443. And up to your requirement to select Full Tunnel or Split Tunnel. And we now support OpenVPN config file.

For example: We pick up Split Tunnel and allows to access 192.168.100.0/24



The screenshot shows the ZyXEL SSL VPN configuration page. The left sidebar contains a navigation menu with options like Dashboard, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, IPsec VPN, and SSL VPN (which is highlighted). The main content area is titled 'VPN > SSL VPN' and includes a 'General Settings' section with an 'Enable' toggle switch. Below this is a 'Download' button for the 'SSL VPN Configuration Download'. The 'Incoming Interface' section has a dropdown menu set to 'ge1 (WAN)'. The 'Clients will use VPN to access' section has two radio buttons: 'Internet and Local Networks (Full Tunnel)' and 'Local Networks Only (Split Tunnel)', with the latter being selected. The 'Local Networks' section shows a table with one entry: 'Network 0' with the IP address '192.168.100.0/24'. The 'Client Network' section has an 'IP Address Pool' set to '192.168.51.0/24' and a 'First DNS Server' set to 'zyWALL'.

The default Address Pool is 192.168.51.0/24 and select the User who can access SSL VPN.

Client Network	
IP Address Pool	192.168.51.0/24
First DNS Server	<input checked="" type="radio"/> ZyWALL <input type="radio"/> Custom Defined
Second DNS Server	
Authentication	
Primary Server	local
Secondary Server	none
User	zyxel_vpn

Set up IKEv2 VPN

VPN > IPSec VPN > Remote Access VPN

Select the incoming interface. And up to your requirement to select Full Tunnel or Split Tunnel.

For example: We pick up Split Tunnel and allows to access 192.168.100.0/24

VPN > IPSec VPN > Remote Access VPN	
Site to Site VPN Remote Access VPN	
General Settings Zyxel's remote VPN solution uses leading IPsec/IKEv2 (EAP-MSCHAPv2) encryption, supported by SecuExtender VPN Client. You can also use native clients built into Windows, Android, macOS and iOS. Enable <input checked="" type="checkbox"/>	
Get SecuExtender VPN Client Software Windows macOS VPN configuration script download Windows iOS/macOS Android (strongSwan)	
Incoming Interface <input checked="" type="radio"/> Interface: get <input type="radio"/> Domain Name / IP:	
Certificate for VPN Validation <input checked="" type="radio"/> Auto <input type="radio"/> Manual: default	
Clients will use VPN to access <input type="radio"/> Internet and Local Networks (Full Tunnel) <input checked="" type="radio"/> Local Networks Only (Split Tunnel) Auto NAT <input checked="" type="checkbox"/>	
Local Network: 192.168.100.0/24	

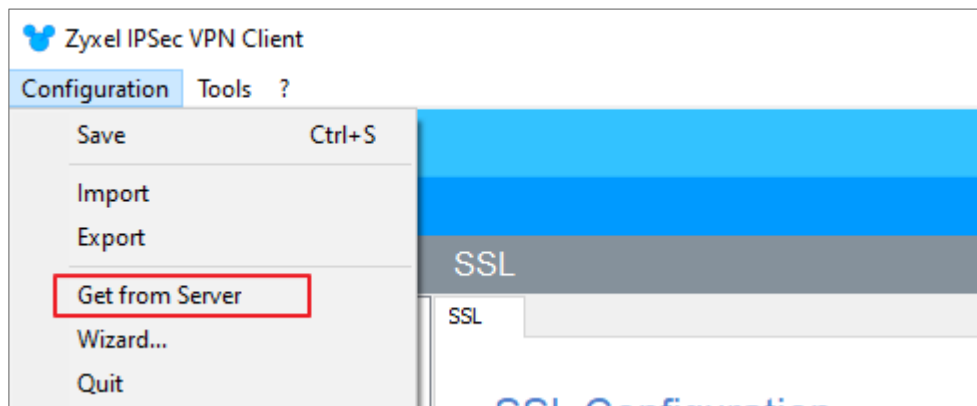
The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.

The screenshot shows the ZyXel VPN configuration interface. On the left is a sidebar with navigation options: Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, IPsec VPN (highlighted), SSL VPN, Security Policy, and Object. The main panel is titled 'Client Network' and contains the following settings:


- IP Address Pool:** 192.168.50.0/24 (highlighted with a red box)
- First DNS Server:** ZyWALL (selected with a radio button)
- Custom Defined:** (empty text box)
- Second DNS Server:** (empty text box)
- Authentication:**
 - Primary Server:** local (dropdown menu)
 - Secondary Server:** none (dropdown menu)
 - User:** zyxel_vpn (highlighted with a red box and a green checkmark icon)
- Advanced Settings:** (expandable section)



Set up Remote Access on TGB Client

The new TGB Client merge SSL VPN and IKEv2 VPN. You don't need additional software for each other.



Input the Gateway Address, Username and password to fetch configuration file.


VPN Configuration Server Wizard
✕

Step 1: Authentication



What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.

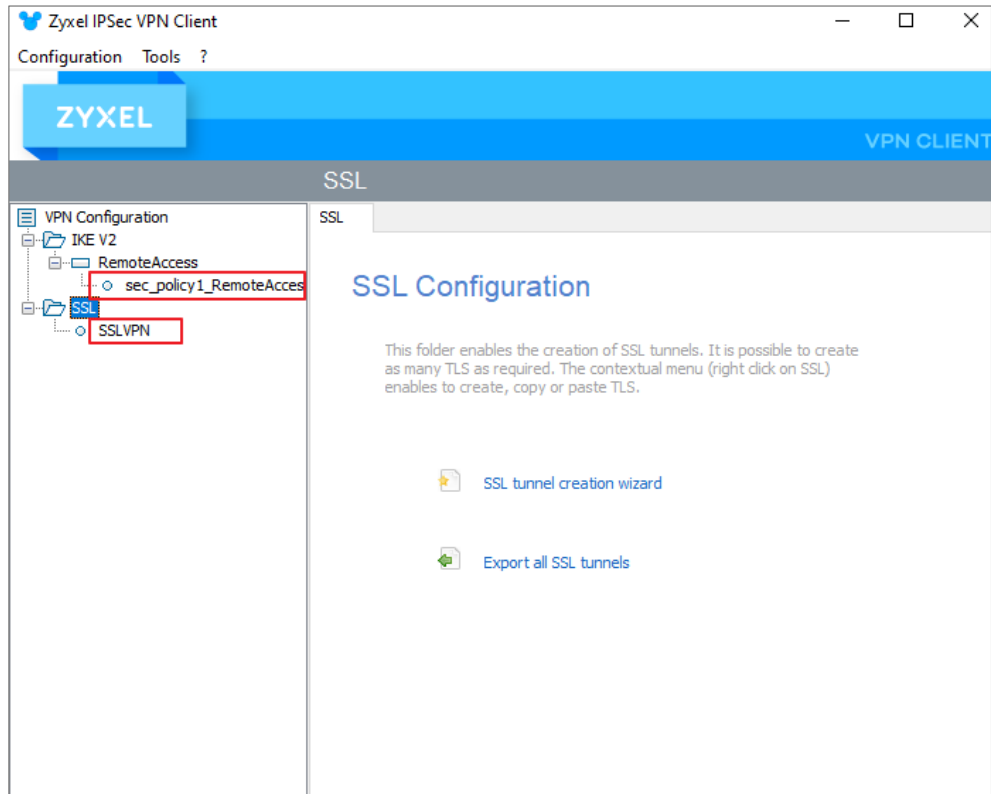
Gateway Address: Port:

Authentication:

Login:

Password:

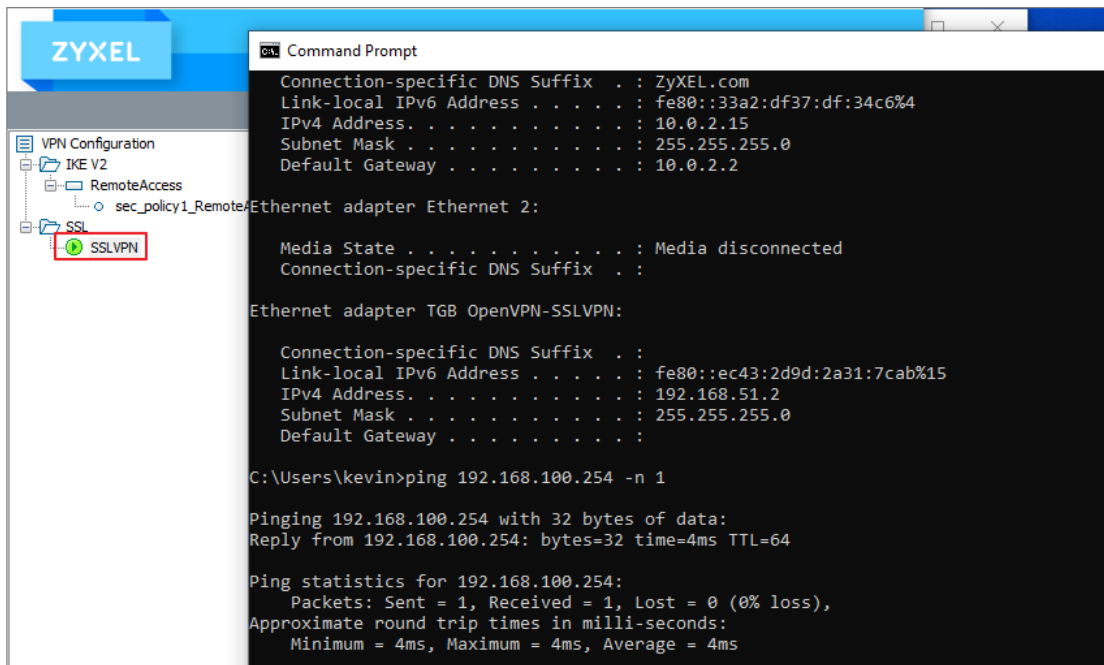
You will obtain IKEv2 as well as SSLVPN settings.



Test SSLVPN Tunnel on TGB Client

Right click the profile and "Open Tunnel" and log in.

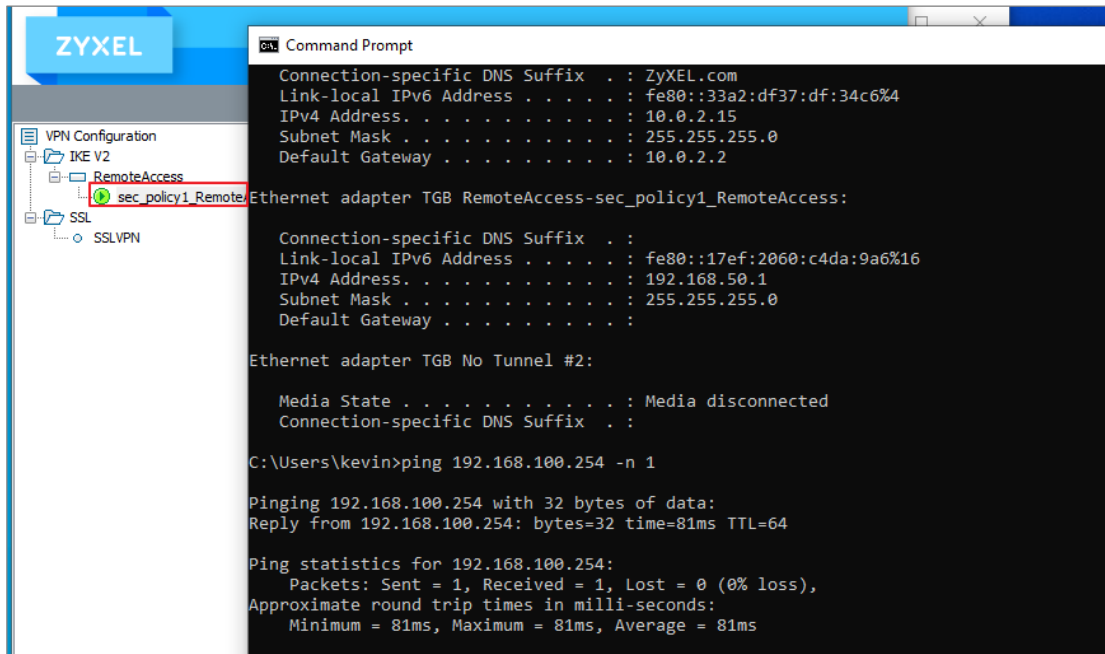
You will see the profile being green and can access internal resource now.



Test IKEv2 Tunnel on TGB Client

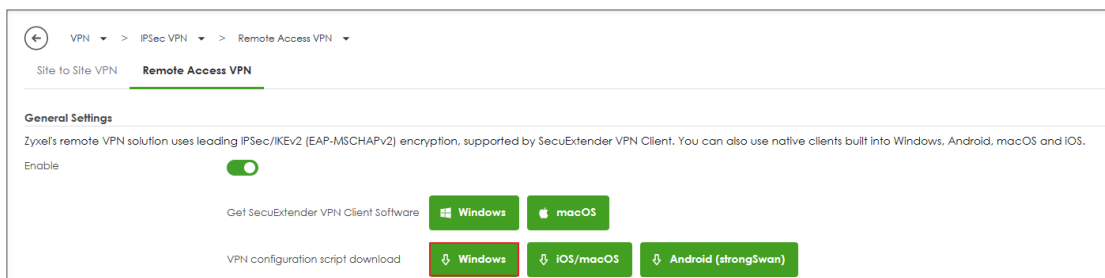
Right click the profile and "Open Tunnel" and log in.

You will see the profile being green and can access internal resource now.

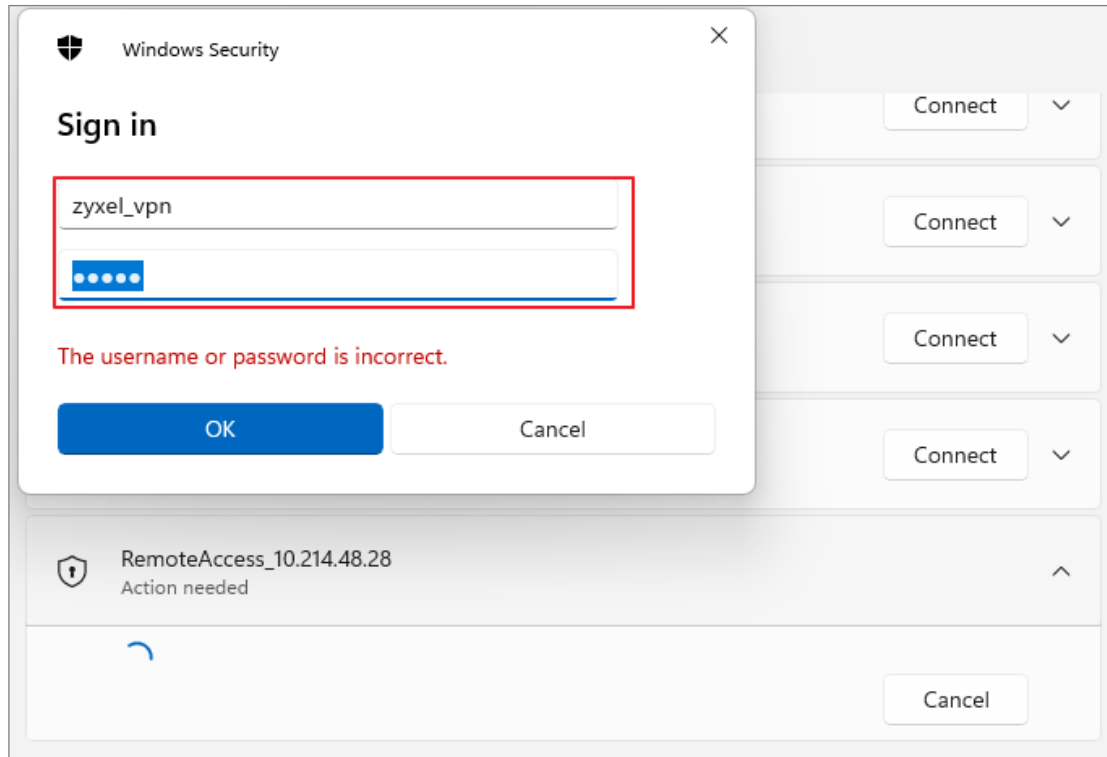


Test IKEv2 Tunnel on Windows Client

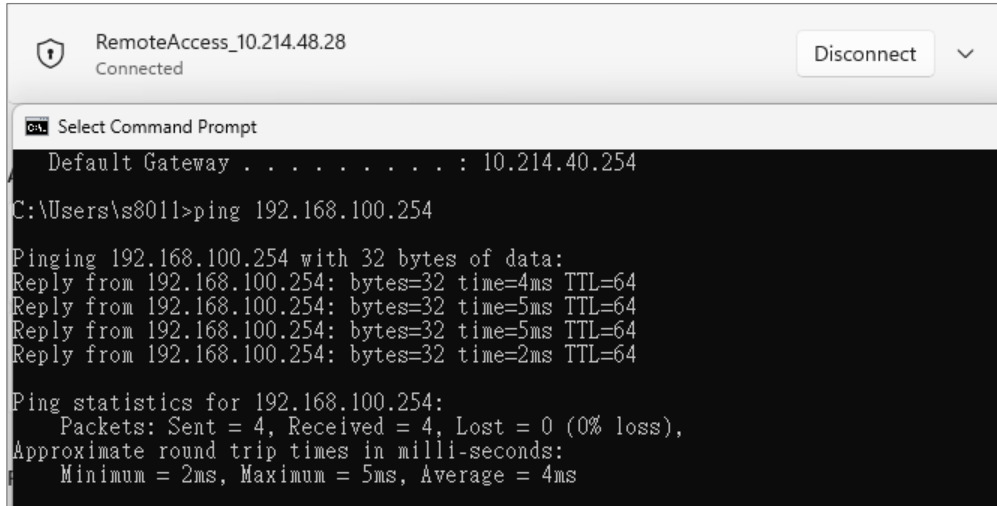
Download Windows VPN configuration script



Perform the windows bat file and input credentials.

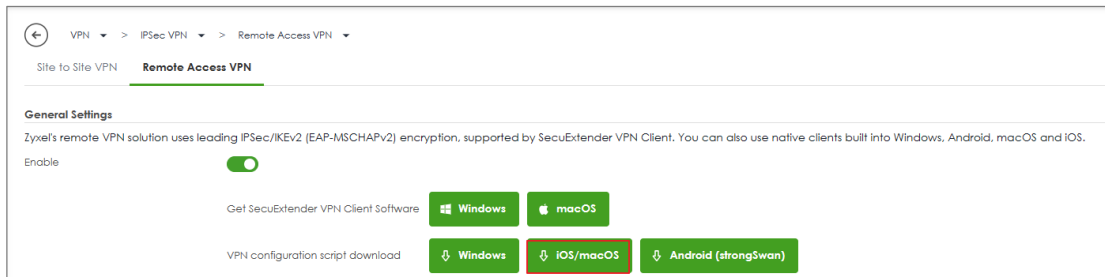


VPN is connected and can access internal resource.

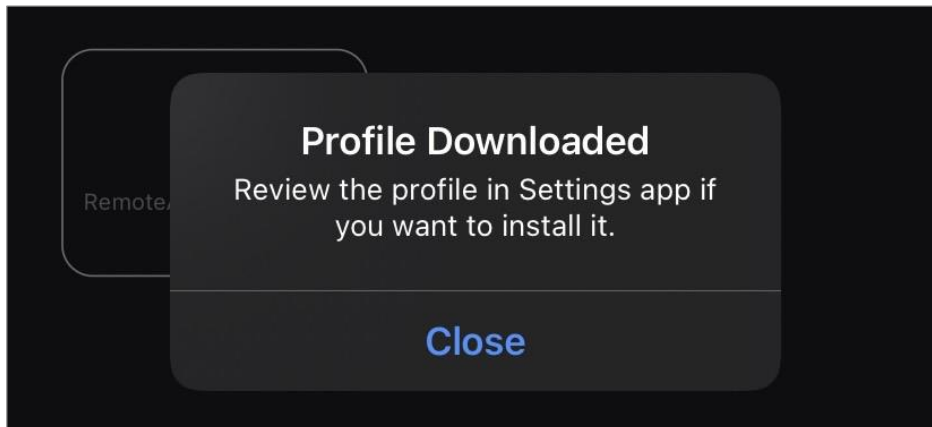


Test IKEv2 Tunnel on iOS Client

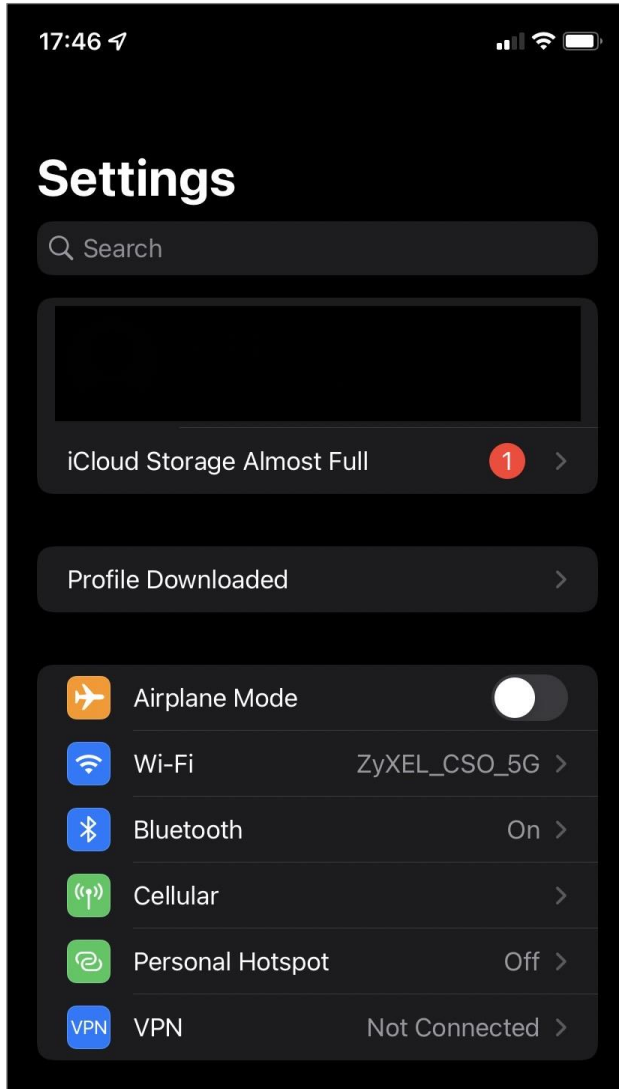
Download iOS/macOS VPN configuration script.



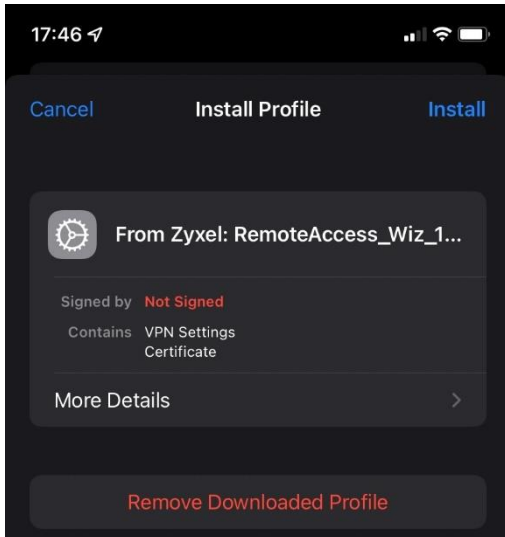
Send the script to Device.



Settings > Profile Downloaded



Press Install.



Enter Username and Password.

A screenshot of an iPhone screen showing the 'Enter Username' dialog. The dialog has three buttons at the top: 'Cancel' (blue), 'Enter Username' (black), and 'Next' (blue). The main text says 'ENTER YOUR USERNAME FOR THE VPN PROFILE "VPN"'. Below this is a text input field containing 'zyxel_vpn' with a clear button (X). At the bottom, it says 'Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.28" profile'.

[Cancel](#)
Enter Password
[Next](#)

ENTER YOUR PASSWORD FOR THE VPN PROFILE
"VPN"

✕

Requested by the "From Zyxel:
RemoteAccess_Wiz_10.214.48.28" profile

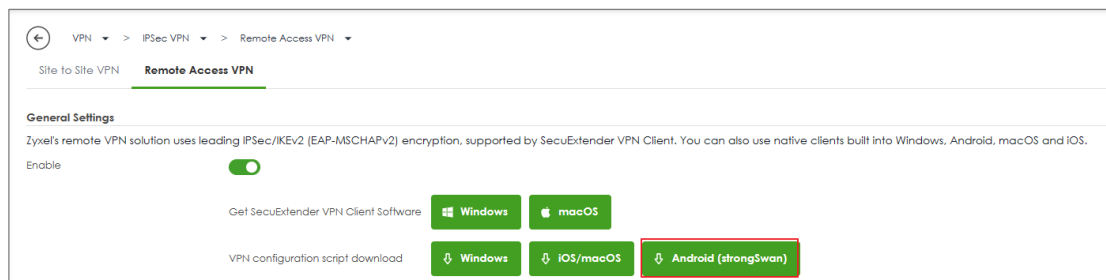
Now, it can connect.

[<](#)
RemoteAccess_Wiz_10.214.48.28
[Edit](#)

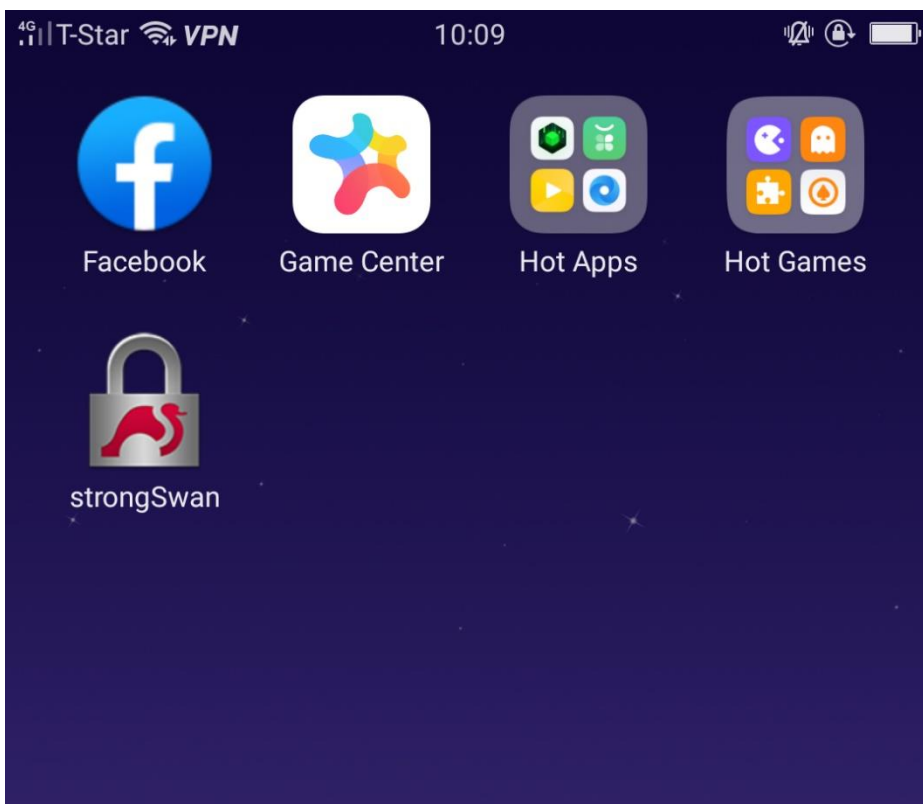
Type	IKEv2
Server	10.214.48.28
Account	zyxel_vpn
Address	192.168.50.1
Connect Time	0:09

Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



Download strongSwan from Google Play Store.



Send the script to device then Install and Import strongSwan profile.

15:51

Import VPN profile **IMPORT**

Profile name
RemoteAccess_10.214.48.28

Server
10.214.48.28

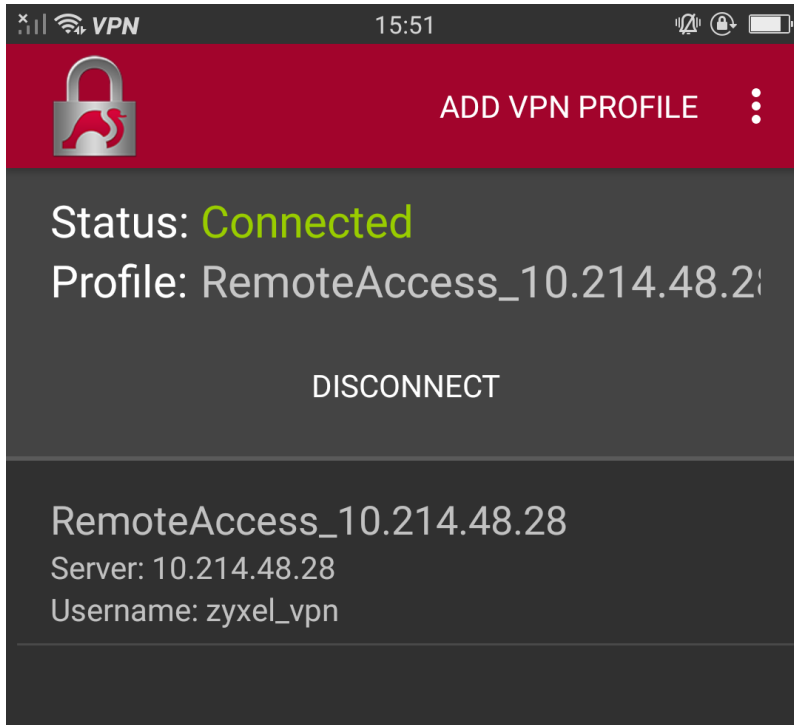
VPN Type
IKEv2 EAP (Username/Password)

Username
zyxel_vpn

Password (optional)
.....

CA certificate
10.214.48.28

VPN is connected.



VPN > SSL VPN

VPN > SSL VPN

General Settings

Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.

Enable

SSL VPN Configuration Download

Download

Incoming Interface

Interface

ge1 (WAN)

DNS Name

(Optional)

Server Port

10443

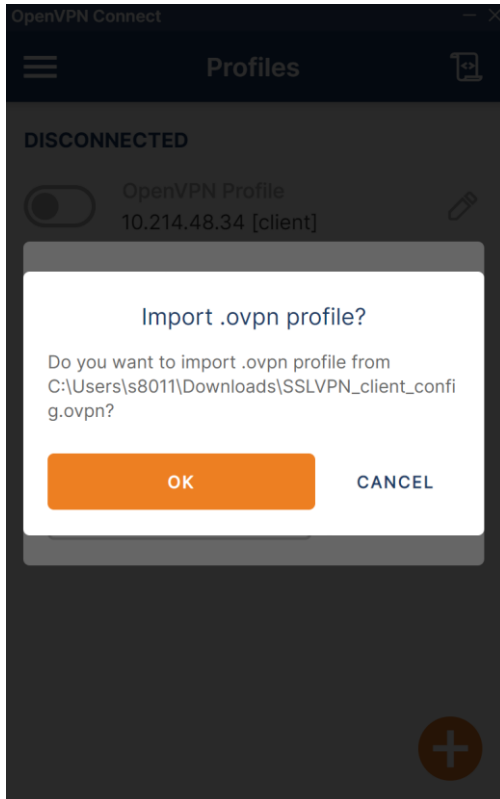
Clients will use VPN to access

Internet and Local Networks (Full Tunnel)

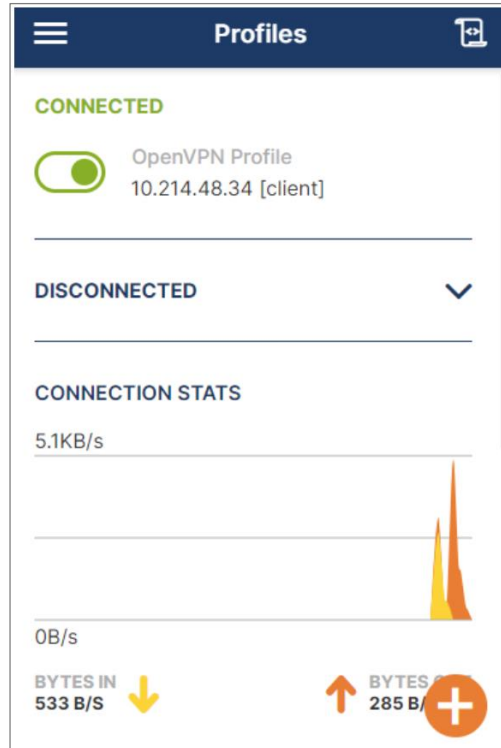
Auto SNAT

Local Networks Only (Split Tunnel)

Import the config file.

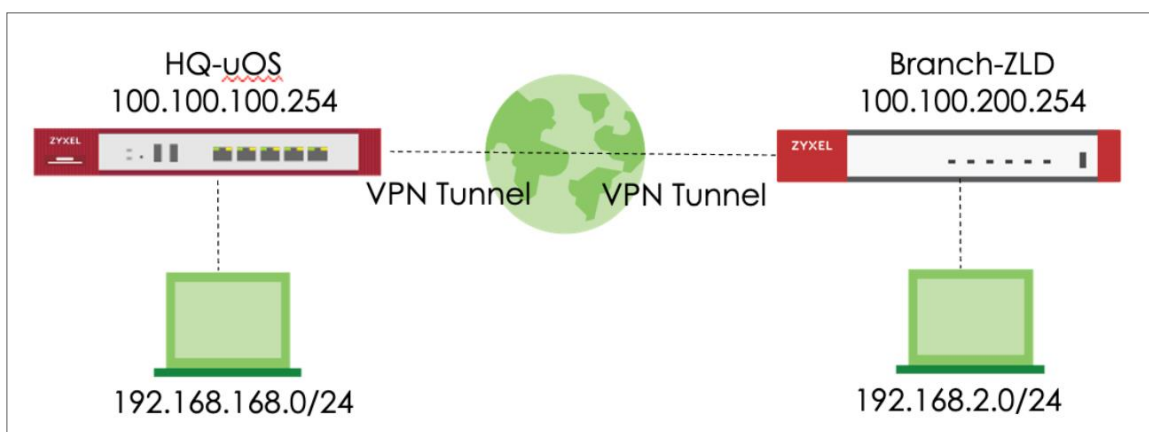


VPN is connected.



How to Configure Site-to-site IPSec VPN between ZLD and uOS device

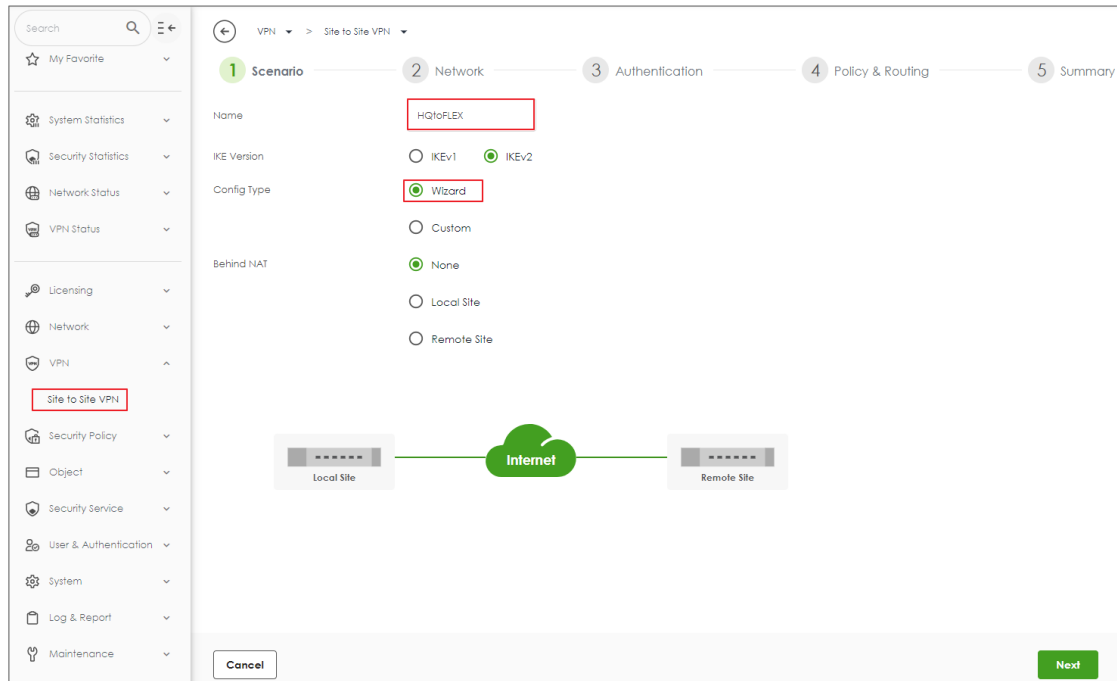
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer gateway is ZLD device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for uOS

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



Search

My Favorite

System Statistics

Security Statistics

Network Status

VPN Status

Licensing

Network

VPN

Site to Site VPN

Security Policy

Object

Security Service

User & Authentication

System

Log & Report

Maintenance

VPN > Site to Site VPN

1 Scenario 2 Network 3 Authentication 4 Policy & Routing 5 Summary

Name: HQ10FLEX

IKE Version: ☐ IKEv1 ☒ IKEv2

Config Type: ☒ Wizard ☐ Custom

Behind NAT: ☒ None ☐ Local Site ☐ Remote Site

Local Site Internet Remote Site

Cancel Next

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN > Site to Site VPN

✓ Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address	Domain Name / IP	100.100.100.254
Peer Gateway Address	Domain Name / IP	100.100.200.254

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to USG FLEX H and Remote Subnet to be the IP address of the network connected to the peer ZyWALL.

VPN
>
Site to Site VPN

Scenario
Network
Authentication
4 Policy & Routing
5 Summary

Type

Route-Based
Policy-Based

Local Subnet

192.168.168.0/24

Remote Subnet

192.168.2.0/24

192.168.168.0/24

Local Site
100.100.100.254

Internet

Remote Site
100.100.200.254

192.168.2.0/24

Cancel

Back

Finish

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

 Edit

Set up IPsec VPN Tunnel for ZLD

VPN > IPsec VPN > VPN Gateway

Select the WAN interface and type the Peer Gateway Address.

Add VPN Gateway

Show Advanced Settings Create New Object ▼

General Settings

☒ Enable

VPN Gateway Name: FLEXtouOS

IKE Version

☐ IKEv1

☒ IKEv2

Gateway Settings

My Address

☒ Interface wan Static -- 100.100.200.254/255.255.0.0

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address ⓘ

Primary 100.100.100.254

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address ⓘ

OK Cancel

Type Pre-shared Key. The default proposal which created by wizard is "Encryption:AES128, Authentication:SHA1, Key Group:DH2". Those are the same as uOS.

Add VPN Gateway

Show Advanced Settings Create New Object ▼

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate RemoteAccess_10 (See [My Certificates](#))

Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

Proposal

#	Encryption	Authentication
1	AES128	SHA1

Key Group: DH2

OK Cancel

VPN > IPSec VPN > VPN Connection

Select VPN Gateway and set Local Subnet to be the IP address of the network connected to be ZyWALL and Remote Subnet to be the IP address of the network connected to the peer USG FLEX H.

Edit VPN Connection FLEXtouOS_P2

Show Advanced Settings Create New Object ▼

General Settings

☒ Enable

Connection Name: FLEXtouOS_P2

☒ Advance

VPN Gateway

Application Scenario

- ☒ Site-to-site
- ☐ Site-to-site with Dynamic Peer
- ☐ Remote Access (Server Role)
- ☐ Remote Access (Client Role)
- ☐ VPN Tunnel Interface

VPN Gateway: FLEXtouOS wan 100.100.100.254, 0.0.0.0

Policy

Local Policy: LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24

Remote Policy: uOS_subnet SUBNET, 192.168.168.0/24

OK Cancel

The default proposal which created by wizard is "Encryption: AES128, Authentication: SHA1, Key Group: DH2". Those are the same as uOS.

Add VPN Connection

Hide Advanced Settings Create New Object

Phase 2 Setting

SA Life Time: 28800 (180 - 3000000 Seconds)

Advanced

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	AES128	SHA1

Perfect Forward Secrecy (PFS): DH2

Related Settings

Zone: IPSec_VPN

Connectivity Check

☒ Enable Connectivity Check

Check Method: icmp

OK Cancel

Test IPSec VPN Tunnel

Ping the PC that is connected to ZLD device

Win 11 > cmd > ping 192.168.2.34

```

Connection-specific DNS Suffix . : 
IPv4 Address. . . . . : 
Subnet Mask . . . . . : 
IPv4 Address. . . . . : 
Subnet Mask . . . . . : 
IPv4 Address. . . . . : 192.168.1.4
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 192.168.168.54
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Ethernet adapter 4:

C:\Windows\system32>ping 192.168.2.34

Pinging 192.168.2.34 with 32 bytes of data:
Reply from 192.168.2.34: bytes=32 time=21ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.2.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 21ms, Average = 7ms
  
```

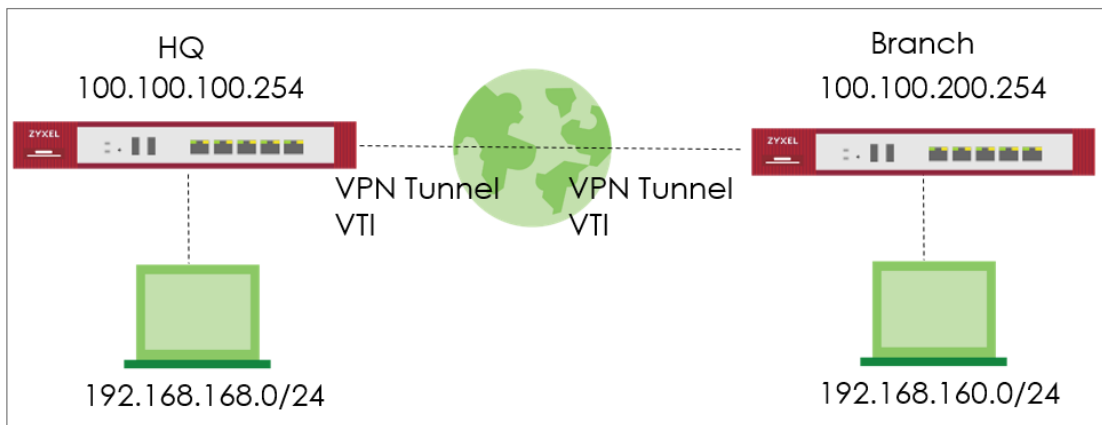
VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check

The screenshot shows the Zyxel VPN Status interface. The 'VPN Status' tab is selected, and the 'IPSec VPN' section is active. Under 'Site to Site VPN', the 'Connectivity Check' button is highlighted with a red box. A 'Connectivity Check' dialog box is open, showing the IP Address '192.168.160.1' and a 'Test' button. The 'Result' section displays: 'ICMP Connectivity Check PASS on sec_policy1_HQtoFLEX'. An 'OK' button is at the bottom right of the dialog.

How to Configure Route-Based VPN

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPsec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.

The screenshot shows the ZyXel VPN configuration interface. On the left is a sidebar menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPNs (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the 'VPN > Site to Site VPN' configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. In the 'Scenario' step, the following settings are visible:

- *Name: HQtoBranch (highlighted with a red box)
- IKE Version: ☐ IKEv1, ☒ IKEv2
- Type: ☒ Site-to-Site (highlighted with a red box), ☐ Custom
- Behind NAT: ☒ None, ☐ Local Site, ☐ Remote Site

 Below the settings is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is then connected to a 'Remote Site'. At the bottom of the configuration area are 'Cancel' and 'Next' buttons.

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN > Site to Site VPN >

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address

Domain Name / IP

100.100.100.254

Peer Gateway Address

Domain Name / IP

100.100.200.254

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default ▾

Cancel Back Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Type to Route-Based and configure the Remote Subnet.

VPN > Site to Site VPN

Scenario Network Authentication **4 Policy & Routing** 5 Summary

Type ☒ Route-Based ☐ Policy-Based

Remote Subnet 192.168.160.0/24

Any Local Site 100.100.100.254 Internet Remote Site 100.100.200.254 192.168.160.0/24

Cancel Back Finish

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing >

Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

VPN > Site to Site VPN

✓ Scenario

✓ Network

✓ Authentication

✓ Policy & Routing

5 Summary

Configuration

Name	HQtoBranch
IKE Version	2
Scenario	wizard
Type	Route

Edit

Network

Local Site	100.100.100.254
Remote Site	100.100.200.254

Authentication

Authentication	pre-shared-key	<div> </div>
----------------	----------------	--------------

Policy & Routing

Remote Subnet	192.168.160.0/24
---------------	------------------

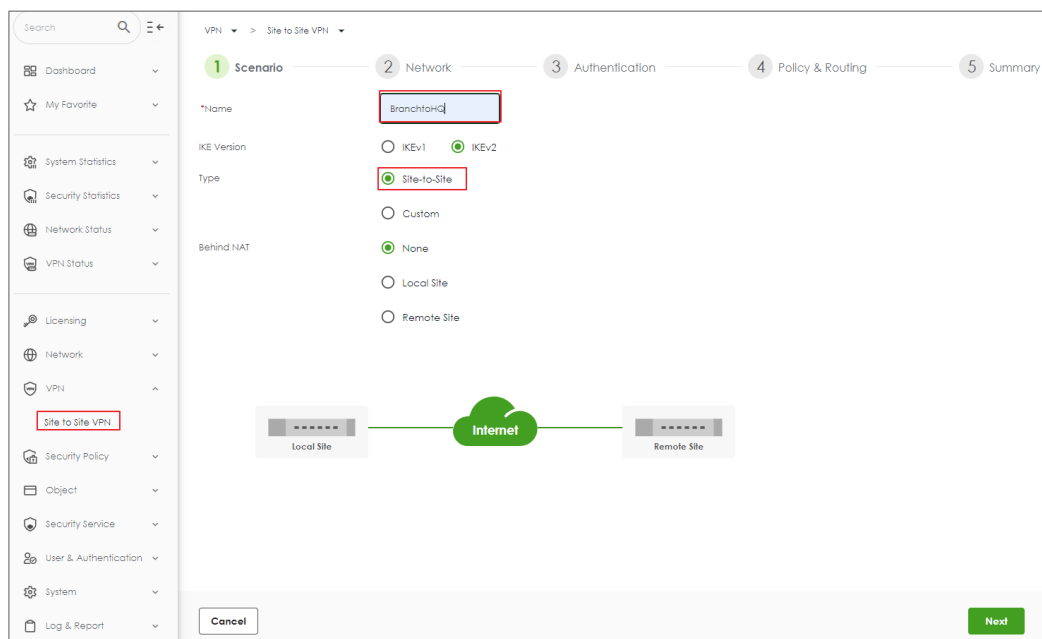
Close

Set up IPsec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site.

Click **Next**.



The screenshot shows the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the 'Scenario' step of a 5-step process (Scenario, Network, Authentication, Policy & Routing, Summary). The configuration details are as follows:

- Name:** BranchHQ (text input field)
- IKE Version:** ☒ IKEv1, ☐ IKEv2
- Type:** ☒ Site-to-Site, ☐ Custom
- Behind NAT:** ☒ None, ☐ Local Site, ☐ Remote Site

Below the configuration options is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is then connected to a 'Remote Site'. At the bottom of the form are 'Cancel' and 'Next' buttons.

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

VPN > Site to Site VPN >

✓ Scenario
2 Network
3 Authentication
4 Policy & Routing
5 Summary

My Address

Domain Name / IP

100.100.200.254

Peer Gateway Address

Domain Name / IP

100.100.100.254

Local Site

100.100.200.254

Internet

Remote Site

100.100.100.254

Cancel

Back

Next

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Type to Route-Based and Remote Subnet.

VPN > Site to Site VPN

✓ Scenario — ✓ Network — ✓ Authentication — **4 Policy & Routing** — 5 Summary

Type ☒ Route-Based ☐ Policy-Based

Remote Subnet 192.168.168.0/24

Any 100.100.200.254 Internet 100.100.100.254 192.168.168.0/24

Cancel Back Finish

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.

VPN > Site to Site VPN >

✓ Scenario
✓ Network
✓ Authentication
✓ Policy & Routing
5 Summary

Configuration

Name	BranchtoHQ	
IKE Version	2	
Scenario	wizard	
Type	Route	

Edit

Network

Local Site	100.100.200.254	
Remote Site	100.100.100.254	

Authentication

Authentication	pre-shared-key	*****
----------------	----------------	-------

Policy & Routing

Remote Subnet	192.168.168.0/24	
---------------	------------------	--

Close

Test IPsec VPN Tunnel

VPN Status > IPsec VPN

Verify the IPsec VPN status.

VPN Status

IPSec VPN

Site to Site VPN

Site to Site VPN

Remote Access VPN

Disconnect

Refresh

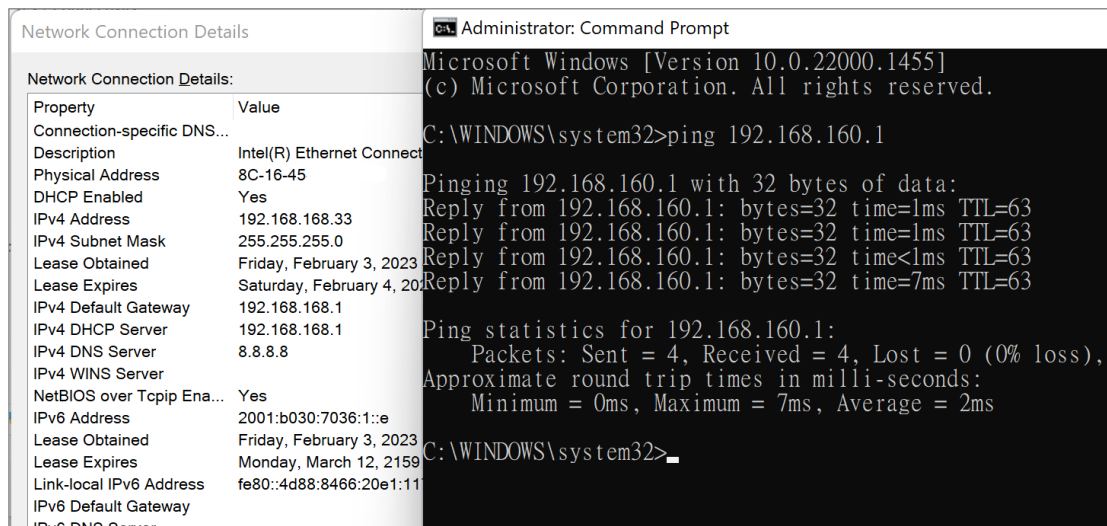
Connectivity Check

Search insights

<div><div></div></div>	#	Name	Policy Route	Remote Gateway	My Address	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
Custom									
<div><div></div></div>	1	HQtoBranch	0.0.0.0/0 <-> 0.0.0.0/0	100.100.200.254	100.100.100.254	183	25962	6 (240 bytes)	0 (0 bytes)

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



Network Connection Details

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect...
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 2023
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

Administrator: Command Prompt

```

Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

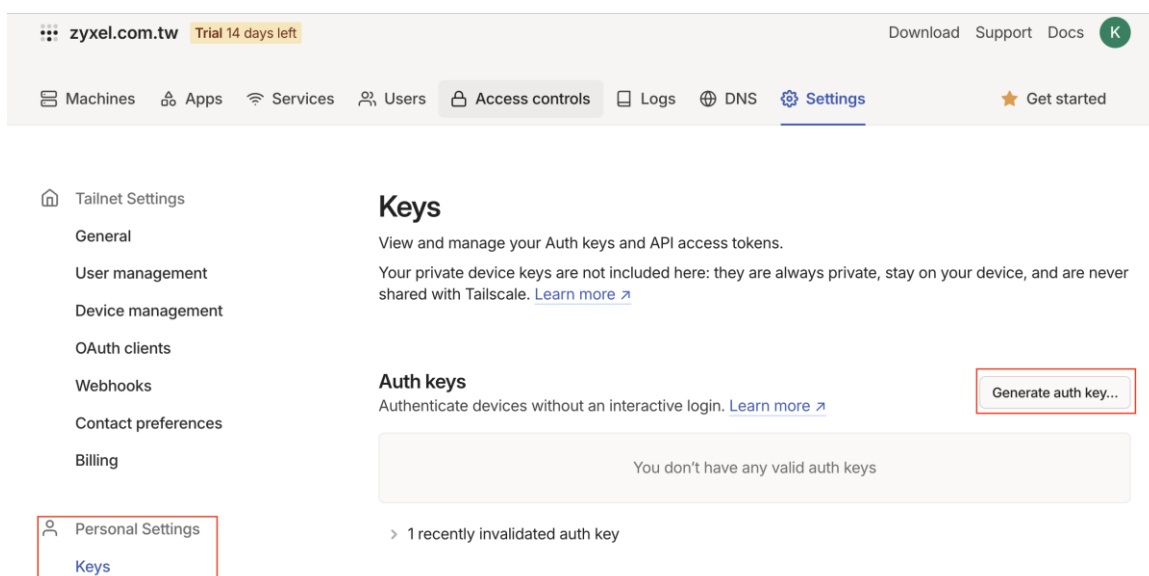

How to Use Tailscale

What's Tailscale?

Tailscale is a secure, peer-to-peer VPN solution that simplifies connecting devices over the internet. Unlike traditional VPNs, Tailscale establishes direct connections between devices without requiring complex firewall configurations or static IP addresses. It uses a mesh network topology, allowing every device to communicate directly with every other device securely.

Start to Tailscale and implement on Firewall

1. Please refer [TailScale KB](#) to create an account and start.
2. Navigate to "Settings -> Personal Settings -> Keys" and "Generate auth key".



The screenshot shows the Tailscale web interface for a user account. The top navigation bar includes the user's email (zyxel.com.tw), a trial status (Trial 14 days left), and links for Download, Support, Docs, and a profile icon. The main navigation menu lists various settings categories: Machines, Apps, Services, Users, Access controls, Logs, DNS, and Settings (which is highlighted). A 'Get started' button is also present. On the left sidebar, under 'Tailnet Settings', the 'Personal Settings' section is expanded, and the 'Keys' sub-section is selected. The main content area is titled 'Keys' and provides instructions on managing auth keys and API access tokens. It includes a 'Generate auth key...' button, which is highlighted with a red box. Below this, a message states 'You don't have any valid auth keys' and a link to view '1 recently invalidated auth key'.

3. Give a Description Name as you want and disable "Reusable" due to security reason then click "Generate key".

Generate auth key ×

Description
Add an optional description for the key.

Reusable ☐
Use this key to authenticate more than one device.

Expiration
Number of days until this auth key expires. This will not affect the [node key expiry](#) of any machine authenticated with this auth key.

— +

Must be between 1 and 90 days.

DEVICE SETTINGS
These settings will apply to any devices authenticated using this key.

Ephemeral ☐
Devices authenticated by this key will be automatically removed after going offline. [Learn more ↗](#)

Tags ☐
Devices authenticated by this key will be automatically tagged. This will also disable node key expiry for the device. [Learn more ↗](#)

Copy the key.

Generated new key



Be sure to copy your new key below. It won't be shown in full again.

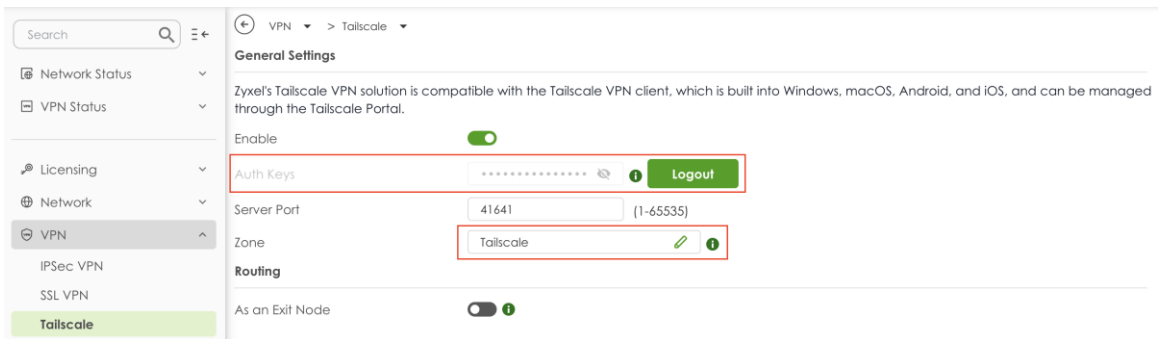
tskey-auth-kc5HbhKcQQ11CNTRL-



This key will expire on Jun 2, 2025. If you'll then want to continue using an auth key, you'll need to generate a new one.

Done

4. Login Firewall and navigate to "VPN -> Tailscale", paste to the "Auth Keys".



Note:

- When you want to change the key, please click Logout.
- You can choose the zone by yourself. We recommend using Tailscale zone for some predefined rules.

- Go back to the Tailscale admin page. You will see the Firewall device.

zyxel.com.tw Trial 14 days left Download Support Docs K

Machines Apps Services Users Access controls Logs DNS Settings Get started

Machines

Manage the devices connected to your tailnet. [Learn more](#) Add device

Search by name, owner, tag, version... Filters

2 machines

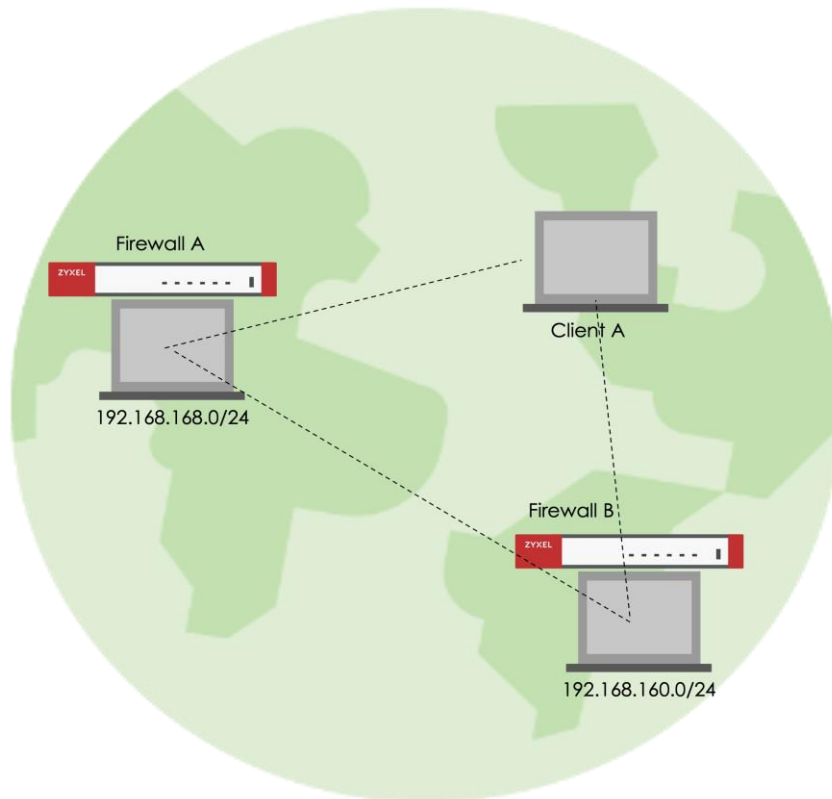
MACHINE	ADDRESSES	VERSION	LAST SEEN
twbnbt123234-01 Kevin.Wu4@zyxel.com.tw	100.95.1	1.80.2 Windows 11 22H2	Connected
usgflex500h Kevin.Wu4@zyxel.com.tw	100.115.1	1.75.16 Linux 4.14.207-10.3.7.0-2	Connected

Click "Disable key expiry" for all client to prevent lost connection while expire.

usgflex500h Kevin.Wu4@zyxel.com.tw Subnets Exit Node	100.115.120.97	1.75.16 Linux 4.14.207-10.3.7.0-2	Connected	Share... <div> <div>Edit machine name...</div> <div>Edit machine IPv4...</div> <div>Share...</div> <div>Disable key expiry</div> </div>
client-a Kevin.Wu4@zyxel.com.tw	100.95.1.123	1.80.2 Windows 11 22H2	Mar 5, 4:50 PM GMT+8	
iphone-15 Kevin.Wu4@zyxel.com.tw	100.78.218.72	1.80.2 iOS 18.3.1	Mar 5, 2:48 PM GMT+8	

Scenario

We have two subnets, 192.168.168.0/24 and 192.168.160.0/24, which are located behind firewalls. Both the firewalls and the Client A are part of the Tailscale VPN network. The objectives are as follows:



Case1: Allow Client A to access the 192.168.168.0/24 and 192.168.160.0/24 subnets

1. Advertised 192.168.168.0/24 in Firewall A.

VPN
>
Tailscale

General Settings

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable ☒

Auth Keys

Server Port (1-65535)

Zone

Routing

As an Exit Node ☐

Advertised Networks

+ Add Remove

Network
<input type="checkbox"/> N_192_168_168

2. Advertised 192.168.160.0/24 in Firewall B.

VPN
>
Tailscale

General Settings

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable ☒

Auth Keys

Server Port (1-65535)

Zone

Routing

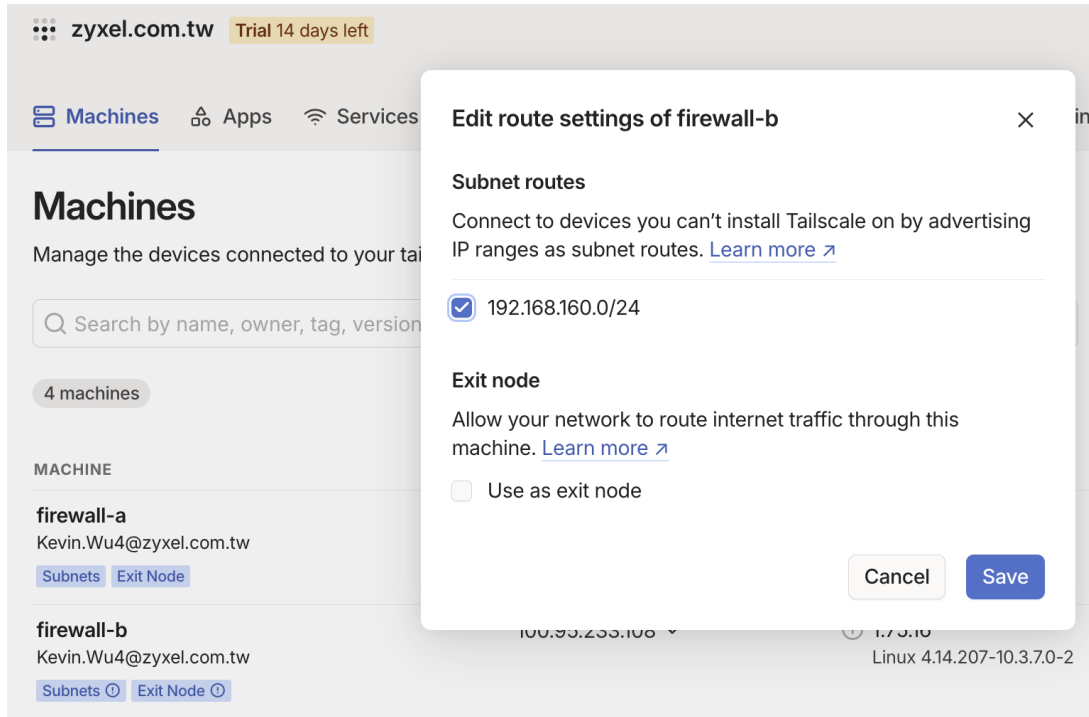
As an Exit Node ☐

Advertised Networks

+ Add Remove

Network
<input type="checkbox"/> N_192_168_160

3. Ensure Both subnets have been approved from Tailscale portal.



Test the Result

Now, Client A know how to route traffic and able to access 192.168.168.1 and 192.168.160.1.

```
C:\Users\NT03234\Downloads>route print | findstr "192.168.168.0 192.168.160.0"
192.168.160.0 255.255.255.0 100.100.100.100 100.95.1.123 0
192.168.168.0 255.255.255.0 100.100.100.100 100.95.1.123 0

C:\Users\NT03234\Downloads>ping -n 2 192.168.168.1

Pinging 192.168.168.1 with 32 bytes of data:
Reply from 192.168.168.1: bytes=32 time=80ms TTL=64
Reply from 192.168.168.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.168.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 80ms, Average = 41ms

C:\Users\NT03234\Downloads>ping -n 2 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=258ms TTL=64
Reply from 192.168.160.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.160.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 258ms, Average = 130ms
```

Case 2: Allow Client A to access internet through Firewall

1. Take Firewall A as example. Enable "Exit Node" and "Default SNAT".

VPN
>
Tailscale

General Settings

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable
☒

Auth Keys

.....

Logout

Server Port

41641

(1-65535)

Zone

Tailscale

Routing

As an Exit Node
☒

Advertised Networks

+ Add

Remove

☐
Network

☐
N_192_168_168

Advanced Settings

Accept routes
☒

Default SNAT
☒

2. Ensure the Exit-Node have been enabled from Tailscale portal.

Edit route settings of firewall-a



Key expiry is enabled

If this machine's [key expires](#), your relayed traffic may be interrupted until you reauthenticate.

Subnet routes

Connect to devices you can't install Tailscale on by advertising IP ranges as subnet routes. [Learn more ↗](#)

☒ 192.168.168.0/24

Exit node

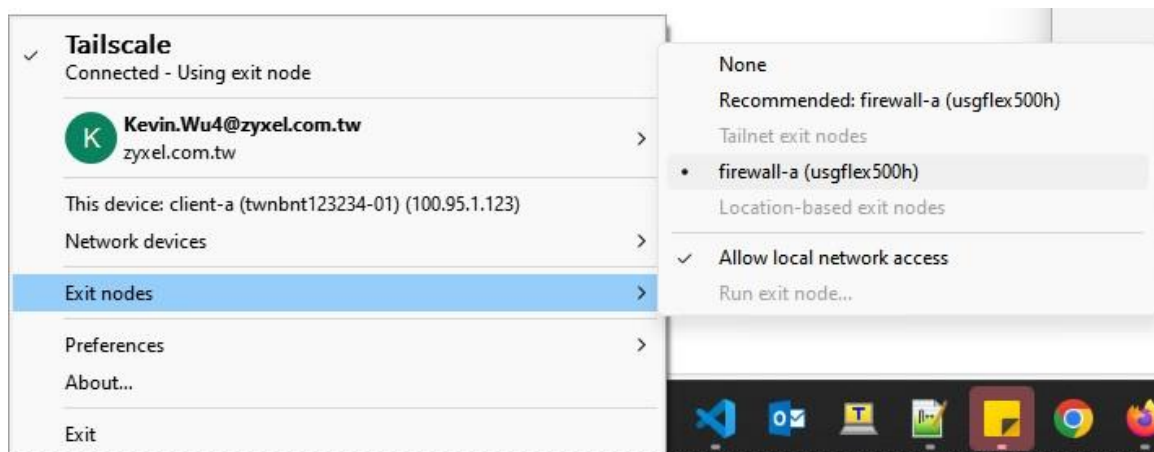
Allow your network to route internet traffic through this machine. [Learn more ↗](#)

☒ Use as exit node

Cancel

Save

3. Client A need to select Firewall A as exit node.



Test the Result

The internet traffic will send to Firewall A.

```
C:\Users\NT03234>route print | findstr "0.0.0.0"
        0.0.0.0          0.0.0.0          192.168.1.1          192.168.1.40          400
        0.0.0.0          0.0.0.0          100.100.100.100      100.95.1.123          0
        224.0.0.0         240.0.0.0         On-link              127.0.0.1             331
        224.0.0.0         240.0.0.0         On-link              192.168.56.1           281
        224.0.0.0         240.0.0.0         On-link              169.254.122.18         281
        224.0.0.0         240.0.0.0         On-link              192.168.1.40           456

C:\Users\NT03234>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops
  0  2 ms  2 ms  1 ms  100.115.120.97
  1  4 ms  2 ms  2 ms  10.214.48.254
```

Case3: The devices within the 192.168.168.0/24 and 192.168.160.0/24 subnets can communicate with each other

Once you completed advertised Networks, you can communicate each other.

Test the Result

The ping test from Firewall A

```
[kevin@wujiayuandeMacBook-Air 0219 % ifconfig en5
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=404<VLAN_MTU,CHANNEL_IO>
    ether 20:7b:d2:5f:c9:d5
    inet6 fe80::10:9bda:e5fd:a6c7%en5 prefixlen 64 secured scopeid 0x16
    inet 192.168.168.4 netmask 0xffffffff00 broadcast 192.168.168.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (1000baseT <full-duplex>)
    status: active
[kevin@wujiayuandeMacBook-Air 0219 % ping 192.168.160.33
PING 192.168.160.33 (192.168.160.33): 56 data bytes
64 bytes from 192.168.160.33: icmp_seq=0 ttl=126 time=3.301 ms
64 bytes from 192.168.160.33: icmp_seq=1 ttl=126 time=3.267 ms
--
```

The ping test from Firewall B

```
IPv4 Address. . . . . : 192.168.160.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::daec:e5ff:fe62:a7b9%23
                          192.168.160.1

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter 藍牙網路連線:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\NT03234\Downloads>ping 192.168.168.4 -n 2

Pinging 192.168.168.4 with 32 bytes of data:
Reply from 192.168.168.4: bytes=32 time=3ms TTL=62
Reply from 192.168.168.4: bytes=32 time=3ms TTL=62

Ping statistics for 192.168.168.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

How to use Ext-group user to connect Remote Access VPN

Remote Access VPN now supports using external user groups for VPN accounts. This article will guide you through the setup process

Before Begin

You already followed Topic "How to configure Remote Access VPN with ZyXel VPN Client" as well as "How to setup AD authentication with Microsoft AD" to complete Remote Access and Authentication server settings.

User & Authentication > User/Group > User

Create a user and select User type as ext-group-user. At this point, the group identifier will Automatically populate with the CN that has the group attribute.

← User & Authentication > User/Group > User >

Profile Management

User Name	VPN		
User Type	ext-group-user		
Authentication Server	AD / AD		
Group Identifier	cn=vpngroup,ou=Group,dc=cs0,dc=com		
Description			
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings		
	Lease Time	1440	minutes
	Reauthentication Time	1440	minutes

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

User Name	<input type="text"/> <input type="button" value="Test"/>
-----------	--

VPN > SSL VPN

Taking SSL VPN as an example, User select the ext-group user you just created. And choosing AD authentication.

VPN

SSL VPN

General Settings

Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.

Enable

i

SSL VPN Configuration Download

Download

Incoming Interface

Interface

ge2 (WAN)

DNS Name

(Optional)

Server Port

10443

Zone

SSL_VPN

i

Clients will use VPN to access

Internet and Local Networks (Full Tunnel)

Auto SNAT

i

Local Networks Only (Split Tunnel)

Client Network

IP Address Pool

192.168.4.0/24

First DNS Server

ZyWALL

Custom Defined

Second DNS Server

Authentication

i

Primary Server

AD / AD

Secondary Server

local

User

VPN

i

Test the Result

VPN Status > SSL VPN > Remote Access VPN

User within the group can successfully connect

VPN Status > SSL VPN > Remote Access VPN

Remote Access VPN

Disconnect
Refresh

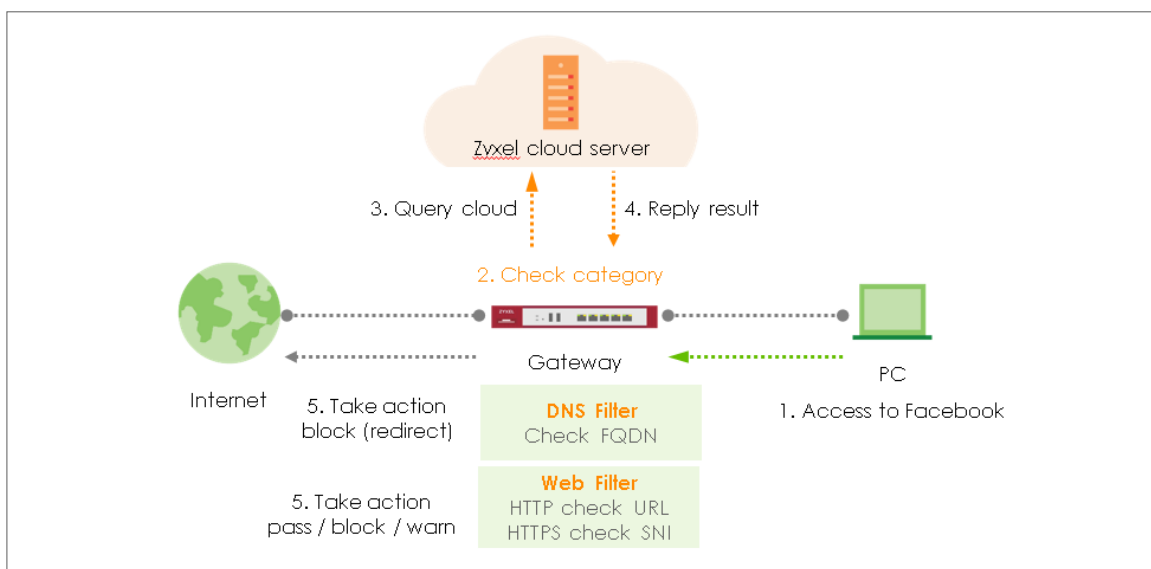
Search insights


#	Username	Assigned IP	Remote IP	Up Time	Reauth/Lease Time	Inbound (Bytes)	Outbound (Bytes)
1	vpntest	192.168.4.2	10.214.48.46	0:00:10	23:59:50 / 23:59:50	13014 bytes	7426 bytes

Chapter 2- Security Service

How to Block HTTPS Websites Using Content Filtering and SSL Inspection

This is an example of using a FLEX Content Filtering, SSL Inspection and Security Policy to block access to malicious or not business-related websites.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up Content Filter

Go to Security Service > Content Filtering. Click Add to create a content filtering profile in Profile Management.

Profile Management

+ Add  Edit  Remove  Reference

Search insights  

<input type="checkbox"/>	Name	Description	Reference
<input type="checkbox"/>	BPP		0
<input type="checkbox"/>	CIP		0

Type profile name and enable log for block action in General Settings.

General Settings

Name

Description

Action

Log

Log allowed traffic ☐

SSL V3 or previous version Connection Drop ☒

Drop Log

Tick Streaming Media category in Managed Categories, and click Apply.

<input type="checkbox"/> Shareware Freeware	<input type="checkbox"/> Social Networking	<input type="checkbox"/> Software Hardware
<input type="checkbox"/> Sports	<input type="checkbox"/> Stock Trading	<input checked="" type="checkbox"/> Streaming Media
<input type="checkbox"/> Technical Business Forums	<input type="checkbox"/> Technical Information	<input type="checkbox"/> Text Spoken Only
<input type="checkbox"/> Text Translators	<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel
<input type="checkbox"/> Usenet News	<input type="checkbox"/> Violence	<input type="checkbox"/> Visual Search Engine

Some changes were made
What do you want to do then?

Set Up SSL Inspection

In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



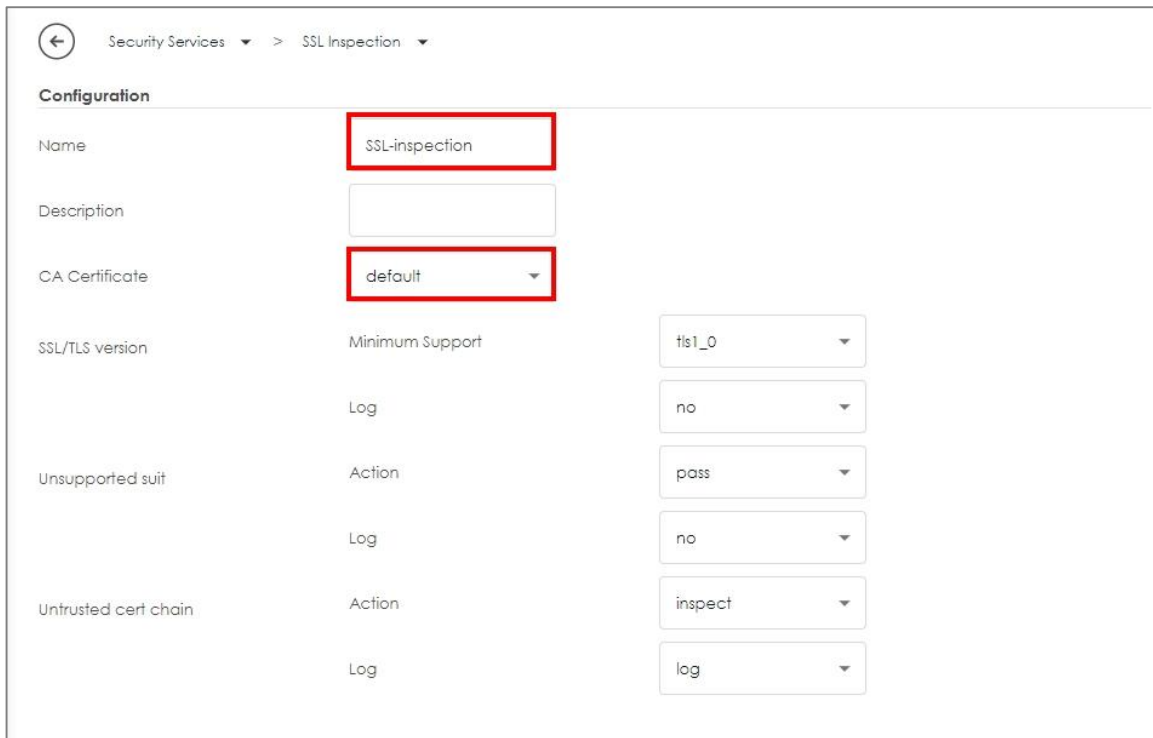
Profile Management

+ Add Edit Remove Reference

Search insights

Name	Description	CA Certificate	Reference
------	-------------	----------------	-----------

Type profile Name, and select the CA Certificate to be the certificate used in this profile. Leave other actions as default settings.



Security Services > SSL Inspection

Configuration

Name: SSL-inspection

Description:

CA Certificate: default

SSL/TLS version: Minimum Support: tls1_0

Log: no

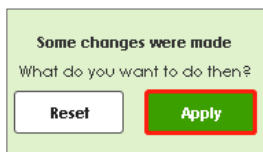
Unsupported suit: Action: pass

Log: no

Untrusted cert chain: Action: inspect

Log: log

Click Apply to add SSL Inspection profile.



Some changes were made

What do you want to do then?

Reset Apply

Set Up the Security Policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Select Content Filtering, and SSL Inspection. Click Apply to save.

Profile			
Application Patrol	none	Log	by profile
Content Filter	Block_Youtube	Log	by profile
SSL Inspection	SSL-inspection	Log	by profile

Export Certificate from FLEX and Import it to Windows

When SSL inspection is enabled and an access website does not trust the FLEX certificate, the browser will display a warning page of security certificate problems.

Go to System > Certificate > My Certificates to export default certificate from FLEX.

System > Certificate > My Certificates

My Certificates Trusted Certificates

PKI Storage Space

Usage 0 %

+ Add Edit Remove Reference Import **Export**

Search insights

✓	Name	Type	Subject	Export	Valid From	Valid To	Refer...
✓	default	SELF	CN=USG_FLEX_200HP_DB...	CN=USG_FLEX_200HP_DBE...	May 29 03:43:22 ...	May 26 03:43:22 ...	2

Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.

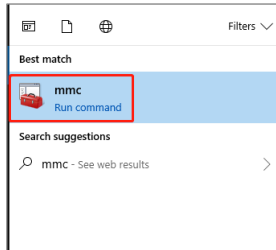
Export Certificate

Password

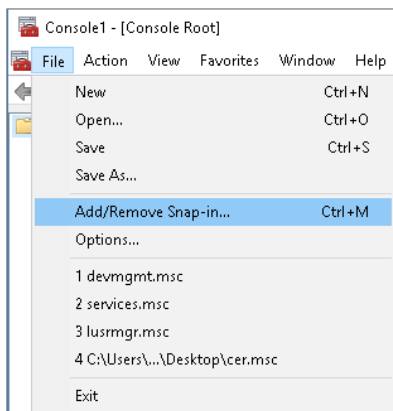
Leave the password field blank to export certificate only or fill in password to export certificate with private key.

Export Certificate

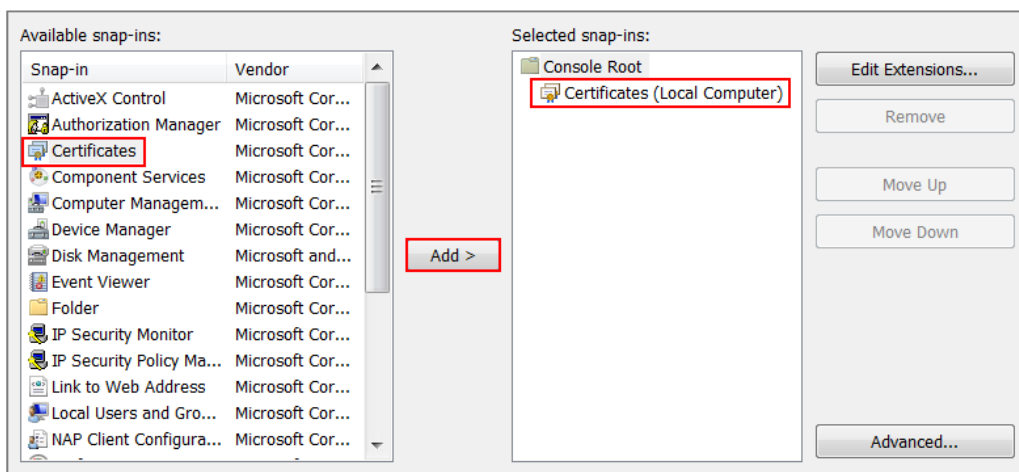
In Windows Start Menu > Search Box, type MMC and press Enter.



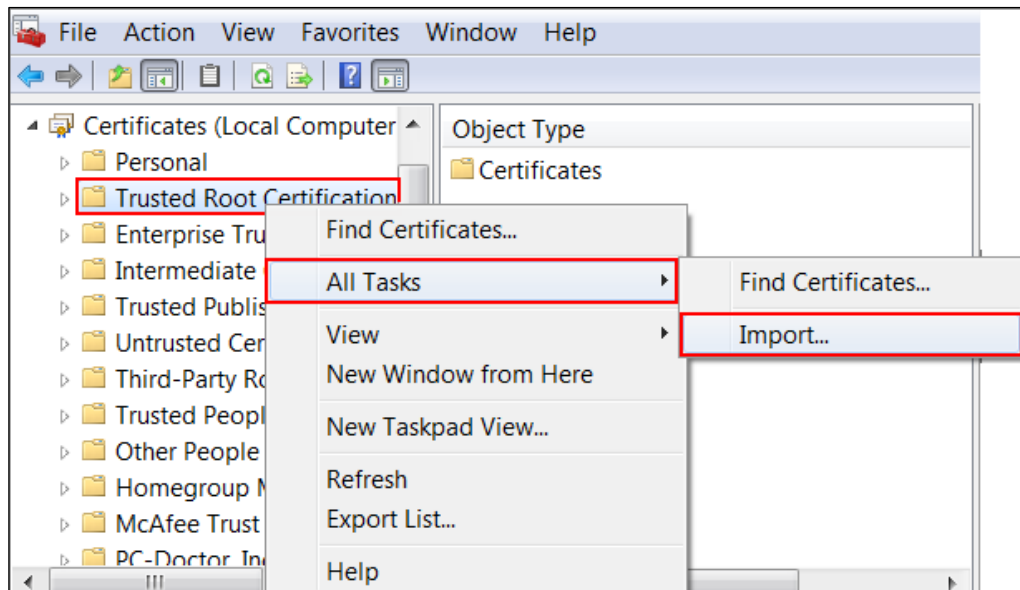
In the mmc console window, click File > Add/Remove Snap-in...



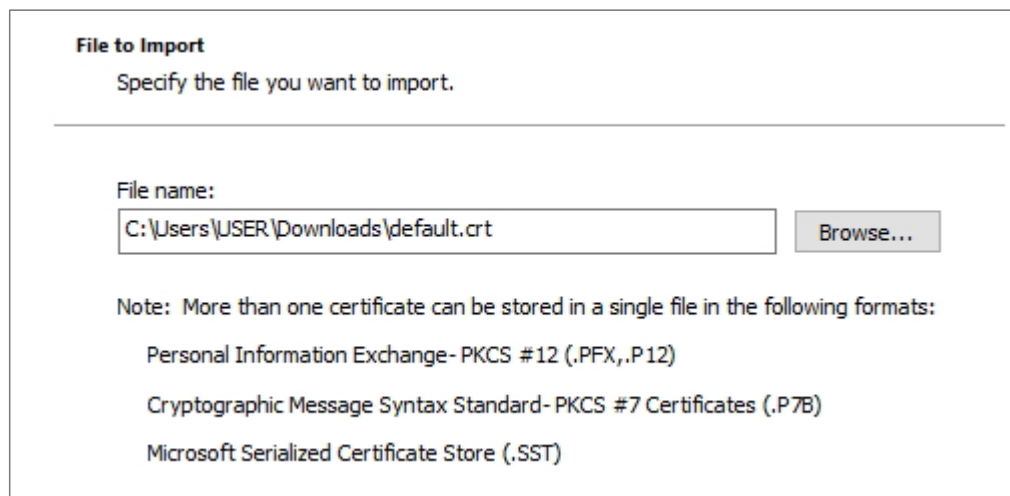
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import...



Click Next. Then, Browse..., and locate the default.crt file you downloaded earlier. Then, click Next.



Select Place all certificates in the following store and then click Browse and find Trusted Root Certification Authorities. Click Next, then click Finish.



The image shows a screenshot of the 'Certificate Import Wizard' window. The title bar includes a back arrow and the text 'Certificate Import Wizard'. The main content area is titled 'Certificate Store' and contains the text: 'Certificate stores are system areas where certificates are kept.' Below this, a horizontal line separates the header from the main options. The text 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' is followed by two radio button options. The first option is 'Automatically select the certificate store based on the type of certificate'. The second option, 'Place all certificates in the following store:', is selected and highlighted with a red rectangular box. Below the selected option, there is a text box labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities'. To the right of this text box is a 'Browse...' button.

← Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

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

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

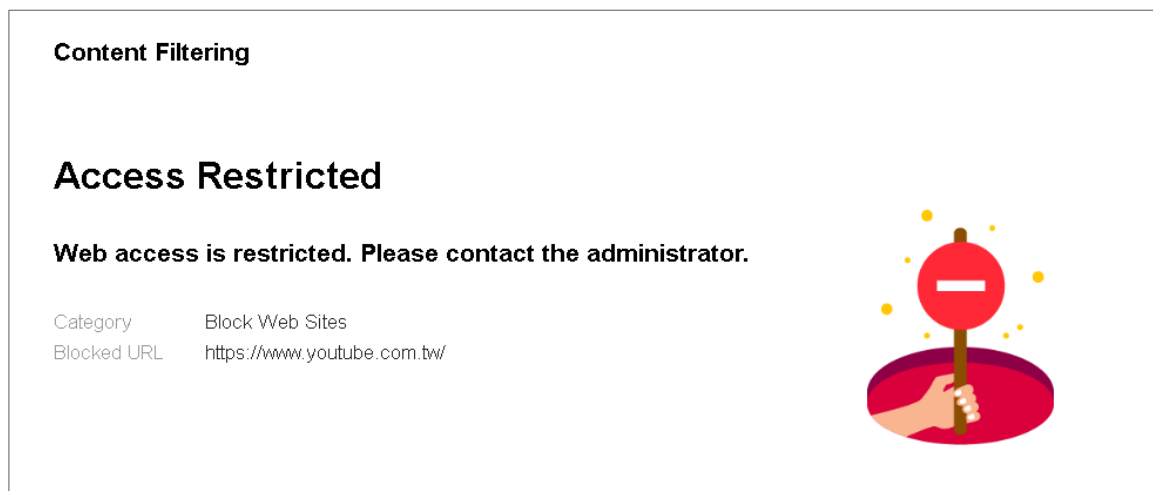
☒ Place all certificates in the following store:

Certificate store:
Trusted Root Certification Authorities

Browse...

Test the Result

Using Web Browser to access the YouTube. The gateway will redirect you to a blocked page.



Go to Log & Report > Log/Events and select Content Filtering to check the logs.

Log & Report

Log / Events

Category

Content Filter

Filter

Refresh

Clear Log

you

#	Time	Category	Message	Source	Destination	Note
71	2023-05-29 19:11:15	content-filter	www.youtube.com:Streaming Media, Rule_name:LAN_Outgoing, SSN (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
103	2023-05-29 19:11:02	content-filter	youtube-uli.google.com: Internet Services, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
154	2023-05-29 19:10:42	content-filter	www.youtube.com:Streaming Media, Rule_name:LAN_Outgoing, SSN (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
258	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS REDIRECT
259	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK
260	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK

Rows per page: 50

1-6 of 6

Go to Security Statistics > SSL Inspection > Summary. Traffic is inspected by SSL inspection.

Security Statistics > SSL Inspection > Summary

Summary Certificate Cache List

General Settings

Refresh Flush Data

Status

Maximum Concurrent Sessions 1000
Concurrent Sessions 238

Summary

SSL Sessions	Total	3553
	Inspected	3430 (96.54%)
	Decrypted	48.24 Mbytes
	Encrypted	48.05 Mbytes
	Blocked	0
	Passed	123

Go to Security Statistics > Content Filter to check summary of all events.

Security Statistics > Content Filter

Last 24 Hours Summary
Click the pie chart to switch to the item events

Top entry by Blocked Category

Refresh Flush Data

Blocked Category HB Count
Streaming Media 18 (100%)

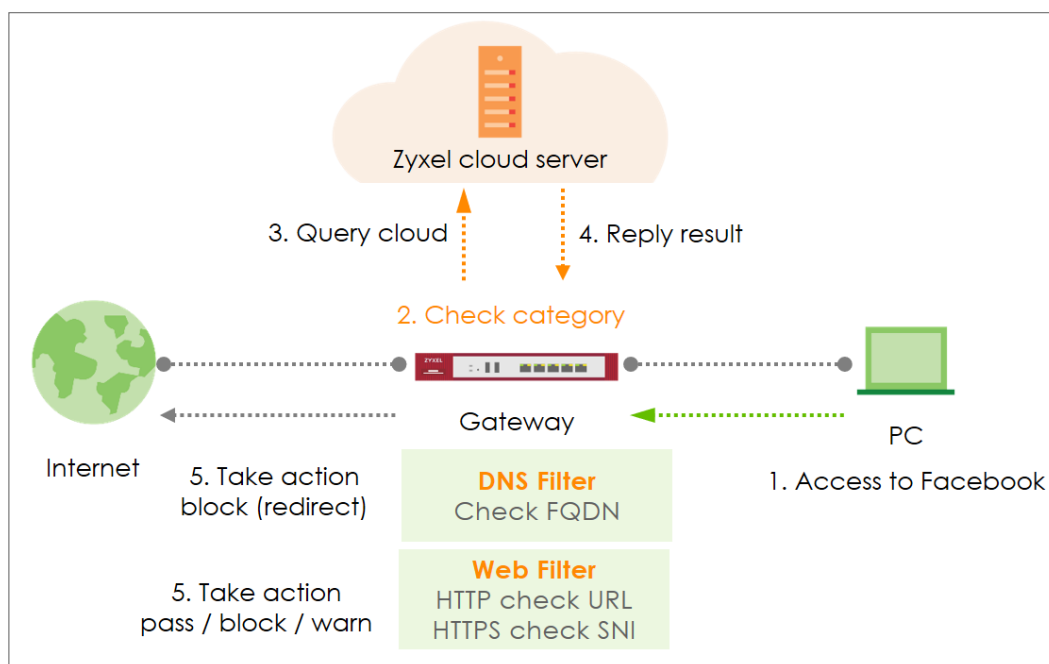
Content Filter Events


Time	Action	URL/Domain	Profile	Category	Source IP	Destination IP
2023-05-29 18:25:10	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87
2023-05-29 18:25:09	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87
2023-05-29 18:25:08	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87

How to Configure Content Filter with HTTPs Domain Filter

The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service. The filtering feature is based on over 100 categories that is built in USG Flex H such as pornography, gambling, hacking, etc.

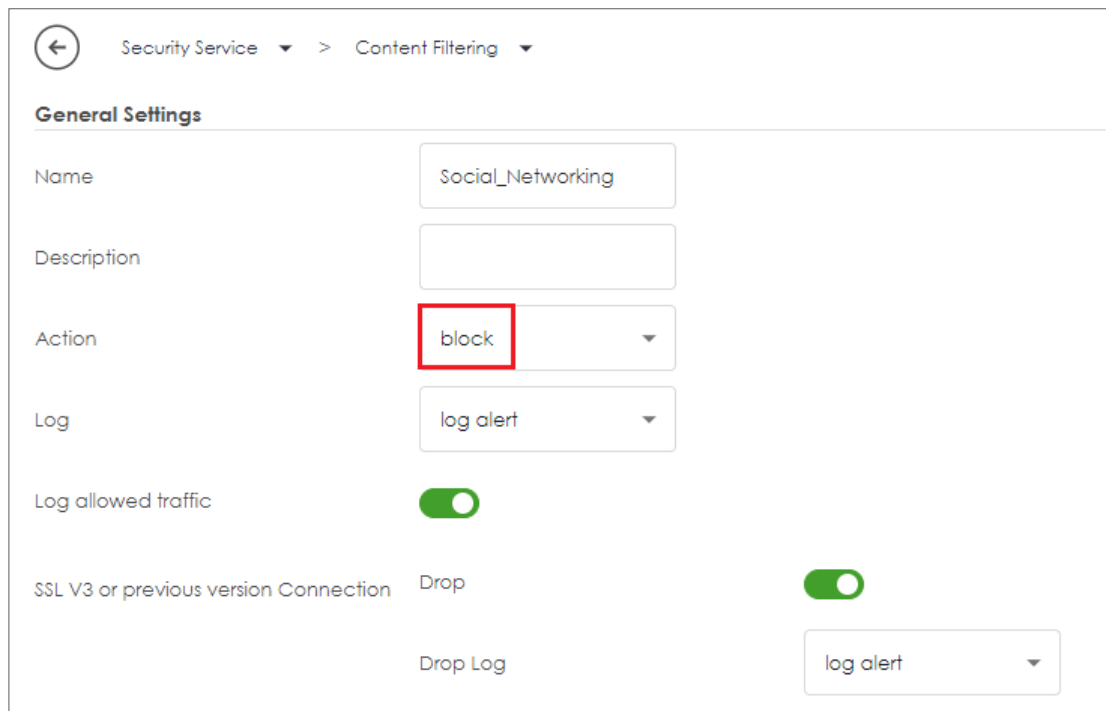
When the user makes an HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then the cloud database, then take action when it matches the block category in the Content Filter profile.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Content Filter

Go to **Security Service > Content Filtering > Profile Management > Add a Content Filter profile**. Configure a **Name** for you to identify the **Content Filter profile** such as "Social_Networking". Configure the **Action** to block when the Content Filter detects events.



Security Service > Content Filtering

General Settings

Name: Social_Networking

Description:

Action: block

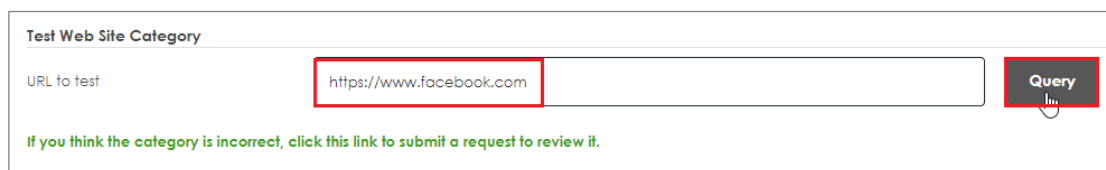
Log: log alert

Log allowed traffic: ☒

SSL V3 or previous version Connection: Drop

Drop Log: log alert

Navigate to **Test Web Site Category** and type URL to test the category and click **Query**.



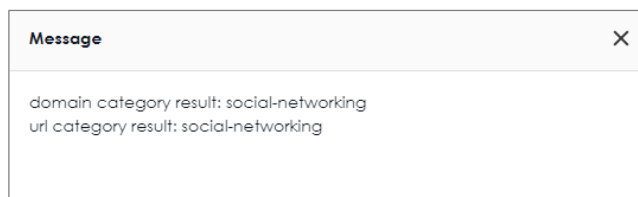
Test Web Site Category

URL to test: https://www.facebook.com

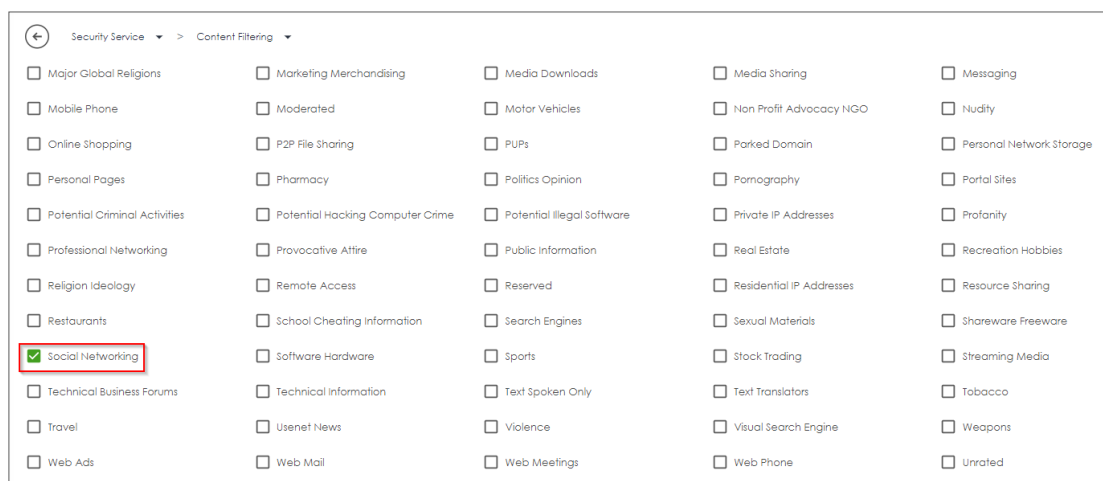
Query

If you think the category is incorrect, click this link to submit a request to review it.

You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



Scroll to the **Managed Categories** section, and select categories in this section to control access to specific types of Internet content.



Set Up the Security Policy

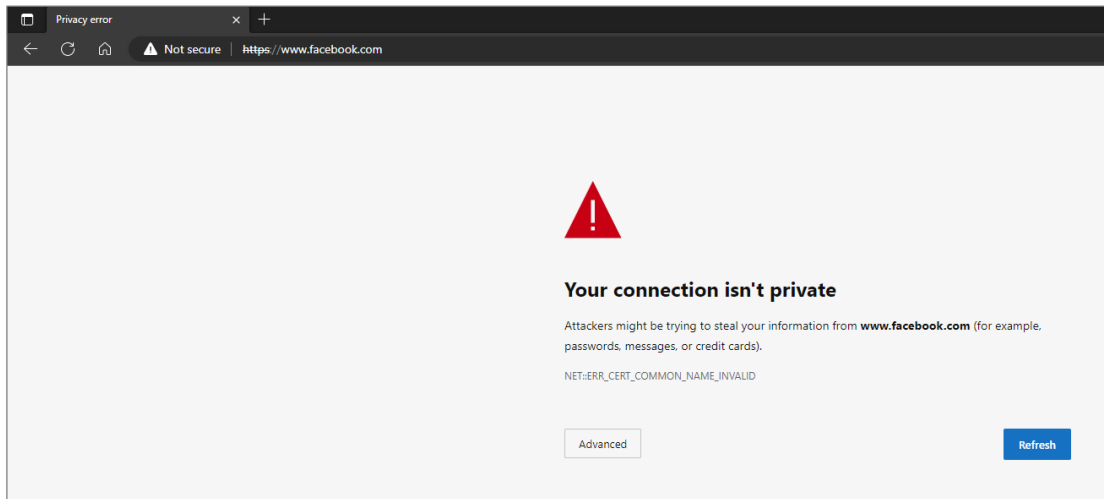
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Social_Networking" on this security policy.

The screenshot displays the ZyXEL Security Policy configuration page. The breadcrumb navigation shows 'Security Policy' > 'Policy Control'. The 'Configuration' section includes a toggle for 'Enable' (turned on), a 'Name' field containing 'Block_Social_Networking', and a 'Description' field. Below these are 'From' (LAN) and 'To' (WAN) dropdowns, each with a green edit icon. Further down are 'Source', 'Destination', 'Service', 'User', and 'Schedule' fields, all set to 'any' or 'none' with green edit icons. The 'Action' dropdown is set to 'allow' and the 'Log' dropdown is set to 'no'. The 'Profile' section at the bottom includes 'Application Patrol' (none), 'Content Filter' (Social_Networking), and 'SSL Inspection' (none). Each profile setting has a 'Log' checkbox and a 'by profile' dropdown menu.

Configuration			
Enable	<input checked="" type="checkbox"/>		
Name	Block_Social_Networking		
Description			
From	LAN		
To	WAN		
Source	any		
Destination	any		
Service	any		
User	any		
Schedule	none		
Action	allow		
Log	no		
Profile			
Application Patrol	none	Log	by profile
Content Filter	Social_Networking	Log	by profile
SSL Inspection	none	Log	by profile

Test Result

Type the URL <http://www.facebook.com/> or <https://www.facebook.com/> onto the browser and cannot browse facebook.

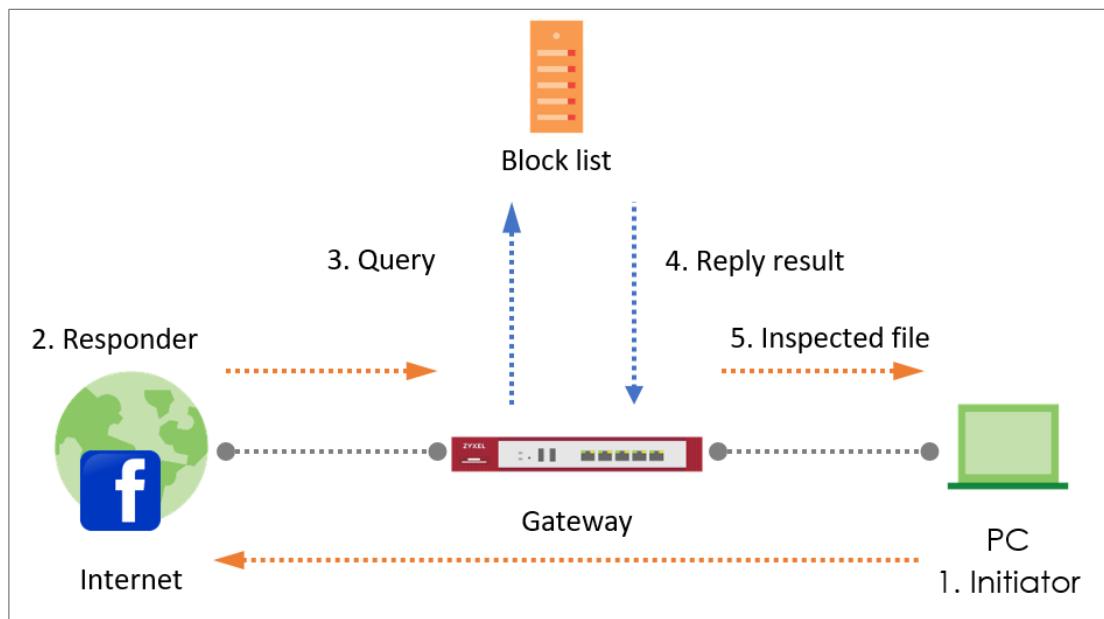



Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

Log & Report > Log / Events						
25	2023-05-22 14:46:31	content-filter	www.facebook.com: Social networking, rule_name: Block_Social_networking	10.214.40.67	172.21.5.1	DNS REDIRECT
26	2023-05-22 14:46:31	content-filter	www.facebook.com: Social networking, rule_name: Block_Social_networking	192.168.168.33	192.168.168.1	DNS REDIRECT

How to Block Facebook Using a Content Filter Block List

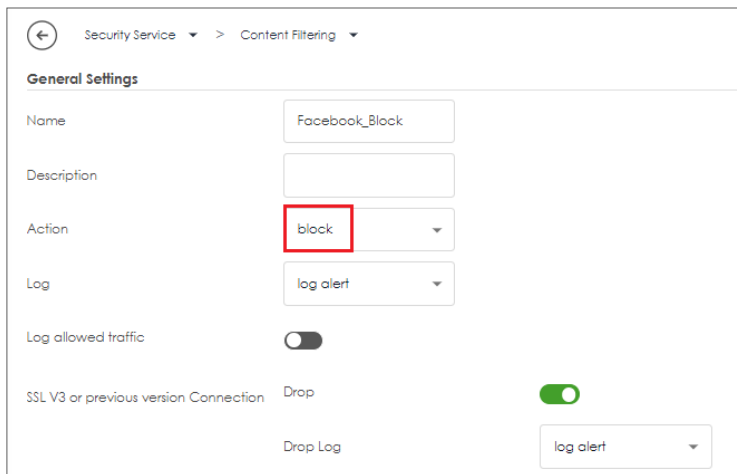
This is an example of using USG Flex H UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Content Filter

In the USG Flex H, go to **Security Service > Content Filtering > Profile Management > Add a Content Filter profile**. Configure a **Name** for you to identify the **Content Filter profile** such as "Facebook_Block". Configure the **Action** to block when the Content Filter detects events.



← Security Service > Content Filtering >

General Settings

Name: Facebook_Block

Description:

Action: **block**

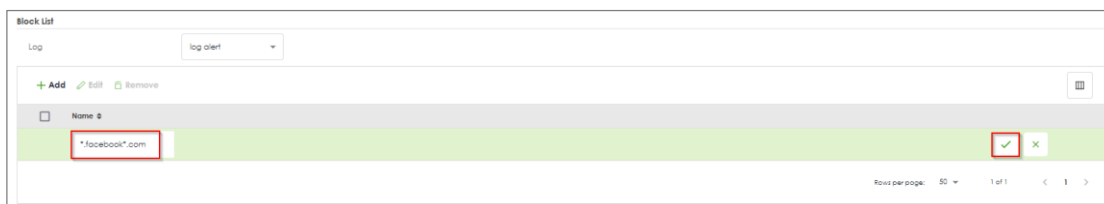
Log: log alert

Log allowed traffic: ☐

SSL V3 or previous version Connection: Drop

Drop Log: log alert

Go to **Block List** and type URL "*.facebook*.com" to add the URL that you want to block.



Block List

Log: log alert

+ Add Edit Remove

Name	URL	Action
	.facebook.com	block

Rows per page: 50 1 of 1 < 1 >

Set Up the Security Policy

Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Facebook_Block" on this security policy.

Security Policy > Policy Control

Configuration

Enable: ☒

Name: Facebook_Block

Description:

From: LAN

To: any (Excluding ZyWALL)

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: allow

Log: no

Profile

Application Patrol: none

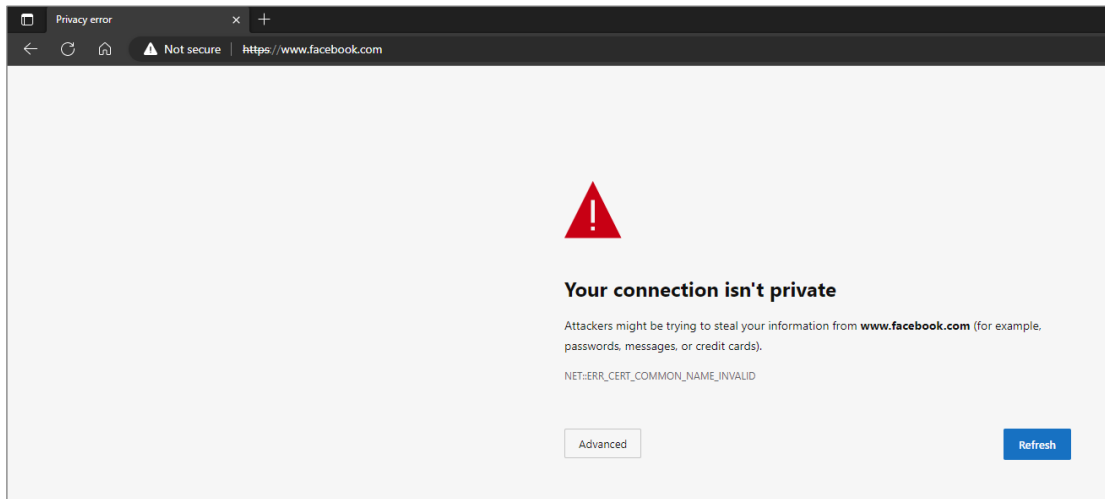
Content Filter: Facebook_Block

SSL Inspection: none

Log: by profile

Test the Result

Type the URL <http://www.facebook.com/> or <https://www.facebook.com/> onto the browser and cannot browse facebook.

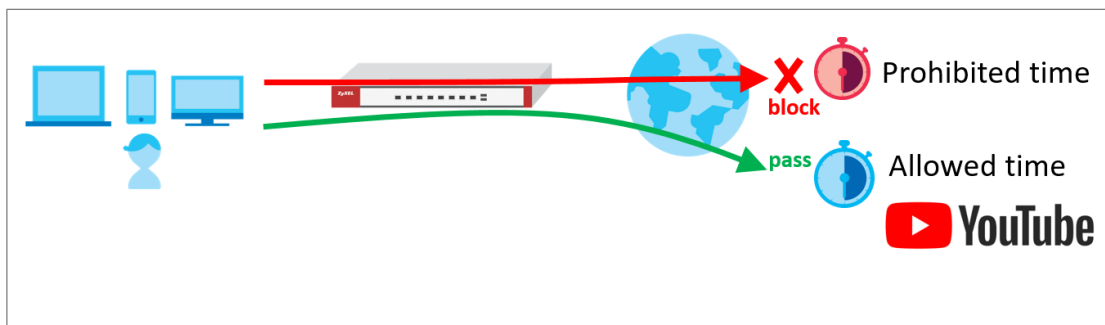



Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

#	Time	Category	Message	Source	Destination	Note
1	2023-05-22 15:36:59	content-filter	www.facebook.com\$Block List, Rule_name:Facebook_Block, \$D\$H (Content Filter)	192.168.168.33	52.23.24.55	WEB BLOCK

How to block YouTube access by Schedule


This is an example of using the USG Flex H to block access YouTube access by schedule. You can use Application Patrol and security policy with schedule settings to make sure that YouTube cannot be accessed in your network at a specific prohibited time. This article will guide you on how to deploy it.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Schedule

Go to **Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day.



Object ▾ > Schedule ▾


Configuration

Name

Description

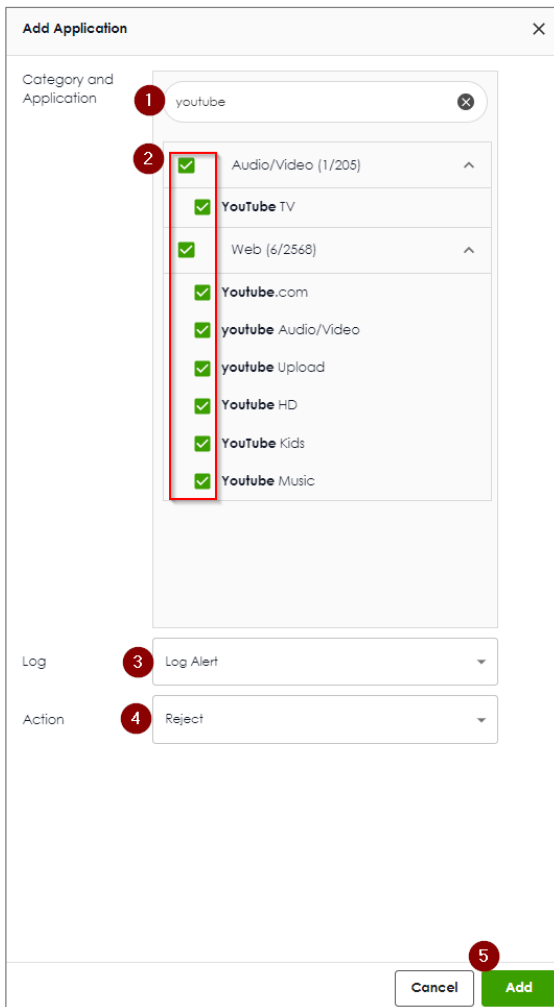
Day Time

Start Time  ▾

Stop Time  ▾

Create the Application Patrol profile

In the USG Flex H, go to **Security Service > App Patrol > General Settings > Application Management**. To add an App Patrol profile, configure the profile name and select "**Search Application**". Then enter the keyword "youtube" to search the key-related results and select all YouTube-related apps and click **Add**.



Add Application

Category and Application

1 youtube

2

- ☒ Audio/Video (1/205) ^
- ☒ YouTube TV
- ☒ Web (6/2568) ^
- ☒ Youtube.com
- ☒ youtube Audio/Video
- ☒ youtube Upload
- ☒ Youtube HD
- ☒ YouTube Kids
- ☒ Youtube Music

Log 3 Log Alert


Action 4 Reject

5

Cancel Add

Set Up the Security Policy

Go to **Object > Service** to add a UDP 443 service object.


Object ▾ > Service ▾

Configuration










Name	<input type="text" value="QUIC_UDP_443"/>	
Description	<input type="text"/>	
IP Protocol	<input type="text" value="UDP"/> ▾	
Starting Port	<input type="text" value="443"/>	(1..65535)
Ending Port	<input type="text" value="443"/>	(1..65535)

Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **service** QUIC_UDP443 and select the **Schedule** that defines when the policy would be applied.

In this example, select "Youtube_Blocked_Time".

← Security Policy > Policy Control >

Configuration

Enable	<input checked="" type="checkbox"/>
Name	Block_QUIC_UDP443
Description	<input type="text"/>
From	LAN 
To	WAN 
Source	LAN1_SUBNET 
Destination	any 
Service	QUIC_UDP_443 
User	any 
Schedule	Youtube_Block_Time 
Action	deny 
Log	log alert 

Add another security policy to block YouTube by schedule. To configure a **Name** and the **From, To** traffic direction. Select the **Schedule** that defines when the policy would be applied. Finally, to scroll down the **Profile**, check **Application Patrol** and select a profile from the list box. In this example, **Schedule**: Youtube_Block_Time; **Application Patrol**: Youtube.

← Security Policy > Policy Control >

Configuration

Enable	<input checked="" type="checkbox"/>		
Name	Block_Youtube		
Description	<input type="text"/>		
From	LAN		
To	WAN		
Source	LAN1_SUBNET		
Destination	any		
Service	any		
User	any		
Schedule	Youtube_Block_Time		
Action	allow	▼	
Log	log alert	▼	

Profile

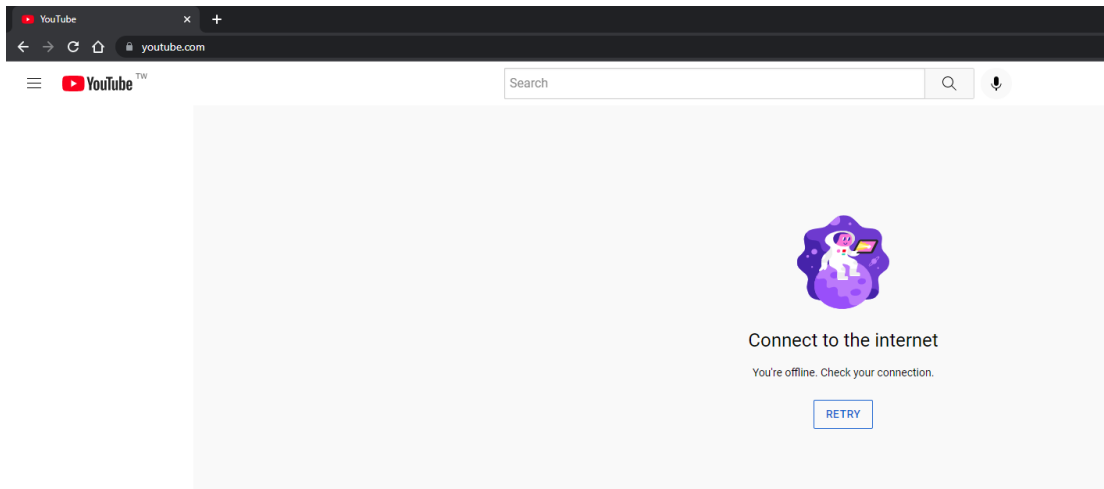
Application Patrol	Youtube	▼	Log	by profile	▼
Content Filter	none	▼	Log	by profile	▼
SSL Inspection	none	▼	Log	by profile	▼

Then go back to the security policy page and move the security priority of block UDP 443 is higher than block YouTube by schedule.

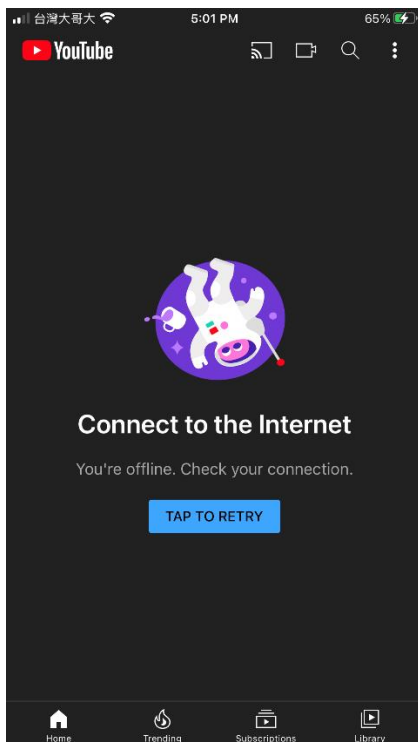
<input type="checkbox"/>	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
<input type="checkbox"/>		1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
<input type="checkbox"/>		2	Block_YouTube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log-alert	

Test the Result

Type the URL <http://www.youtube.com/> or <https://www.youtube.com/> onto the browser and cannot browse YouTube.



Open the YouTube APP on the phone and cannot access to YouTube.




Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

#	Time	Category	Message	Source	Destination	Note
3	2023-05-21 21:35:26	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT
5	2023-05-21 21:35:26	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT
18	2023-05-21 21:35:16	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
20	2023-05-21 21:35:16	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
25	2023-05-21 21:35:10	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	142.251.43.14	ACCESS REJECT
27	2023-05-21 21:35:10	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	142.251.43.14	ACCESS REJECT
30	2023-05-21 21:35:04	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
34	2023-05-21 21:35:01	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
38	2023-05-21 21:34:54	app-patrol	Rule_name\$lock_Youtube App(Web)youtube \$D:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT

How to Control Access to Google Drive

This is an example of using a FLEX UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Create app patrol profile

Go to Security Service > App patrol > Profile management, and click Add to create profile



App Patrol

General Settings

Collect Statistics: Enable ☒

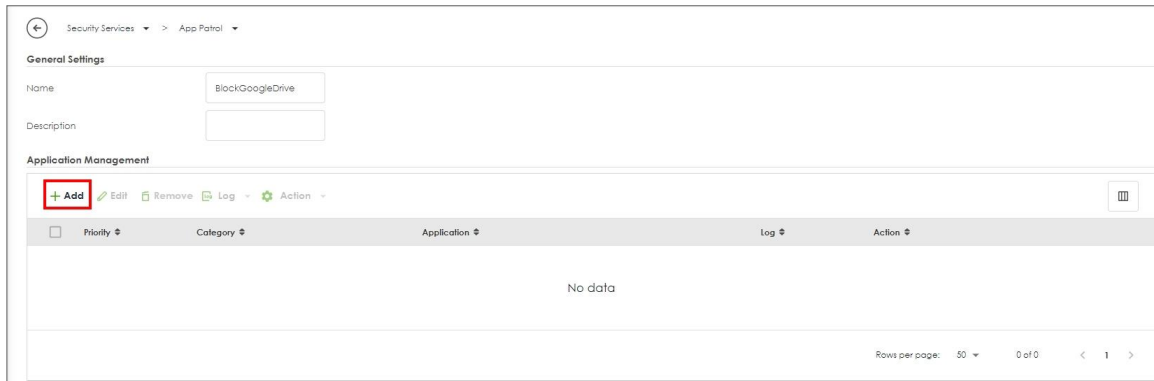
Analyze All Traffic: ☒ 1

Profile Management

+ Add Edit Remove Reference

Name	Description	Reference
default_profile		1

Click add to add application in this profile.



Security Services > App Patrol

General Settings

Name: BlockGoogleDrive

Description:

Application Management

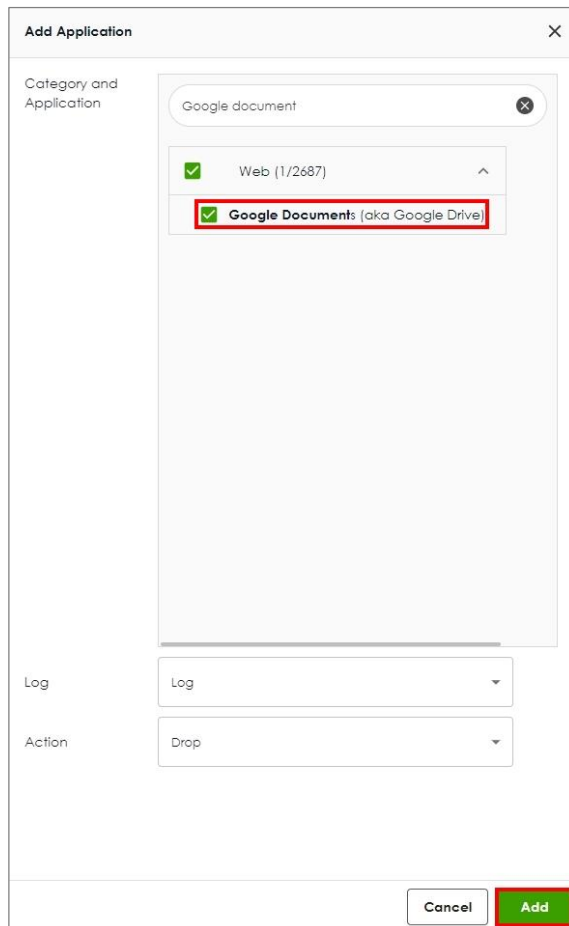
+ Add Edit Remove Log Action

Priority	Category	Application	Log	Action
No data				

Rows per page: 50 0 of 0 < 1 >

Search **Google Documents(aka Google Drive)**, and select this Application.

Action set to Drop, and click Add.



Add Application

Category and Application

Google document

Web (1/2687)

Google Documents (aka Google Drive)

Log

Log

Action

Drop

Cancel Add

Set Up SSL Inspection on the FLEX

In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



Profile Management

+ Add Edit Remove Reference

Search insights

Name	Description	CA Certificate	Reference

Type profile Name, and select the CA Certificate to be the certificate used in this profile.
Leave other actions as default settings.

← Security Services > SSL Inspection

Configuration

Name	SSL-inspection		
Description			
CA Certificate	default		
SSL/TLS version	Minimum Support	f1s1_0	
	Log	no	
Unsupported suit	Action	pass	
	Log	no	
Untrusted cert chain	Action	inspect	
	Log	log	

Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Select Application Patrol, and SSL Inspection.

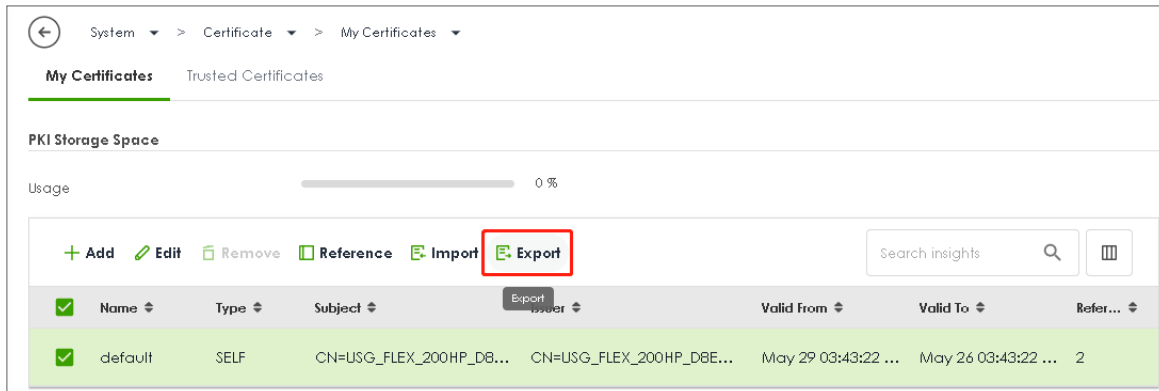
Profile

Application Patrol	BlockGoogleDrive	Log	by profile
Content Filter	none	Log	by profile
SSL Inspection	SSL-inspection	Log	by profile

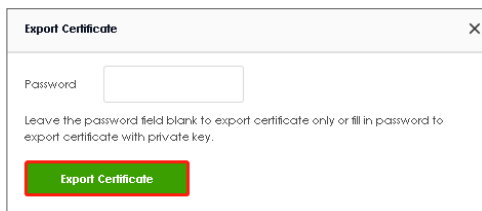
Export Certificate from FLEX and import to Lan hosts

When SSL inspection is enabled and an access website does not trust the FLEX certificate, the browser will display a warning page of security certificate problems.

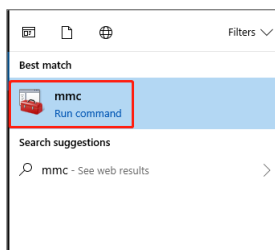
Go to System > Certificate > My Certificates to export default certificate from FLEX.



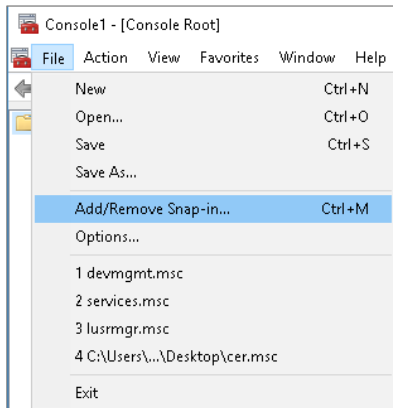
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



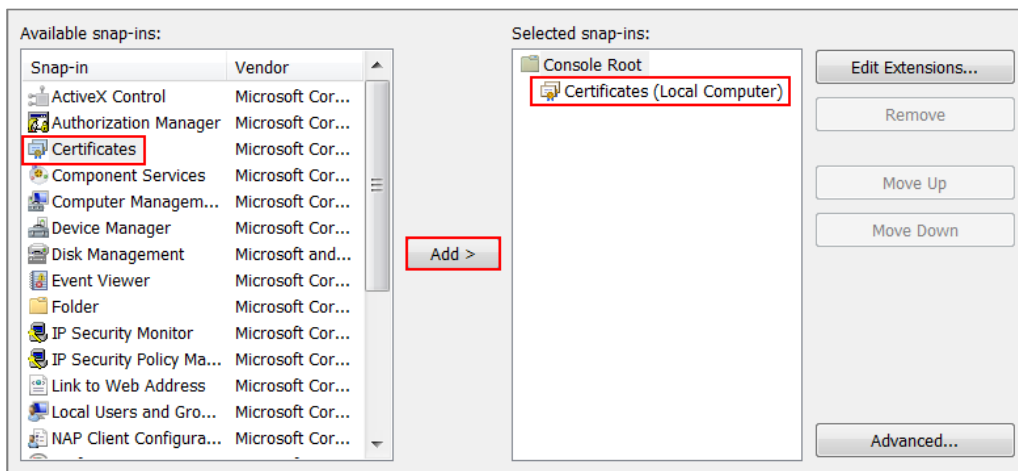
In Windows Start Menu > Search Box, type MMC and press Enter.



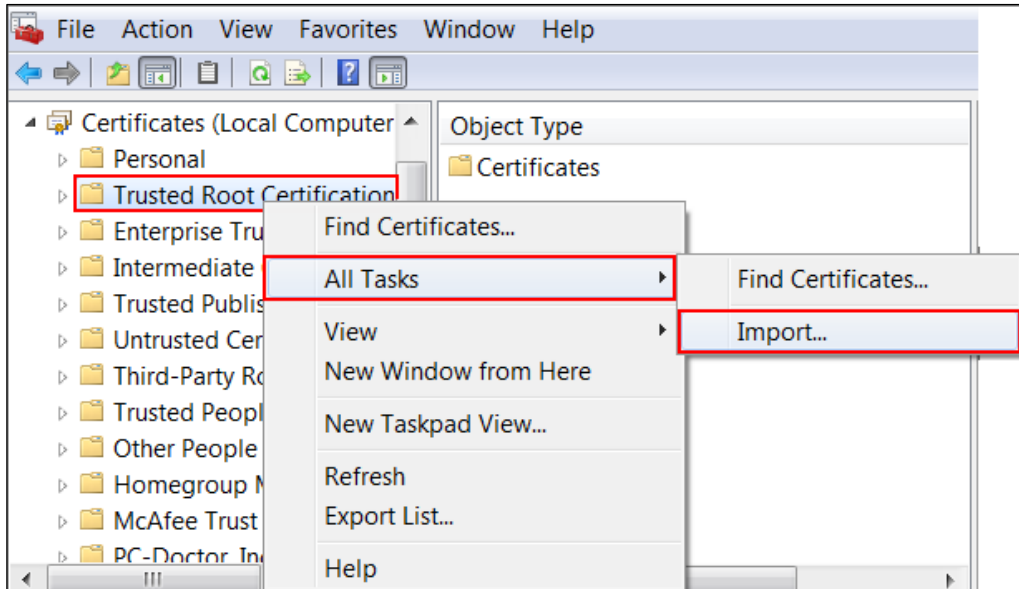
In the mmc console window, click File > Add/Remove Snap-in...



In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import...



Click Next. Then, Browse..., and locate the default.crt file you downloaded earlier. Then, click Next.

File to Import

Specify the file you want to import.

File name:

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

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Select Place all certificates in the following store and then click Browse and find Trusted Root Certification Authorities. Click Next, then click Finish.



Certificate Store

Certificate stores are system areas where certificates are kept.

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

☐ Automatically select the certificate store based on the type of certificate
☒ Place all certificates in the following store:

Certificate store:

Test the Result

Access to Google drive from Lan host to verify if it is blocked by firewall Application patrol.

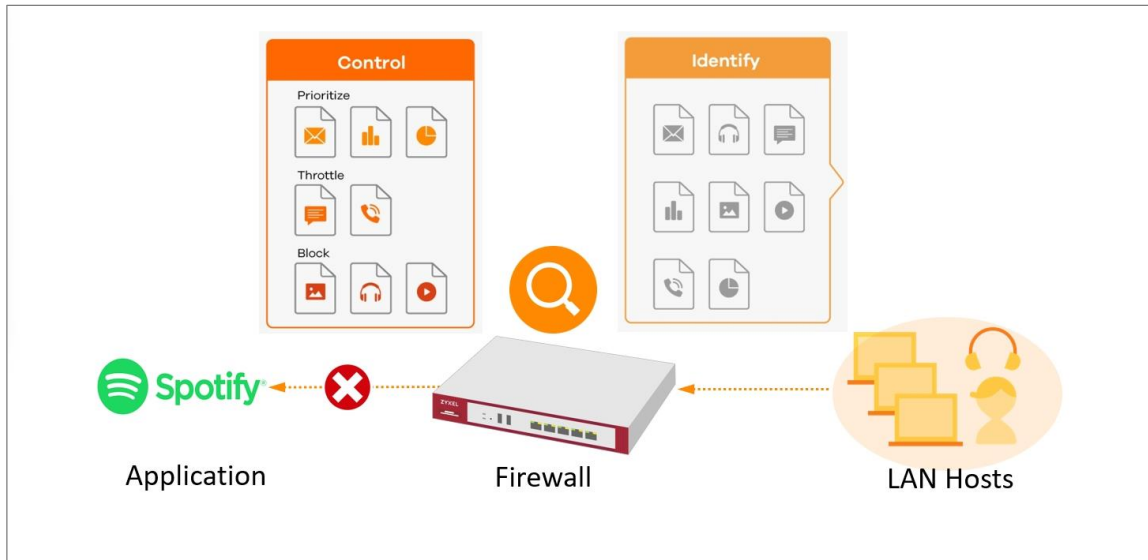
Go to Log & Report > Log/Events and select Application Patrol to check the logs.




#	Time	Category	Message	Source	Destination	Note
5	2023-09-15 14:45:53	Application Patrol	Rule_name:LAN_Outgoing App:[Web]google_docs SID: 97583104	192.168.168.33	142.251.43.14	ACCESS BLOCK

How to Block the Spotify Music Streaming Service

This is an example of using a FLEX UTM App Patrol Profile in a Security Policy to block the Spotify Music Streaming Service. You can use Application Patrol and Policy Control to ensure that the Spotify Music Streaming Service cannot be accessed on the LAN.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Create a App Patrol profile

Go to Security Service > App patrol > Profile management, and click Add to create profile.



App Patrol

General Settings

Collect Statistics: Enable ☒

Analyze All Traffic: ☒ 1

Profile Management

+ Add Edit Remove Reference

Name	Description	Reference
default_profile		1

Click add to add application in this profile.



General Settings

Name: APP9211

Description:

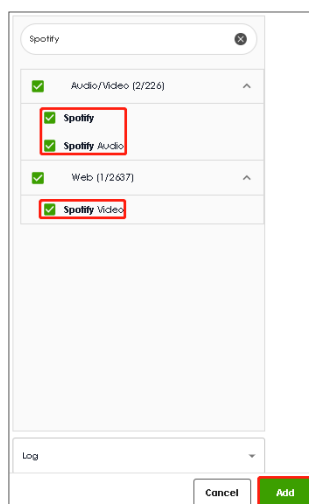
Application Management

+ Add Edit Remove Log Action

Add	Priority	Category	Application	Log	Action
No data					

Rows per page: 50 0 of 0 < 1 >

Search Spotify, and select this Application. Action set to Drop, and click Add.



Spotify

Audio/Video (2/226)

- ☒ Spotify
- ☒ Spotify Audio

Web (1/2637)

- ☒ Spotify Video

Log

Cancel Add

Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Apply Application Patrol profile to Security policy.

Profile			
Application Patrol	APP9211	Log	by profile
Content Filter	none	Log	by profile
SSL Inspection	none	Log	by profile

Test the Result

Access to Spotify from Lan host to verify if it is blocked by firewall Application patrol.

Go to Log & Report > Log/Events and select Application Patrol to check the logs.

Log & Report

>

Log / Events

Category

Application Patrol

Filter

Refresh

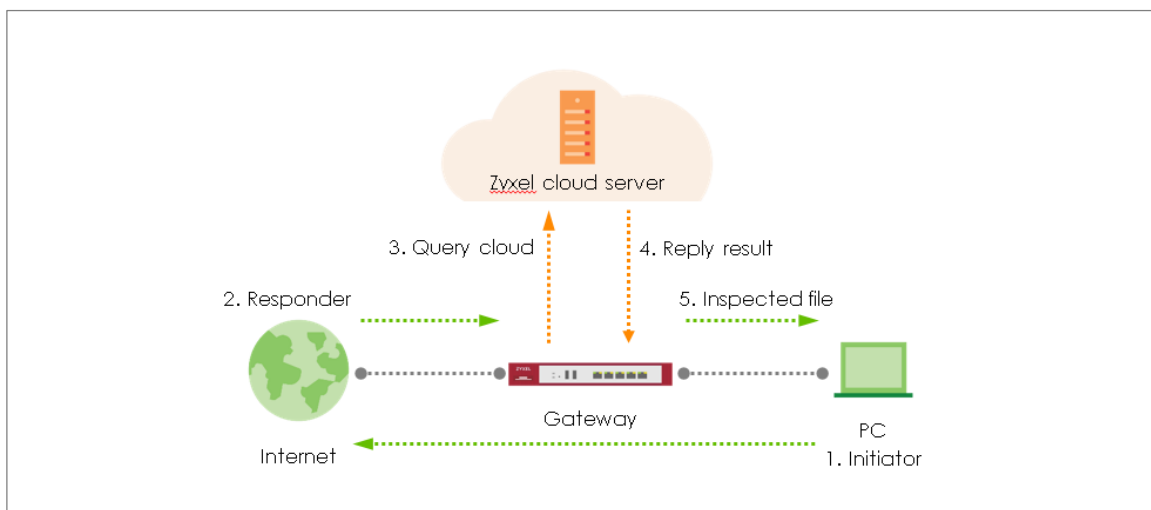
Clear Log

Search insights

#	Time	Category	Message	Source	Destination	Note
6	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
7	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
8	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
9	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
17	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
18	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK
19	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.1.68.34	35.186.224.25	ACCESS BLOCK

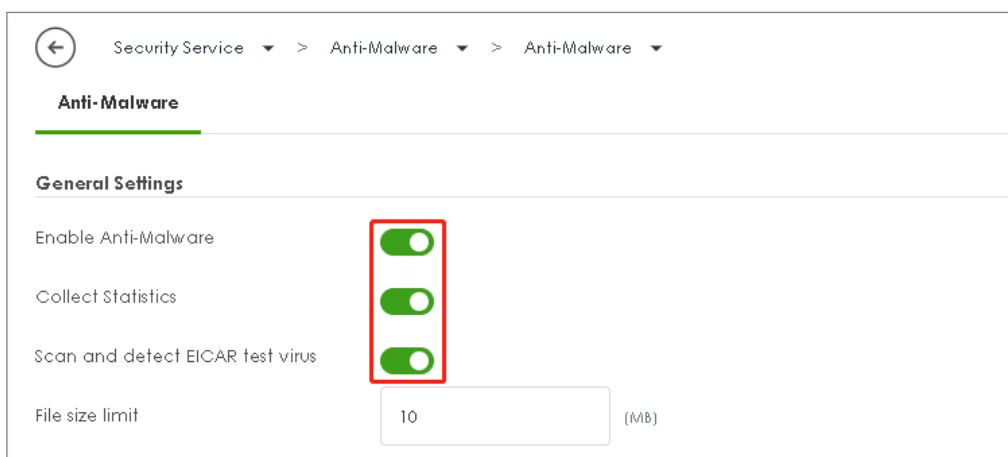
How does Anti-Malware Work

There are many viruses exist on the internet and it may be auto-downloaded on unexpected situation when you surfing between websites. The Anti-Malware is a good choose to protecting your computer to downloads unsafe application or files.



Enable Anti-Malware function to protecting your traffic

Go to Security Service > Anti-Malware. Turn on this feature. Select Collect Statistics and Scan and detect EICAR test virus.



Security Service > Anti-Malware > Anti-Malware

Anti-Malware

General Settings

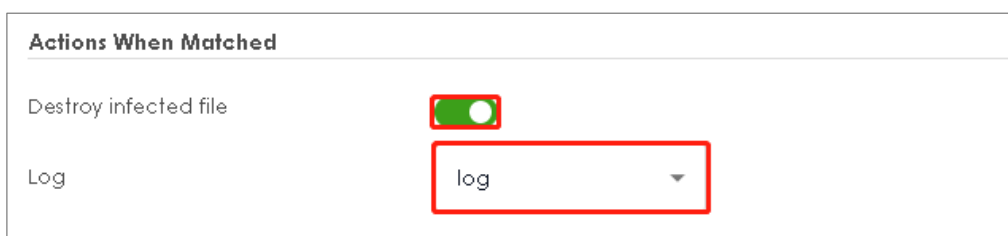
Enable Anti-Malware ☒

Collect Statistics ☒

Scan and detect EICAR test virus ☒

File size limit (MB)

Select Destroy infected file and log in Actions When Matched



Actions When Matched

Destroy infected file ☒

Log

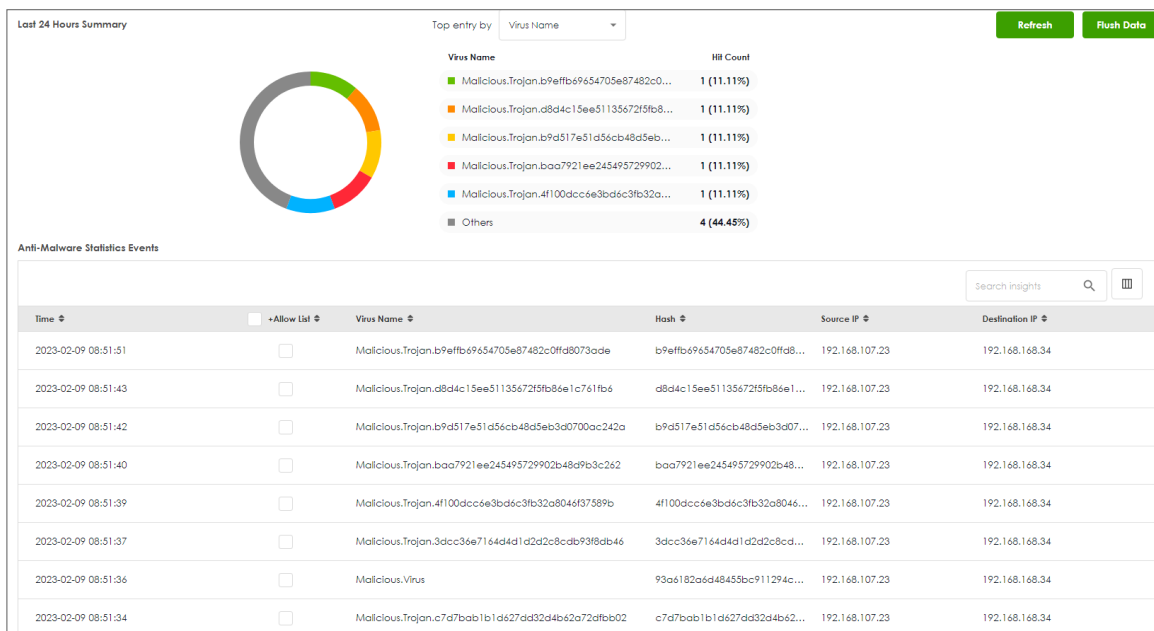
Test the Result

Download EIACR file from a LAN host to verify if Anti-malware works for detection.

Go to Log & Report > Log/Events and select Anti Malware to check the logs.

Category: Anti Malware						
Filter Refresh Clear Log						
<input type="text" value="Search Insights"/>						
#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus Infected SS:N Type:Cloud Query Virus:Malicious.Trojan.44d88612fea8a8f36de82e1278abb02f File:eicar.com.txt Protocol:HTTP md5:44d88612fea8a8f36de82e1278abb02f	89.238.73.97	192.168.168.36	FILE DESTROY

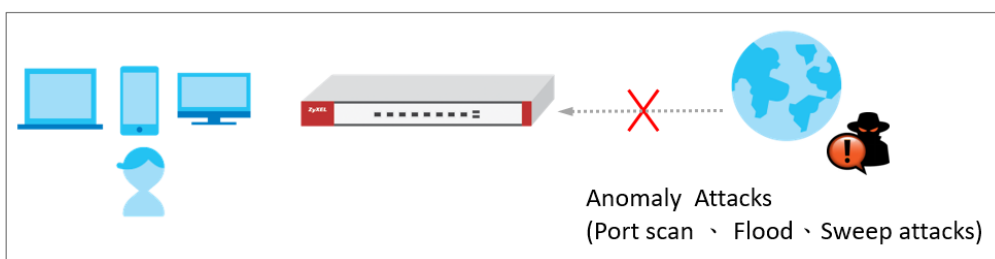
Go to Security Statistics > Anti-Malware to check summary of all events.




How to Detect and Prevent TCP Port Scanning with DoS

Prevention

This is an example of using a USG Flex H DoS Prevention Profile to protect against anomalies based on violations of protocol standards (RFCs Requests for Comments) and abnormal traffic flows such as port scans.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the DoS Prevention

In the USG Flex H, go to **Security Policy > Dos Prevention > Add a profile**. Configure a **Name** for you to identify the **profile** such as "DoS_Prevention". Configure the **Scan Detection** and **Flood Detection** to block when the Dos prevention events were detected.

Security Policy > Dos Prevention

General Settings

Name: DoS_Prevention
Description:

Scan Detection

Sensitivity: Medium
Block Period: 5 (1-3600 seconds)

Active Inactive Log Action

Status	Name	Log	Action
<input type="checkbox"/> Active	(portscan) IP Protocol Scan	log	block
<input type="checkbox"/> Active	(portscan) TCP Portscan	log	block
<input type="checkbox"/> Active	(portscan) UDP Portscan	log	block
<input type="checkbox"/> Active	(Sweep) ICMP Sweep	log	block
<input type="checkbox"/> Active	(Sweep) IP Protocol Sweep	log	block
<input type="checkbox"/> Active	(Sweep) TCP Sweep	log	block
<input type="checkbox"/> Active	(Sweep) UDP Sweep	log	block

Flood Detection

Block Period: 5 (1-3600 seconds)

Edit Active Inactive Log Action

Status	Name	Log	Action	Threshold
<input type="checkbox"/> Active	(flood) ICMP Flood	log	block	1000
<input type="checkbox"/> Inactive	(flood) IP Flood	log	block	1000
<input type="checkbox"/> Active	(flood) TCP Flood	log	block	1000
<input type="checkbox"/> Inactive	(flood) UDP Flood	log	block	1000

Set Up the DoS Prevention Policy

In the USG Flex H, go to **Security Policy > Dos Prevention > DoS Prevention Policy**. Configure a **Name** for you to identify the **policy** such as "DoS_Prevention". Configure the **From** and **Anomaly Profile** to block when the DoS prevention events were detected.

Security Policy > DoS Prevention > DoS Prevention Policy

DoS Prevention Policy
Profile

General Settings

Enable DoS Prevention
☒

Policies

+ Add Edit Remove Active Inactive Move

	Status	Priority	Name	From	Anomaly Profile
<input type="checkbox"/>	Active	1	DoS_Prevention	WAN	DoS_Prevention

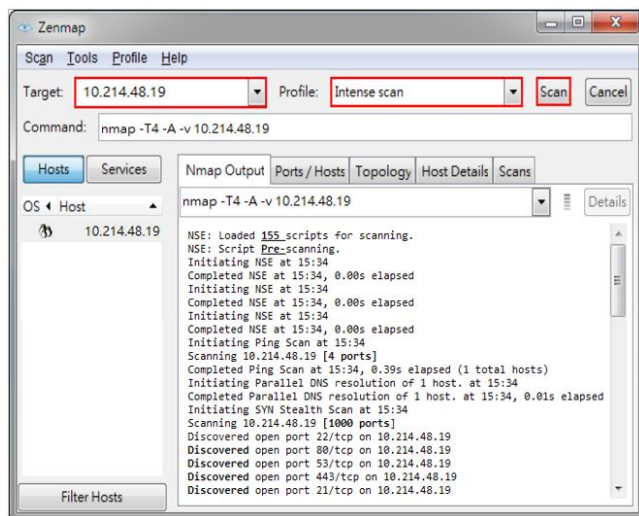
|

Test the Result

Using the port scan tool Nmap or hping3 to scan the wan interface.

For example, using Nmap security scanner for testing the result:

Open the Nmap GUI, set the Target to be the WAN IP of USG Flex H (10.214.48.19 in this example) and set Profile to be Intense Scan and click Scan.



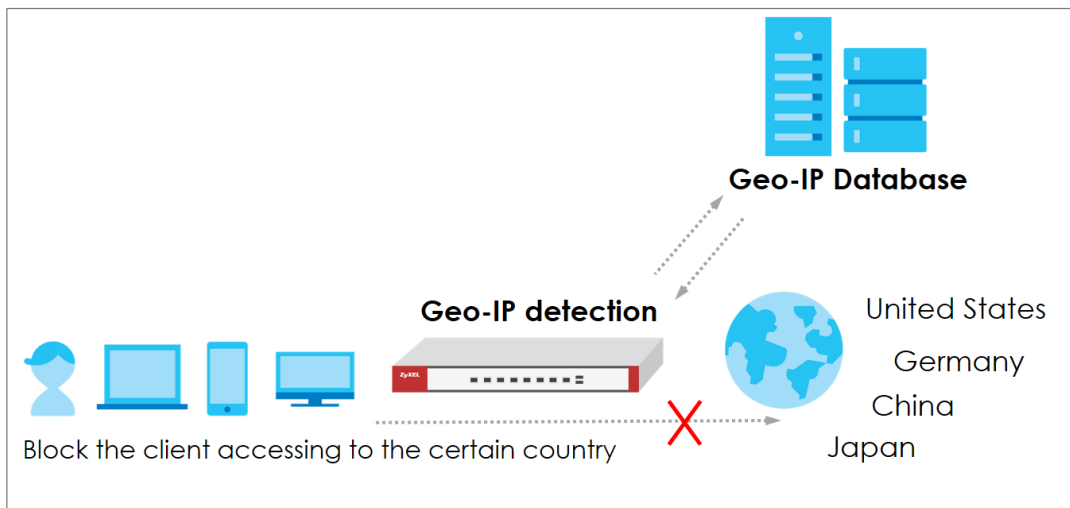
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.


Log & Report > Log / Events						
Category		Filter		Refresh		Clear Log
#	Time	Category	Message	Source	Destination	Note
1	2023-08-21 07:34:50	Dos Prevention	Rule_id1 from WAN to Any, [type:Scan-Detection]tcp portscan ActionDrop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK
2	2023-08-21 07:34:43	Dos Prevention	Rule_id1 from WAN to Any, [type:Scan-Detection]tcp portscan ActionDrop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK
3	2023-08-21 07:34:36	Dos Prevention	Rule_id1 from WAN to Any, [type:Scan-Detection]tcp portscan ActionDrop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK

How to block the client from accessing to certain country using Geo IP?

The Geo IP offers to identify the country-based IP addresses; it allows you to block the client from accessing a certain country based on the security policy.

When the user makes HTTP or HTTPS request, USG Flex H queries the IP address from the cloud database, then takes action when it matches the block country in the security policy.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500H (Firmware Version: uOS 1.10)

Set Up the Address Object with Geo IP

Navigate to **Object > Address > Geo IP > Add geo IP related objects.**

Object > Address

Configuration

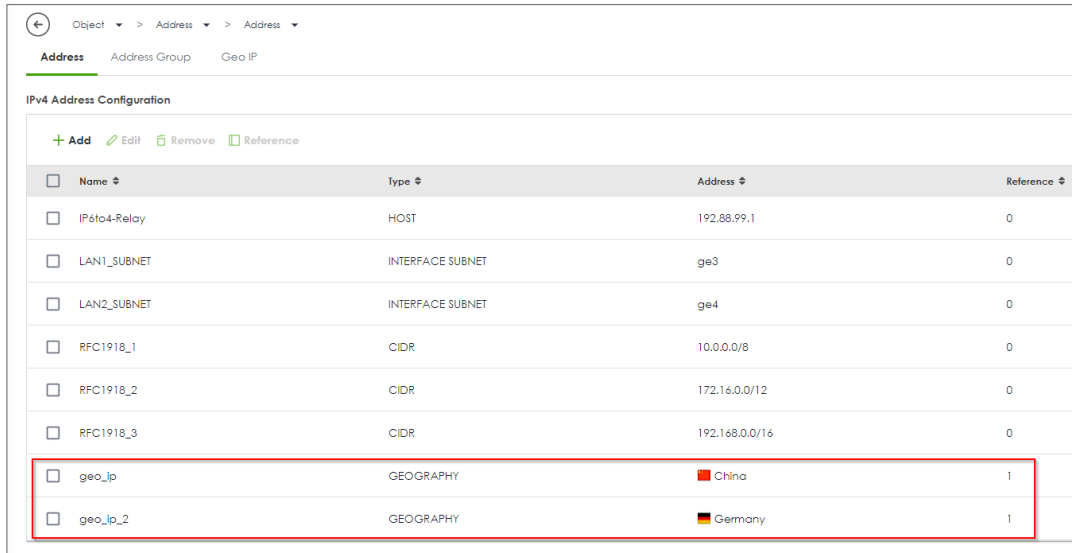
Name	geo_ip
Description	
Address Type	GEOGRAPHY
Region	China

Object > Address

Configuration

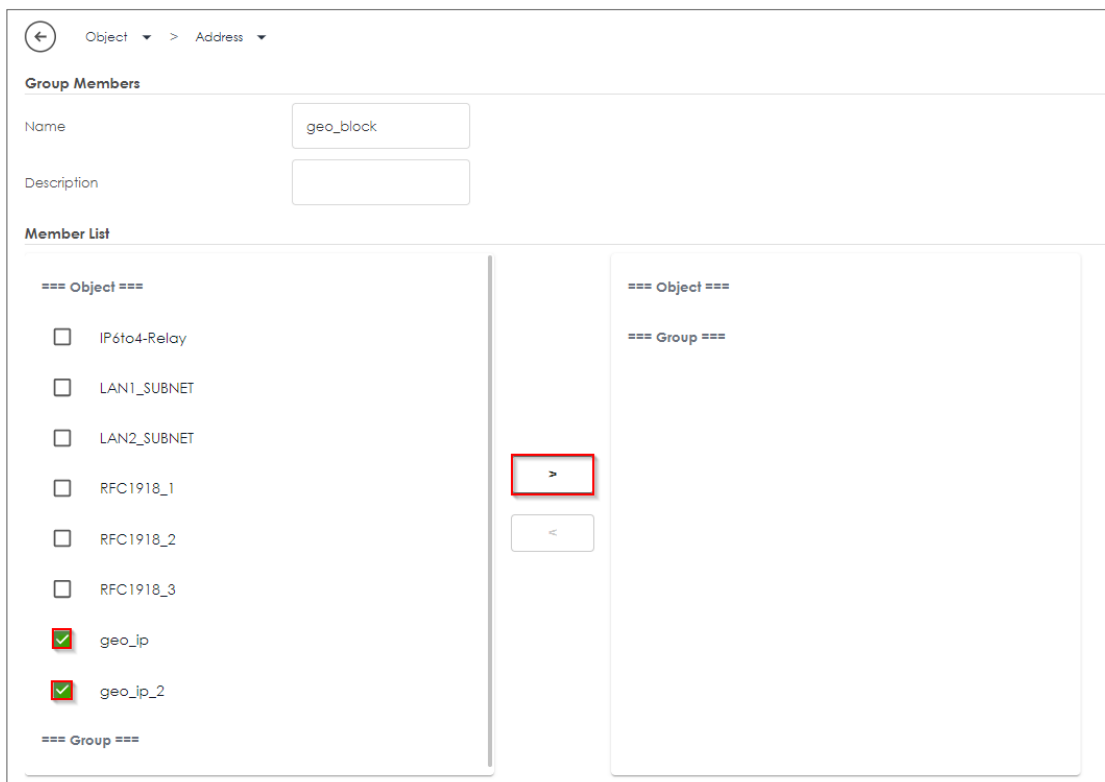
Name	geo_ip_2
Description	
Address Type	GEOGRAPHY
Region	Germany

Navigate to **Object > Address > Address**, you can see the customized GEOGRAPHY address object.



Name	Type	Address	Reference
IP6to4-Relay	HOST	192.88.99.1	0
LAN1_SUBNET	INTERFACE SUBNET	ge3	0
LAN2_SUBNET	INTERFACE SUBNET	ge4	0
RFC1918_1	CIDR	10.0.0.0/8	0
RFC1918_2	CIDR	172.16.0.0/12	0
RFC1918_3	CIDR	192.168.0.0/16	0
geo_ip	GEOGRAPHY	China	1
geo_ip_2	GEOGRAPHY	Germany	1

Go to **Object > Address > Address Group > Add Address Group Rule**, add all customized GEOGRAPHY addresses into the same **Member** object.



Group Members

Name:

Description:

Member List

=== Object ===

- ☐ IP6to4-Relay
- ☐ LAN1_SUBNET
- ☐ LAN2_SUBNET
- ☐ RFC1918_1
- ☐ RFC1918_2
- ☐ RFC1918_3
- ☒ geo_ip
- ☒ geo_ip_2

=== Group ===

=== Object ===

=== Group ===

>










<

Set Up the Security Policy

Go to **Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set deny Geo IP traffic from LAN to WAN (geo_block_policy in this example).

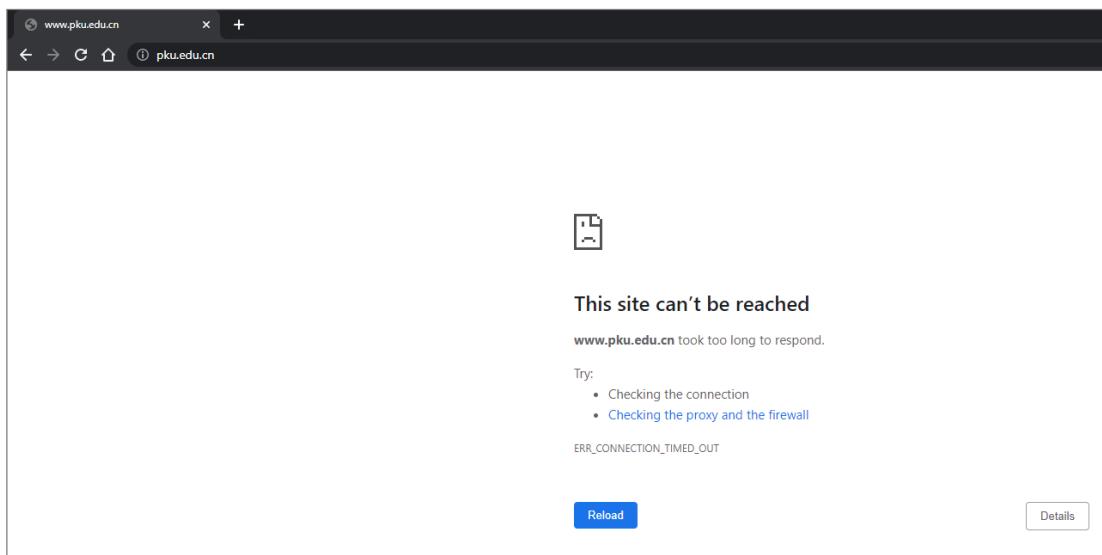
← Security Policy > Policy Control >

Configuration

Enable	<input checked="" type="checkbox"/>
Name	geo_block_policy
Description	<input type="text"/>
From	LAN 
To	WAN 
Source	any 
Destination	geo_block 
Service	any 
User	any 
Schedule	none 
Action	deny 
Log	log 

Test the Result

When the LAN PC tries to access a website that matches the blocked geographical location, it is unable to reach those sites.

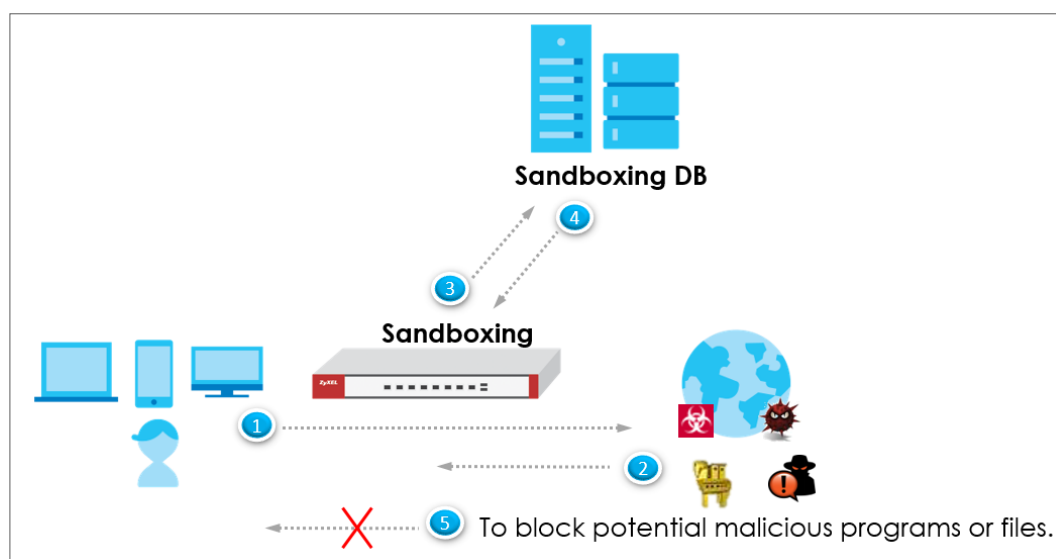



To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

#	Time	Category	Message	Source	Destination	Note
7	2023-05-21 18:16:34	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
8	2023-05-21 18:16:34	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
9	2023-05-21 18:16:30	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
10	2023-05-21 18:16:30	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
11	2023-05-21 18:16:28	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
12	2023-05-21 18:16:28	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
13	2023-05-21 18:16:27	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK

How to Use Sandbox to Detect Unknown Malware?

This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Sandbox

Navigate to **Security Service > Sandbox**. Enable Sandbox option and choose the desired action when the Sandbox detects malicious and suspicious files. Additionally, select the desired file type for submission; currently, we support the following file types: Executables (exe), MS Office Document (doc...), Macromedia Flash Data (swf), PDF Document (pdf), RTF Document (rtf), and ZIP Archive (zip).

ZYXEL NETWORKS USG FLEX 500H

Search

Security Service > Sandbox > Sandbox

Sandbox

Enable Sandbox ☒

Collect Statistics ☒

Action For Malicious File

Log For Malicious File

Action For Suspicious File

Log For Suspicious File

File Type For Submission

Available	Member
	<input type="checkbox"/> Executables (exe)
	<input type="checkbox"/> MS Office Document (doc...)
	<input type="checkbox"/> Macromedia Flash Data (swf)
	<input type="checkbox"/> PDF Document (pdf)
	<input type="checkbox"/> RTF Document (rtf)
	<input type="checkbox"/> ZIP Archive (zip)

Test the Result

When downloading the file, the firewall will query the Sandbox DB to detect whether it is a malicious or suspicious file. You can navigate to **Log & Report > Log/Events** to see the sandbox related logs.



#	Time	Category	Message	Source	Destination	Note
2	2023-07-31 16:18:14	Sandbox	Query File name: wildfire-test-pe-file.exe, md5: a2b6588b52a6b6c6a7e164b70114b4a57, file id: 58207, protocol: HTTP, htd: 27	34.84.44.247	192.168.168.34	SANDBOX QUERY

How to Configure Reputation Filter- IP Reputation

As cyber threats such as scanners, botnets, phishing, etc. grow increasingly, how to identify suspect IP addresses of threats efficiently becomes a crucial task.

With regularly updated IP database, FLEX prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

This example illustrates how to configure IP Reputation on FLEX gateway to detect cyber threats for both incoming and outgoing traffic.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the IP reputation filter

Go to Security Service > Reputation Filter > IP reputation. Turn on this feature. Select Block on Action field. The threat level threshold is measured by the query score of IP signature database.

IP Reputation	DNS Threat Filter	URL Threat Filter
IP Blocking		
Enable	<input checked="" type="checkbox"/>	
Action	block ▼	
Threat Level Threshold	high ▼	
Log	log ▼	
Statistics	<input checked="" type="checkbox"/>	

Select categories in Types of Cyber Threats Coming from the Internet, and Types of Cyber Threats Coming from The Internet and Local Networks.

Types of Cyber Threats Coming From The Internet		
<input checked="" type="checkbox"/> Anonymous Proxies	<input checked="" type="checkbox"/> Denial of Service	<input checked="" type="checkbox"/> Exploits
<input checked="" type="checkbox"/> Negative Reputation	<input checked="" type="checkbox"/> Scanners	<input checked="" type="checkbox"/> Spam Sources
<input checked="" type="checkbox"/> TOR Proxies	<input checked="" type="checkbox"/> Web Attacks	<input checked="" type="checkbox"/> Phishing
Types of Cyber Threats Coming From The Internet And Local Networks		
<input checked="" type="checkbox"/> Botnets		

Go to Security Service > Reputation Filter > IP reputation > White List and Black List to manually adding IP addresses to Black List.

IP Reputation

DNS Threat Filter

URL Threat Filter

Allow List

Enable

☒

Log

no

+ Add

Edit

Remove

Active

Inactive

<input type="checkbox"/>	Status	IPv4 Address
No data		

Rows per page: 50 0 of 0 < 1 >

Block List

Enable

☒

Log

log

+ Add

Edit

Remove

Active

Inactive

<input type="checkbox"/>	Status	IPv4 Address
<input type="checkbox"/>	<input checked="" type="checkbox"/>	107.155.48.246

Test the Result

Verify an IP in Test IP Threat Category. In Test IP Threat Category, enter a malicious IP and query the result.

Test IP Threat Category

IP to test

104.244.14.252

Query

Message

threat-level result: High

category result: BotNetsPhishing

Try to generate ICMP packet from LAN to destination IP 107.155.48.246, and 104.244.14.252

Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.

Log & Report > Log / Events

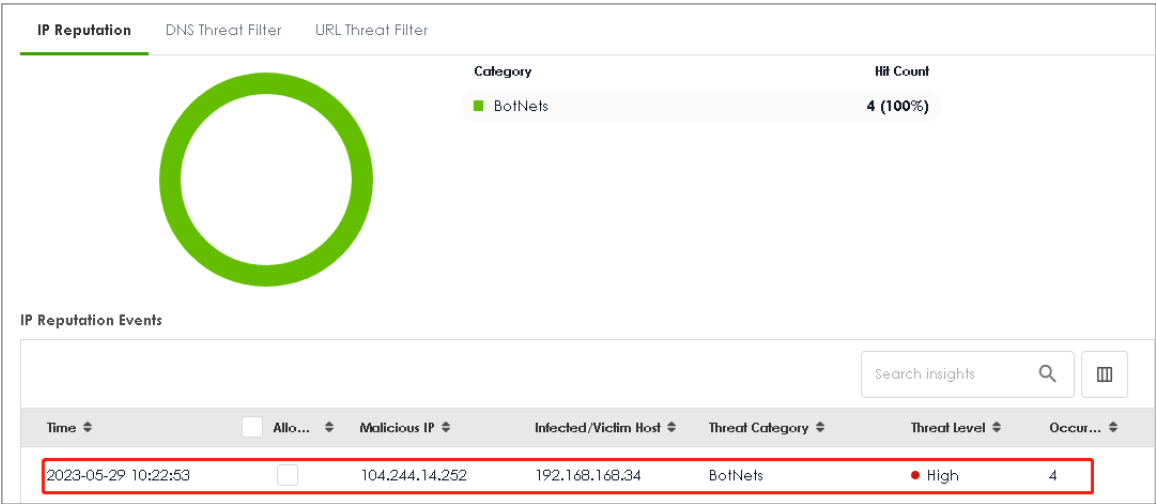
Category IP Reputation

Filter Refresh Clear Log

Search insights

#	Time	Category	Message	Source	Destination	Note
1	2023-05-29 10:42:19	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
2	2023-05-29 10:42:18	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
3	2023-05-29 10:42:17	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
50	2023-05-29 10:22:56	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
51	2023-05-29 10:22:55	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
52	2023-05-29 10:22:54	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
53	2023-05-29 10:22:53	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK

Go to Security Statistics > Reputation Filter > IP reputation to check summary of all events.



How to Configure Reputation Filter- URL Threat Filter

URL Threat Filter can avoid users to browse some malicious URLs (such as anonymizers, browser exploits, phishing sites, spam URLs, spyware) and allows administrator to manage which URLs can be browsed or not.

This example demonstrates how to configure the URL Threat Filter to redirect web access after the client hits the URL Threat Filter categories.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the URL Threat Filter

Go to Security Service > Reputation Filter > URL Threat Filter. Turn on this feature. Select Block on Action field. When a client hits URL Threat Filter, the page will be Blocked. Choose Log-alert on Log field.

IP Reputation
DNS Threat Filter
URL Threat Filter

URL Blocking

Enable	<input checked="" type="checkbox"/>
Action	block ▼
Log	log alert ▼
Statistics	<input checked="" type="checkbox"/>

Security Threat Categories

<input checked="" type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Browser Exploits	<input checked="" type="checkbox"/> Malicious Downloads
<input checked="" type="checkbox"/> Malicious Sites	<input checked="" type="checkbox"/> Phishing	<input checked="" type="checkbox"/> Spam URLs
<input checked="" type="checkbox"/> Spyware Adware Keyloggers		

Test the Result

Verify a URL in the Security Threat Categories. In Test URL Threat Category, enter a malicious URL and query the result.

Test URL Threat Category

URL to test

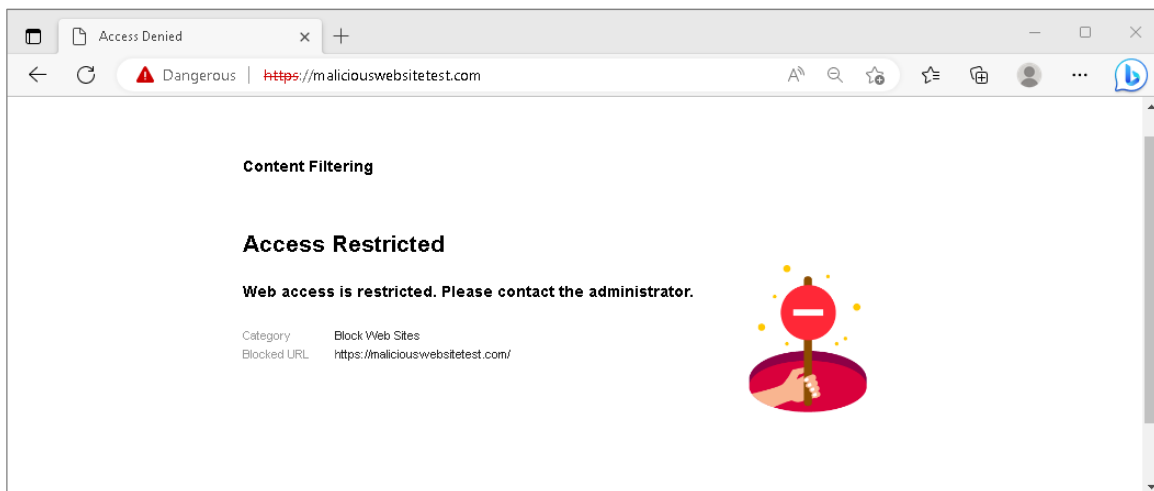
https://maliciouswebs

Query

Message

domain category result: information-security,malicious-sites(threat)
url category result: information-security,malicious-sites(threat)

Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



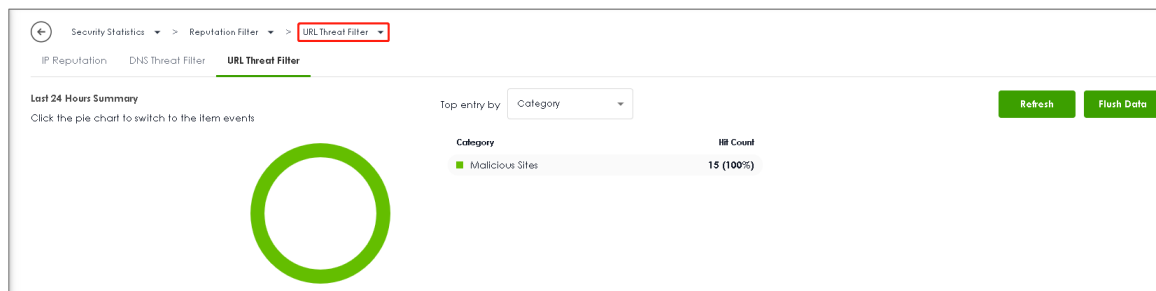
Go to Log & Report > Log/Events and select URL Threat Filter to check the logs.

Log & Report > Log / Events

Category: **URL Threat Filter** Filter Refresh Clear Log

#	Time	Category	Message	Source	Destination	Note
2	2023-05-28 15:41:06	url-threat-filter	maliciouswebsiteest.com/Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
3	2023-05-28 15:41:05	url-threat-filter	maliciouswebsiteest.com/Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
4	2023-05-28 15:41:05	url-threat-filter	maliciouswebsiteest.com/Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
5	2023-05-28 15:41:05	url-threat-filter	maliciouswebsiteest.com/Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
6	2023-05-28 15:41:05	url-threat-filter	maliciouswebsiteest.com/Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK

Go to Security Statistics > Reputation Filter > URL Threat Filter to check summary of all events.



URL Threat Filter Events

Search insights

Time	Allow list	URL	Category	Source IP	Destination IP
2023-05-28 02:33:39	<input type="checkbox"/>	maliciouswebsiteest.com/	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 02:33:40	<input type="checkbox"/>	maliciouswebsiteest.com/favicon.ico	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 02:33:41	<input type="checkbox"/>	maliciouswebsiteest.com/favicon.ico	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 07:40:47	<input type="checkbox"/>	maliciouswebsiteest.com	Malicious Sites	192.168.168.34	50.63.7.226
2023-05-28 07:40:51	<input type="checkbox"/>	maliciouswebsiteest.com	Malicious Sites	192.168.168.34	50.63.7.226
2023-05-28 07:40:55	<input type="checkbox"/>	maliciouswebsiteest.com	Malicious Sites	192.168.168.34	50.63.7.226

How to Configure Reputation Filter- DNS Threat Filter

DNS Threat Filter is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the administrator.

When a client wants to access a malicious domain, the query is sent to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. The cloud server identifies that this is bad site. What gateway can do here is send the redirect IP address where we deploy a blocked page to the client. The client will connect to redirect IP address instead of the real IP address of malicious domain, and get the blocked page with the web access. This example shows how to configure DNS Threat Filter to redirect web access after client hit the filter profile.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the DNS Threat Filter

Go to Security Service > Reputation Filter > DNS Threat Filter. Turn on this feature. Select Redirect on Action field. When a client hits DNS Threat Filter, the page will be redirected to the default blocked page or a custom IP address. Choose Log-alert on Log field. Configure Default on Redirect IP field to allow gateway redirect to the default blocked page.

IP Reputation
DNS Threat Filter
URL Threat Filter

DNS Threat Filter

Enable
☒

Action

redirect

Log

log alert

Redirect IP

default

Malform DNS packets

Action

drop

Log

log

Statistics
☒

Security Threat Categories

☒ Anonymizers
☒ Browser Exploits
☒ Malicious Downloads

☒ Malicious Sites
☒ Phishing
☒ Spam URLs

☒ Spyware Adware Keyloggers

Test the Result

Verify a domain name in the Security Threat Categories. In Test Domain Name Category, enter a malicious domain and query the result.

Test Domain Name Category

Domain name to test **Query**

If you think the category is incorrect, click this link to submit a request to review it.

Message ✕

domain category result: information-security, **malicious-sites(threat)**
url category result: information-security, malicious-sites(threat)

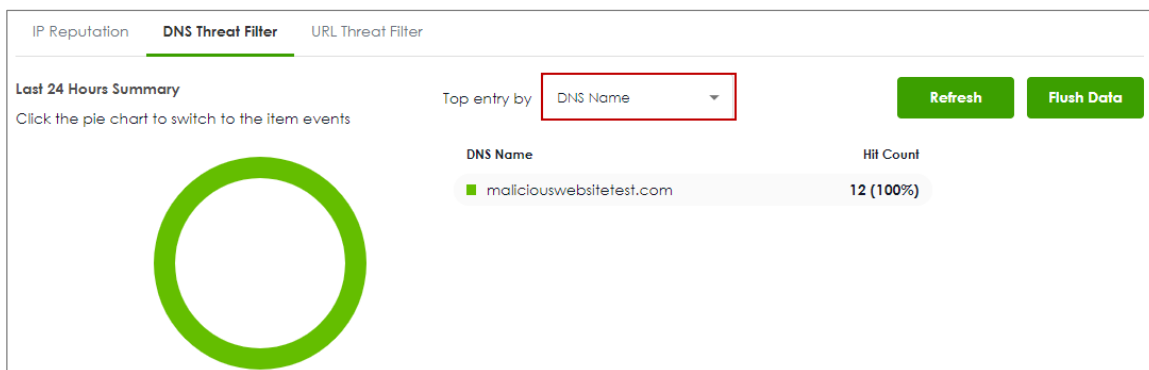
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



Go to Log & Report > Log/Events and select DNS Threat Filter to check the logs.

Category DNS Threat Filter Filter Refresh Clear Log Search insights						
#	Time	Category	Message	Source	Destination	Note
1	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS BLOCK
2	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS BLOCK
3	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS REDIRECT

Go to Security Statistics > Reputation Filter > DNS Threat Filter to check summary of all events.



DNS Threat Filter Events

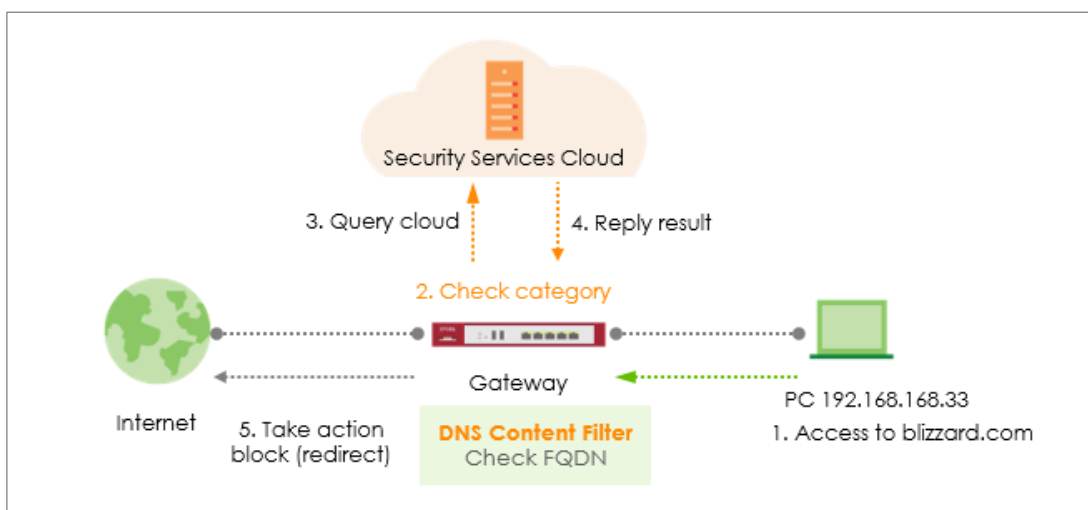
Search insights


Time	<input type="checkbox"/> +Allow ...	DNS Name	Category	Source IP
2023-05-21 16:29:36	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:44:04	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:47:02	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:49:26	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33

How to Configure DNS Content Filter

Compared to web content filter, DNS content filter is a stronger tool for SMB because it can restrict the number of attacks faced by network access, thereby helping to reduce the remediation workload of IT professionals.

DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those known domains hosting malicious content. This example shows how to configure DNS Content Filter to block users in the local network to access the gaming websites.



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the DNS Content Filter

Go to Security Service > Content Filtering > For DNS Domain scan. Turn on this feature. Select Redirect IP for the Blocked Domain. If user selects the default, when client hits DNS Content Filter profile, the page will be redirected to block page <http://dnsft.cloud.zyxel.com/>.

Content Filtering

For DNS Domain scan:

Enable DNS Domain scan ☒

Blocked Domain Redirect IP default

Category Server is unavailable Action pass

Log log

Collect Statistics ☒

Add a new profile in Profile Management to block gaming websites.

Profile Management

[+ Add](#) [Edit](#) [Remove](#) Search insights

Name	Description	Reference
<input type="checkbox"/> BPP		
<input type="checkbox"/> CIP		
<input checked="" type="checkbox"/> block_games		

Action: block

Log: log or log alert

General Settings

Name

Description

Action

block

Log

log

Log allowed traffic

SSL V3 or previous version Connection

Drop

Drop Log

no

Enable the checkbox of "Games" in managed categories.

Managed Categories

Select All Categories
Clear All Categories

☐ 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

Apply the profile to security policy. In this example, the profile is applied to security policy rule "LAN_Outgoing".

General Settings

Enable

Configuration

Allow Asymmetrical Route

+ Add
Edit
Remove
Active
Inactive
Move

Search insights

	St...	Pri...	Name	From	To	Source	Destination	Service	User	Schedule	Act...	Log	Profile
<input type="checkbox"/>		1	LAN_Out...	LAN	any (Ex...	any	any	any	any	none	allow	no	<div></div>
<input type="checkbox"/>		2	DMZ_to_...	DMZ	WAN	any	any	any	any	none	allow	no	block_games

Test the Result

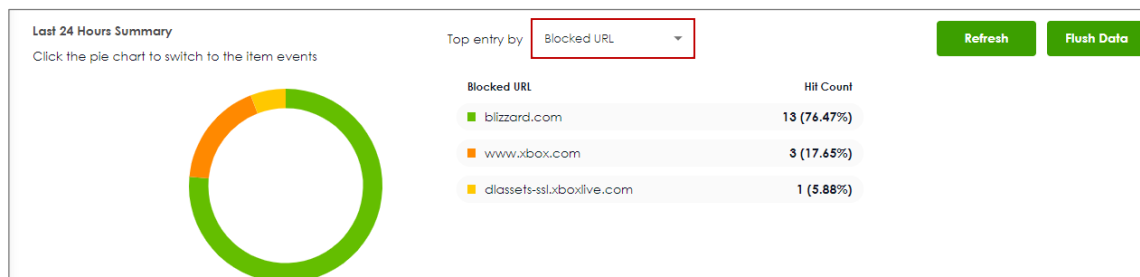
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



Go to Log & Report > Log/Events and select Content Filter to check the logs.

Category: Content Filter Filter Refresh Clear Log						
#	Time	Category	Message	Source	Destination	Note
471	2023-05-28 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
472	2023-05-28 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
506	2023-05-28 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
507	2023-05-28 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
508	2023-05-28 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
509	2023-05-28 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
754	2023-05-28 14:20:09	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK

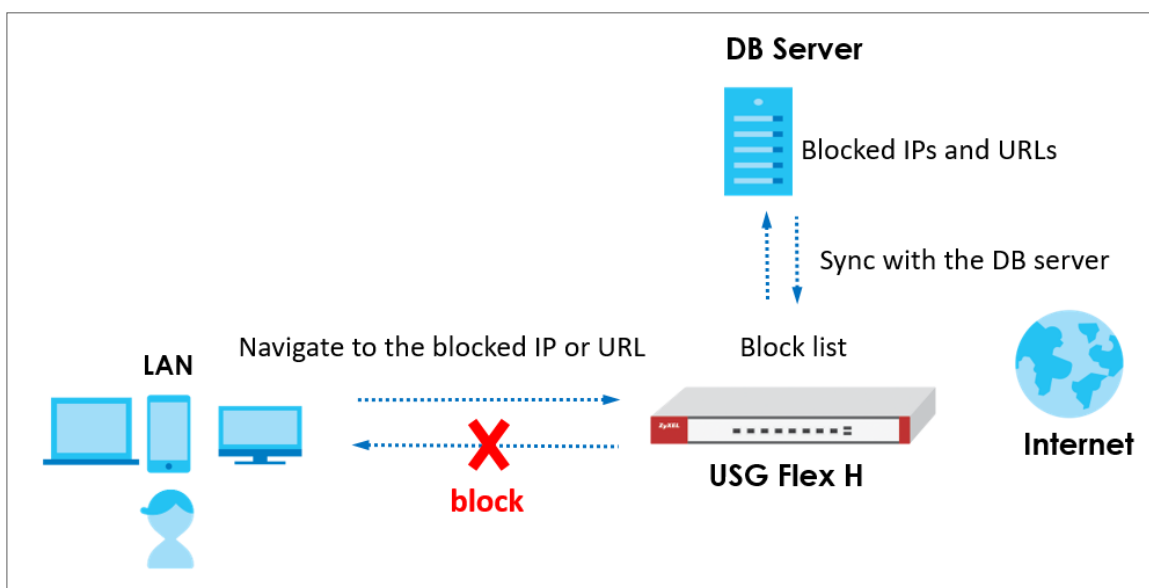
Go to Security Statistics > Content Filter to check summary of all events.




Content Filter Events						
<div> <div>Search insights</div> <div> </div> </div>						
Time ↕	Action ↕	URL/Domain ↕	Profile ↕	Category ↕	Source IP ↕	Destination IP ↕
2023-05-28 14:20:09	BLOCK	www.xbox.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 14:19:53	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:59:19	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:56:40	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:55:45	BLOCK	dassets-ssl.xboxlive.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:55:13	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1

External Block List for Reputation Filter

The administrator can configure an external block list for the Reputation Filter to expand its usage. This article will provide guidance on setting up the external block list for the IP Reputation and DNS Threat Filter/URL Threat Filter.

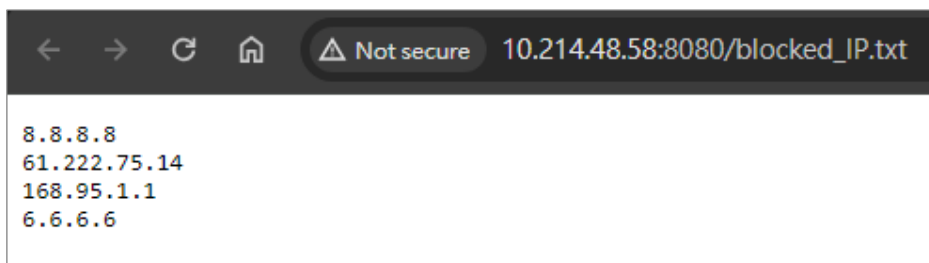


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Set Up the DB server

The administrator can set up websites to maintain external block lists. The USG Flex H firewall can update the external block list via a URL. For example,

http://10.214.48.58:8080/blocked_IP.txt



http://10.214.48.58:8080/blocked_URL.txt



Set Up the External Block List of IP Reputation

Navigate to Security Services > External Block List > IP Reputation and add a service URL such as http://10.214.48.58:8080/blocked_IP.txt and then click "Update Now" to update the block list.

Security Services
> External Block List
> IP Reputation

IP Reputation
DNS Threat Filter/URL Threat Filter

External Block List

Enable
☒

Profile Management

+ Add
Remove

	Name	Source URL	Description
<input type="checkbox"/>	Block_IP_List	http://10.214.48.58:8080/blocked_IP.txt	

Signature Update

Synchronize the signature to the latest version with online update server.

Update Now

Auto Update
☐

☐ Every N Hours

☒ Daily

☐ Weekly

☐ Weekly

If the IP Reputation external block list is updated successfully and you can observe the corresponding log message.

Log & Report > Log / Events

Category: All Log
Refresh
Clear Log
Export

Search inside

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port
1	2024-03-12 19:30:08	External Block List	Update IP reputation external block list completed(Block_IP_List).	0.0.0.0	0.0.0.0	0

Set Up the External Block List of DNS Threat Filter/URL Threat Filter

Navigate to Security Services > External Block List > DNS Threat Filter/URL Threat Filter and add a service URL such as http://10.214.48.58:8080/blocked_URL.txt and then click "Update Now" to update the block list.

The screenshot shows the 'DNS Threat Filter/URL Threat Filter' configuration page. At the top, there's a breadcrumb trail: Security Services > External Block List > DNS Threat Filter/URL Threat Filter. Below this, there are two tabs: 'IP Reputation' and 'DNS Threat Filter/URL Threat Filter', with the latter being selected. The 'External Block List' section has an 'Enable' toggle switch that is turned on. Under 'Profile Management', there are '+ Add' and 'Remove' buttons. A table lists the configured profiles:

Name	Source URL	Description
Block_URL_List	http://10.214.48.58:8080/blocked_URL.txt	

Below the table is the 'Signature Update' section, which includes a description: 'Synchronize the signature to the latest version with online update server.' and an 'Update Now' button. There is also an 'Auto Update' toggle switch, which is currently turned off. Under 'Auto Update', there are three radio button options: 'Every N Hours', 'Daily' (which is selected), and 'Weekly'. Each option has associated dropdown menus for frequency, time, and day.

If the DNS/URL threat filter external block list is updated successfully and you can observe the corresponding log message.

The screenshot shows the 'Log & Report' section, specifically the 'Log / Events' tab. It includes a search bar and buttons for 'Refresh', 'Clear Log', and 'Export'. The log entry is as follows:

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port
1	2024-03-12 19:31:06	External Block List	Update DNS/URL threat filter external block list completed(Block_URL_List).	0.0.0.0	0.0.0.0	0

Test the Result

For instance, if the IP addresses 8.8.8.8 and 168.95.1.1 exist in the external block list, attempts to access these blocked IPs will be blocked as expected.

```
C:\Users\<redacted>>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\<redacted>>ping 168.95.1.1

Pinging 168.95.1.1 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.

Ping statistics for 168.95.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Go to Log & Report > Log / Events to observe block messages.

Log & Report > Log / Events							
Category All Log Refresh Clear Log Export							
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 11:23:59	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
2	2024-03-13 11:23:58	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
3	2024-03-13 11:23:57	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
4	2024-03-13 11:23:56	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
5	2024-03-13 11:23:19	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
6	2024-03-13 11:23:18	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
7	2024-03-13 11:23:17	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
8	2024-03-13 11:23:16	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK

Attempts to access URLs that exist in the block list will also be blocked as expected.

Not secure
https://www.bot.com.tw

Web Page Blocked!!

You have tried to access a web page which belongs to a DNS Filter category that is blocked.

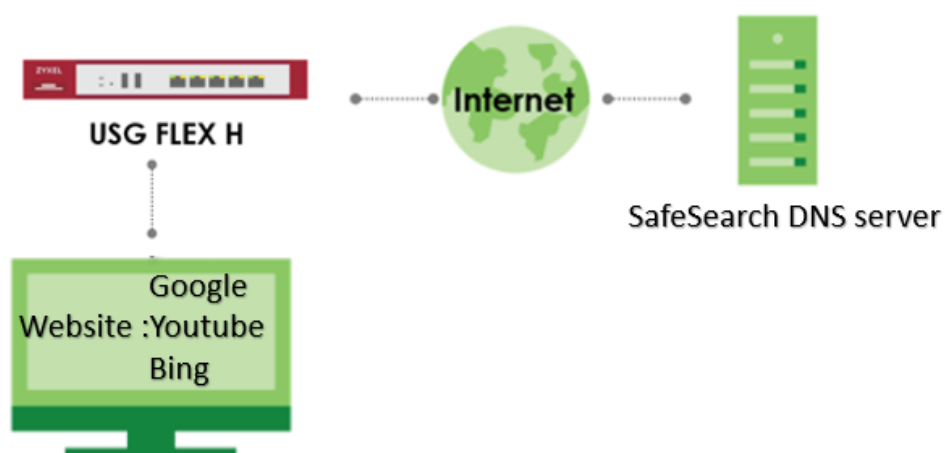
Go to Log & Report > Log / Events to observe block messages.

Log & Report > Log / Events							
Category All Log Refresh Clear Log Export							
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	NOT A TYPE
2	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	NOT A TYPE
3	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	A TYPE

How to set up DNS SafeSearch?

SafeSearch is a feature that acts as an automated filter of pornography and potentially offensive and inappropriate content.

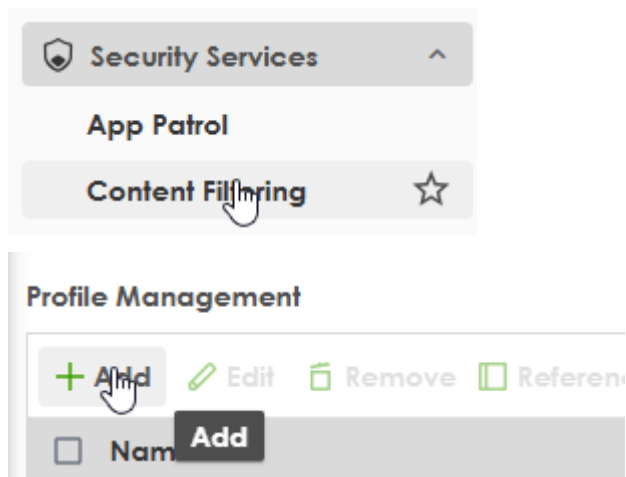
This guide explains how to configure your gateway to set up DNS Safe Search.



💡 Note: DNS SafeSearch is supported on USG Flex H series. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.35).

Step 1: Set up a SafeSearch Profile

Log in to Local Web GUI - Navigate to Security Services > Content Filtering.



Configure the Profile

DNS Safesearch: Click the button to enable the function.

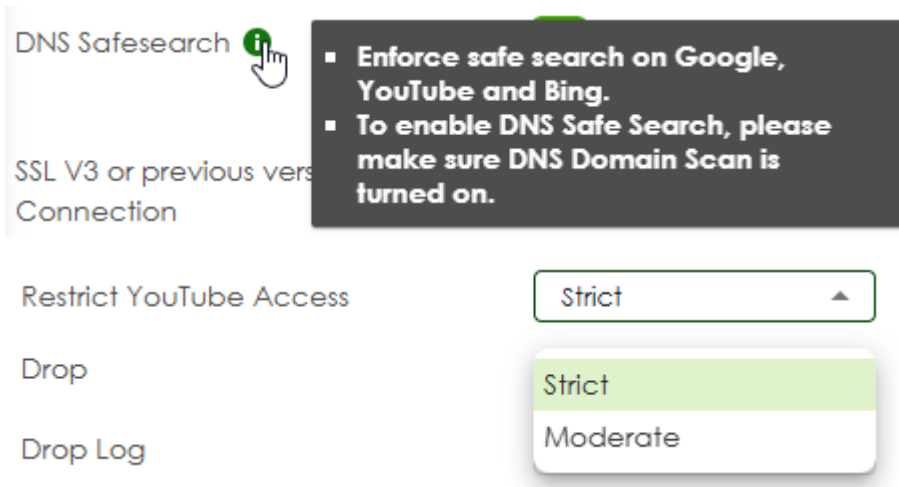
Enforce safe search on Google, Youtube, Bing.

To enable DNS Safe Search, please make sure DNS Domain Scan is turned on.

Restrict Youtube Access: The Restrict YouTube Access setting allows you to choose between Strict and Moderate modes.

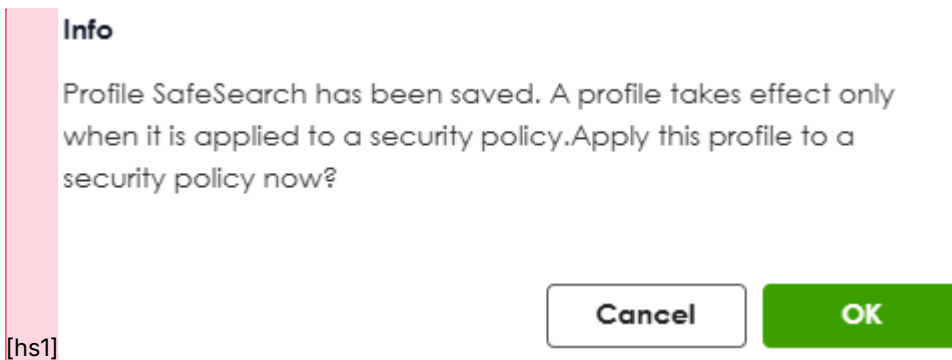
The screenshot shows the configuration page for a 'SafeSearch' profile. The page is titled 'General Settings' and includes the following fields and controls:

- Name:** SafeSearch
- Description:** SafeSearch
- Action:** block
- Log:** no
- Log allowed traffic:** ☐
- DNS Safesearch:** ☒
- Restrict YouTube Access:** Moderate
- SSL V3 or previous version Connection:** Drop
- Drop Log:** no



Step 2: Apply the safe search profile to Security Policy Rule

After completing the profile, a message will pop up to guide you in applying the profile to the Security Policy Rule

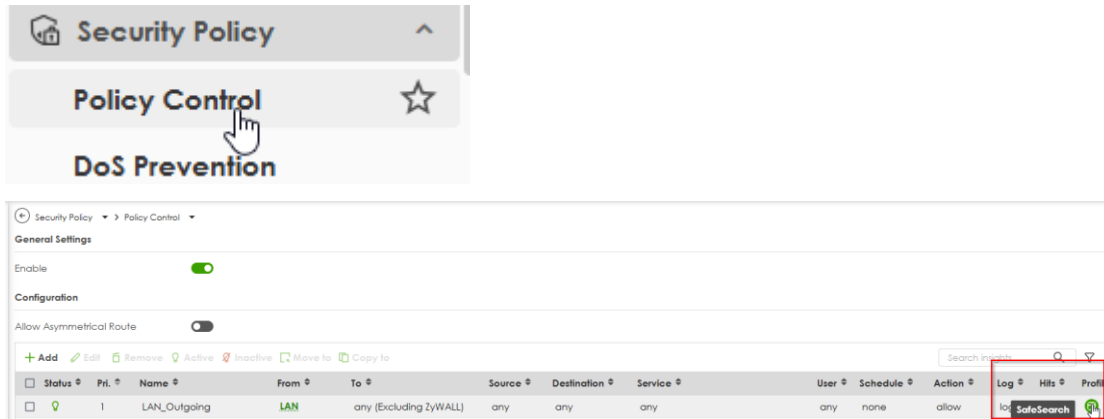


Click OK and apply the profile to the desired rule

Apply SafeSearch to a security policy

	Status	Pri.	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log
<input checked="" type="checkbox"/>	🟢	1	LAN_Outgoing	LAN	any (Excluding ZyWALL)	any	any	any	any	none	allow	log
<input type="checkbox"/>	🟢	2	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no
<input type="checkbox"/>	🟢	3	IPSec_VPN_Outgoing	IPSec_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
<input type="checkbox"/>	🟢	8	SSL_VPN_Outgoing	SSL_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
<input type="checkbox"/>	🟢	10	NEBULAVPN_Outgoing	NEBULAVPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
<input type="checkbox"/>	🟢	12	Tailscale_Outgoing	Tailscale	any (Excluding ZyWALL)	any	any	any	any	none	allow	no

After implementation, please navigate to Security Policy > Policy Control to check if the rule has been correctly set up.



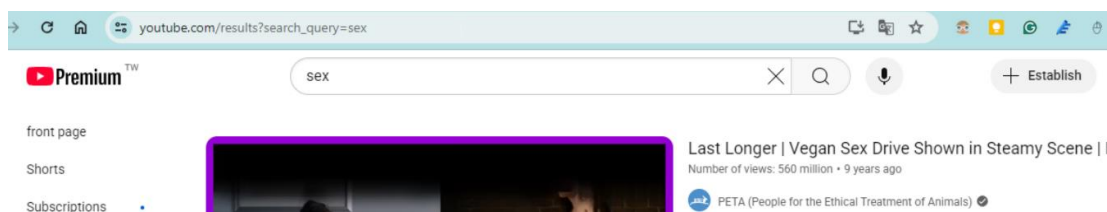
Step 3: Verified SafeSearch Function

Before verified the SafeSearch, if there is no other setting on DNS, normally the query result will display as below.

www.youtube.com

```
C:\Users\kukum>nslookup www.youtube.com
Server: UnKnown
Address: 192.168.168.1

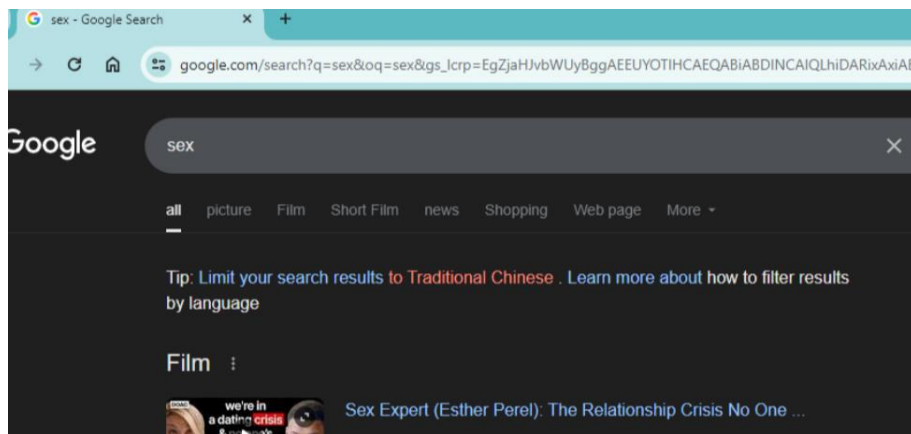
Non-authoritative answer:
Name: youtube-ui.l.google.com
Addresses: 2404:6800:4012:9::200e
           2404:6800:4012:6::200e
           2404:6800:4012:5::200e
           2404:6800:4012:8::200e
           142.250.66.78
           142.250.204.46
           142.250.196.206
           142.250.198.78
Aliases: www.youtube.com
```



www.google.com

```
C:\Users\kukum>nslookup www.google.com
Server: UnKnown
Address: 192.168.168.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4012:9::2004
          142.250.196.196
```

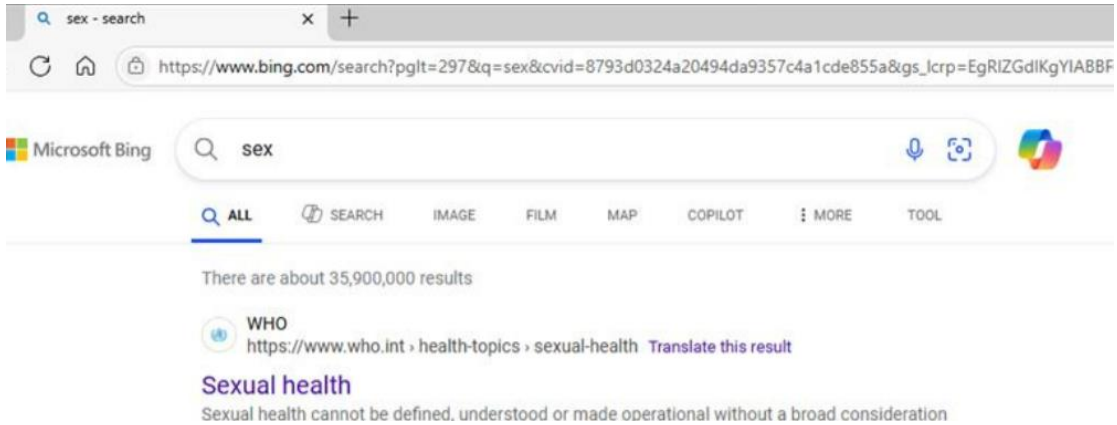


www.bing.com

```
C:\Users\kukum>nslookup www.bing.com
Server: UnKnown
Address: 192.168.168.1

Non-authoritative answer:
Name: e86303.dscx.akamaiedge.net
Addresses: 2001:b034:1c:200::d247:e3d1
          2001:b034:1c:200::d247:e3d8
          2001:b034:1c:200::d247:e3d0
          2001:b034:1c:200::d247:e3d2
          2001:b034:1c:200::d247:e3d3
          210.71.227.211
          210.71.227.208
          210.71.227.210
          210.71.227.209
          210.71.227.216
          210.71.227.202
          210.71.227.218

Aliases: www.bing.com
          www-www.bing.com.trafficmanager.net
          www.bing.com.edgekey.net
```



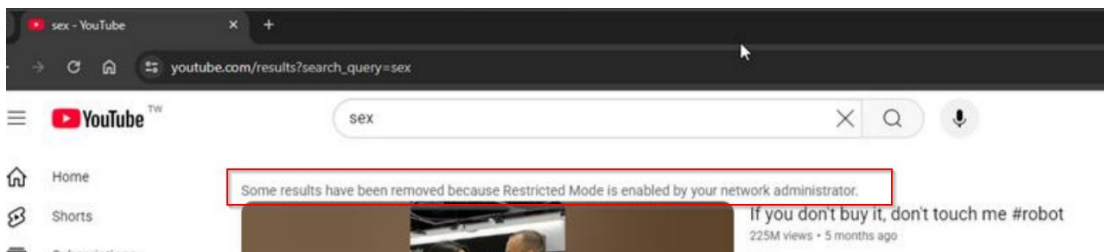
Ensure that the DNS server assignment is automatic get from the firewall.

IP assignment:	Automatic (DHCP)
DNS server assignment:	Automatic (DHCP)

www.youtube.com

```
C:\Users\kukum>nslookup www.youtube.com
Server: UnKnown
Address: 192.168.168.1

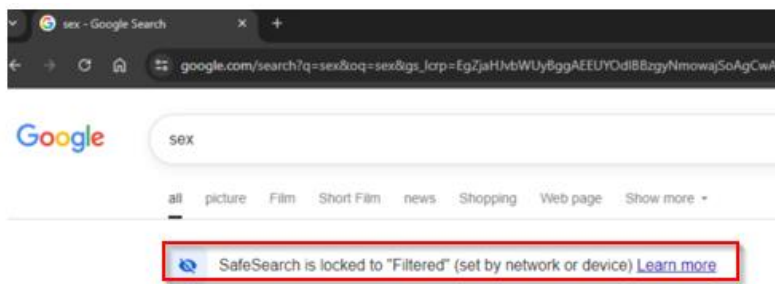
Name: www.youtube.com
Address: 216.239.38.120
Aliases: www.youtube.com
```



www.google.com

```
C:\Users\kukum>nslookup www.google.com
Server: UnKnown
Address: 192.168.168.1

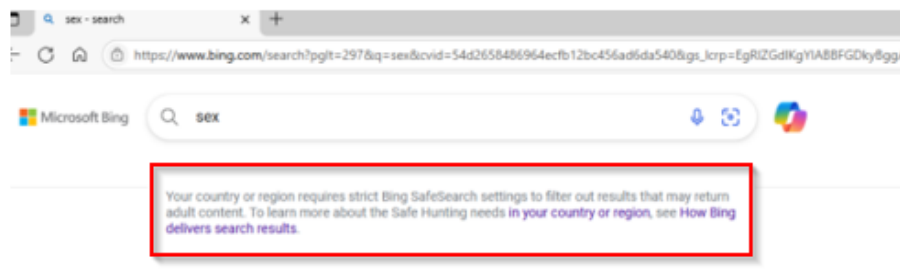
Name:      www.google.com
Address: 216.239.38.120
Aliases:   www.google.com
```



www.bing.com

```
C:\Users\kukum>nslookup www.bing.com
Server: UnKnown
Address: 192.168.168.1

Name:      a-0017.a-msedge.net
Address: 150.171.27.16
Aliases:   www.bing.com
           strict.bing.com
           strict-bing-com.a-0017.a-msedge.net
```



Troubleshooting

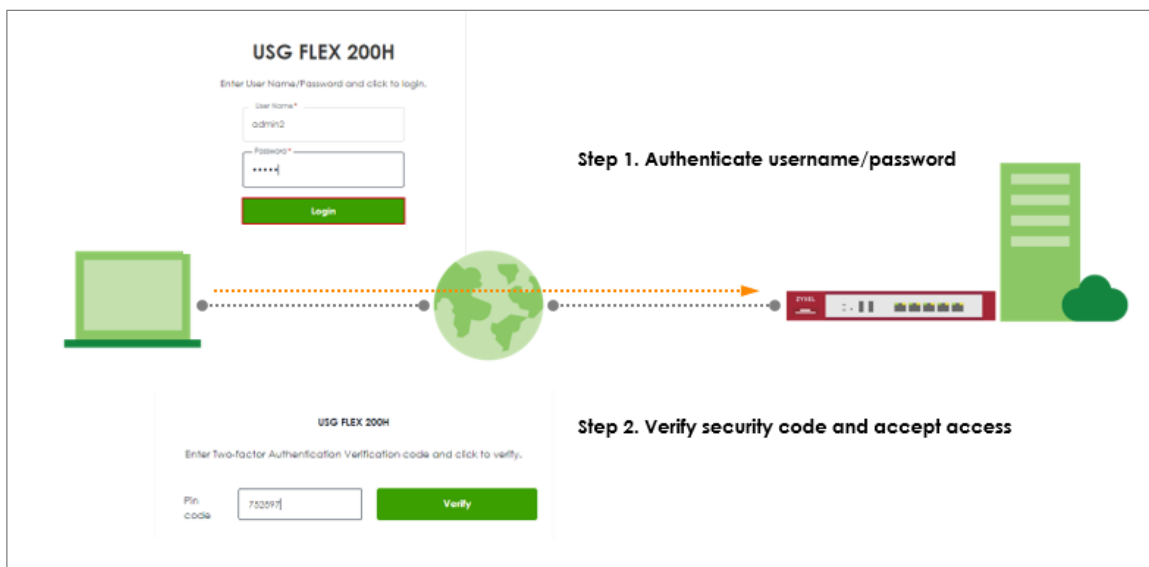
DNS Safe Search is not working

- Double-check the Ethernet or Wi-Fi adapter: Ensure that the DNS IP address is set as automatic get DHCP assignment.
- Devices are using alternative DNS servers (e.g., hardcoded DNS like 8.8.8.8).
- DNS over HTTPS (DoH) or DNS over TLS (DoT) may be enabled and bypassing your filtering.
- Cached DNS or browser settings are showing previous search results without SafeSearch applied.

Chapter 3- Authentication

How to Use Two Factor with Google Authenticator for Admin Access

Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for admin access.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Two Factor with Google Authenticator Flow

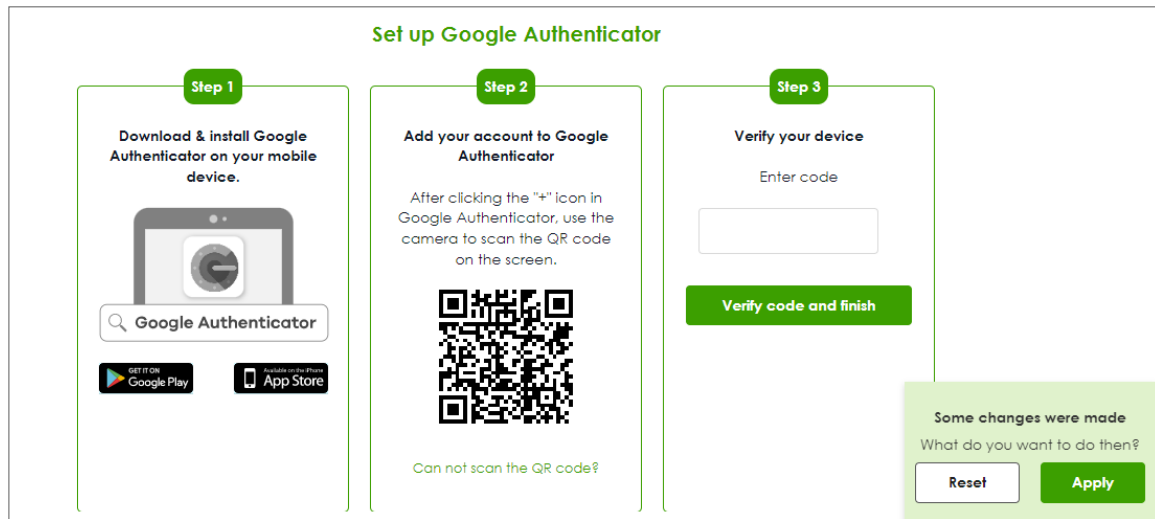
1. Enable Google Authentication on specific admin user.
2. Set up Google Authenticator.
3. Configure valid time and login service types.

Enable Google Authentication on specific admin user

Go to User & Authentication > User/Group. Select a specific local administrator and enable Two-factor authentication.

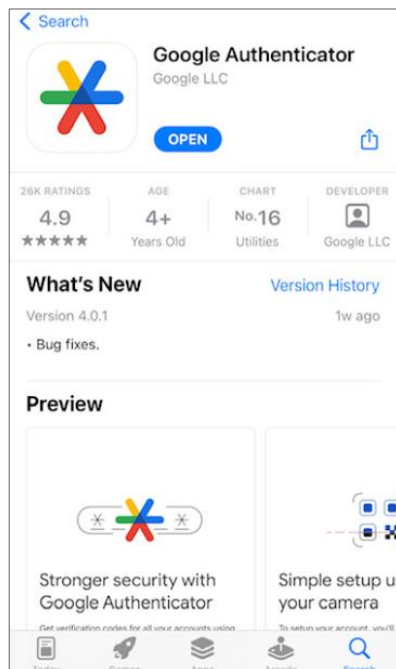
Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.

Set up Google Authenticator

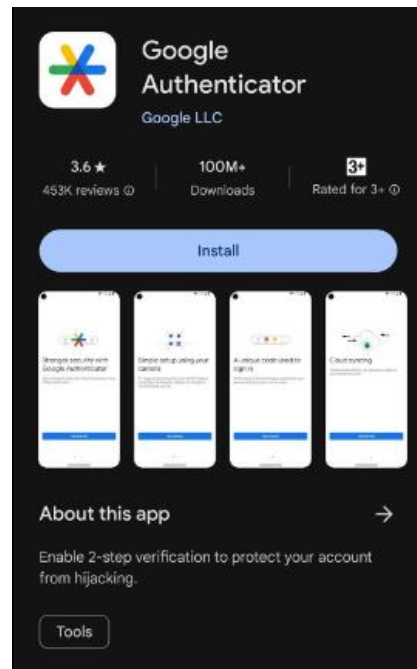


1. Download and install Google Authenticator on your mobile device.

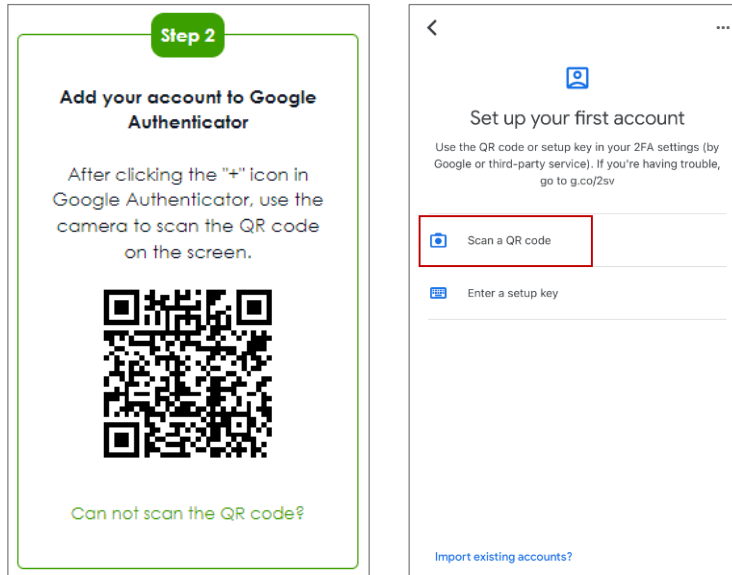
Apple Store



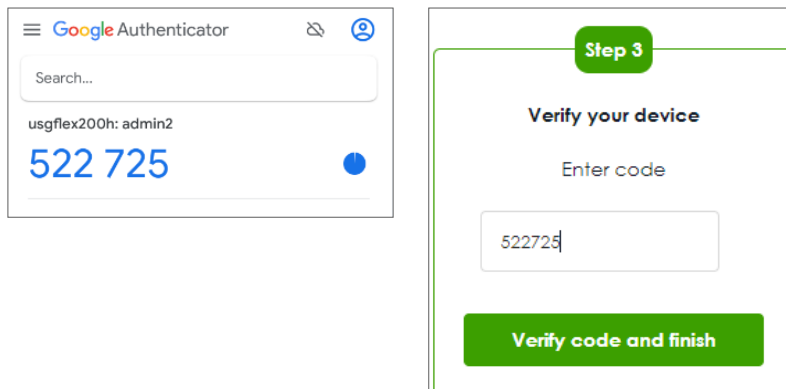
Google Play



2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



- After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.

View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

Download

84177830

93398990

96834809

97350265

59001448

Regenerate backup codes

Configure valid time and login service types

Go to User & Authentication > User Authentication. Two factor authentication for admin access is enabled by default. You need to select which services require two-factor authentication for admin user manually. The valid time is the deadline that admin needs to submit the two-factor authentication code to get the access. The access request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes.

Two-factor Authentication

Admin Access

Enable ☒

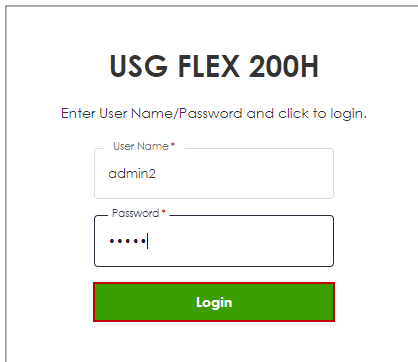
Valid Time (1-5 minutes)

Two-factor Authentication for Services:

☒ Web ☒ SSH

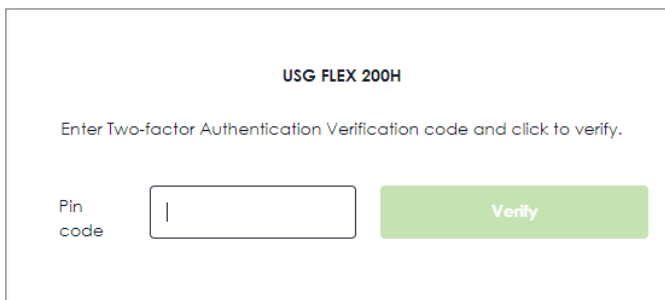
Test the Result

1. Login with the admin account "admin2".



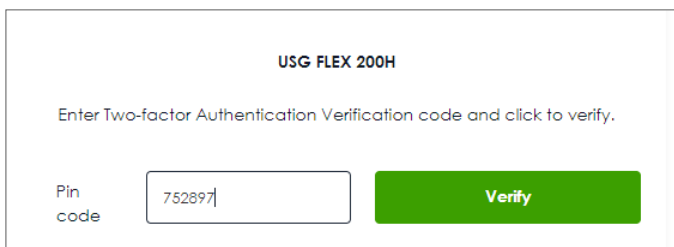
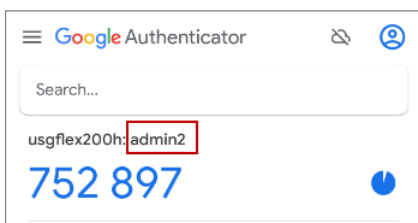
The image shows the login page for the USG FLEX 200H. At the top, it says "USG FLEX 200H". Below that, it says "Enter User Name/Password and click to login." There are two input fields: "User Name" with the value "admin2" and "Password" with masked characters ".....". A green "Login" button is at the bottom.

2. A pop-up window appears for administrator to enter the verification code.



The image shows the verification page for the USG FLEX 200H. At the top, it says "USG FLEX 200H". Below that, it says "Enter Two-factor Authentication Verification code and click to verify." There is a "Pin code" label next to an input field. A green "Verify" button is to the right of the input field.

3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



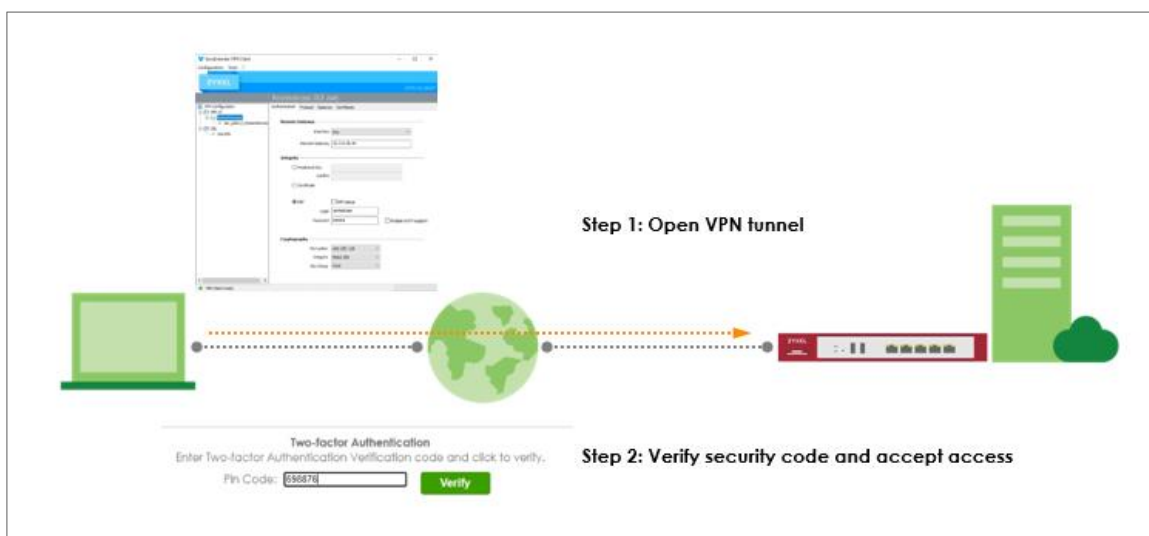
The image shows the verification page for the USG FLEX 200H, similar to the previous one. However, the "Pin code" input field now contains the code "752897". The "Verify" button remains green.


4. Authorize with username, password and the token code successfully. Go to Log & Report > Log/Events and select "User" to check the login status.

<div> Category User Filter Refresh Clear Log </div> <div> Search insights </div>						
#	Time	Categ...	Message	Source	Destination	Note
2	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
3	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
4	2023-05-21 14:26:34	user	user: admin2(10.214.36.16) is waiting to authorize.	0.0.0.0	0.0.0.0	two-factor auth.
5	2023-05-21 14:26:34	user	Administrator admin2(MAC=) from http/https has logged in Device	10.214.36.16	0.0.0.0	Account: ad...

How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN

Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for Remote Access VPN and SSL VPN.



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Two Factor with Google Authenticator Flow

4. Enable Google Authentication on a user.
5. Set up Google Authenticator.
6. Configure valid time and VPN types.

Enable Google Authentication on a User

Go to User & Authentication > User/Group. Select a local user and enable Two-factor authentication.

← User & Authentication ▾ > User/Group ▾ > User ▾

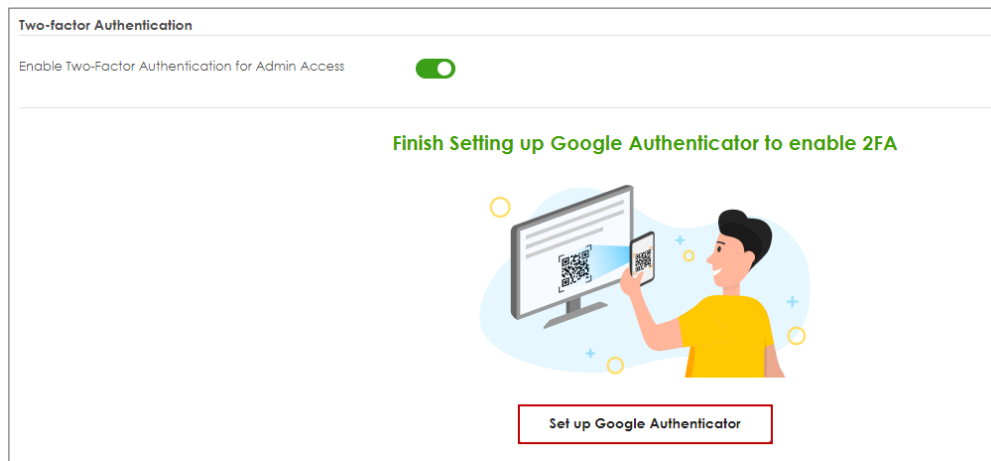
Profile Management

User Name	vpntestuser		
User Type	user		
Password	<input type="password" value="....."/>		
Retype	<input type="password" value="....."/>		
Description	<input type="text"/>		
Email 1	<input type="text"/>		
Email 2	<input type="text"/>		
Mobile Number	<input type="text"/>		
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings	<input type="radio"/> Use Manual Settings	
	Lease Time	1440	minutes
	Reauthentication Time	1440	minutes

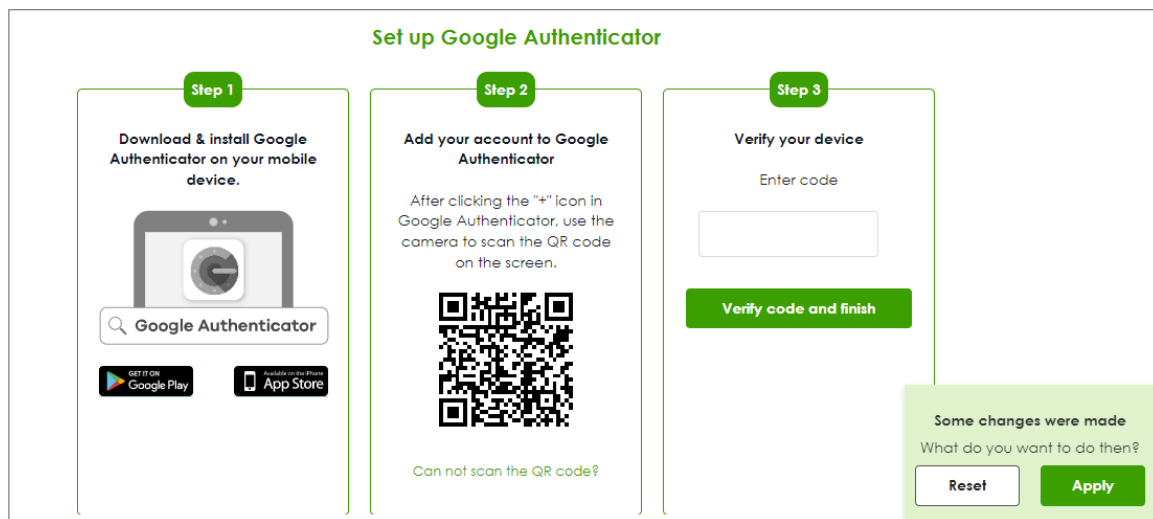
Two-factor Authentication

Enable Two-Factor Authentication for VPN Access ☒

Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.

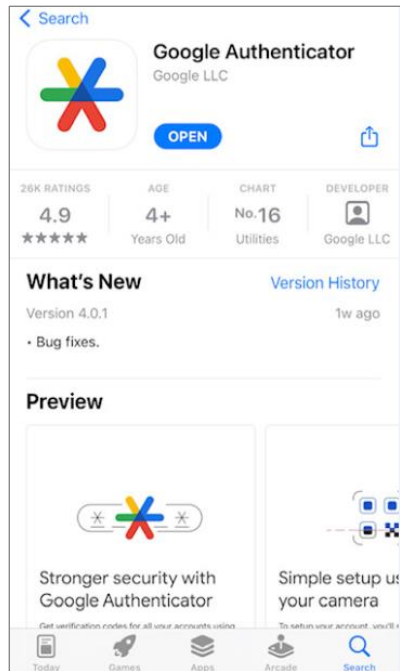


Set up Google Authenticator

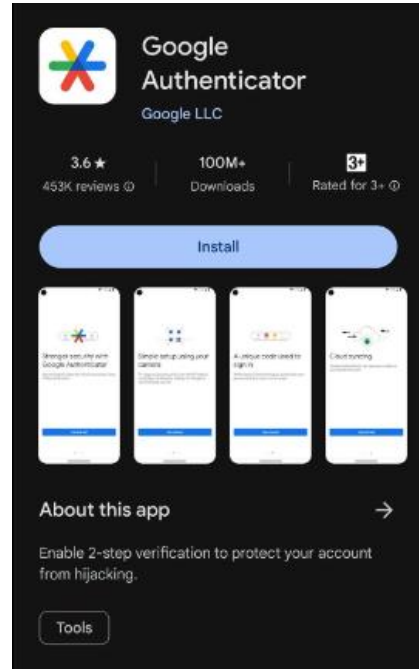


- Download and install Google Authenticator on your mobile device.

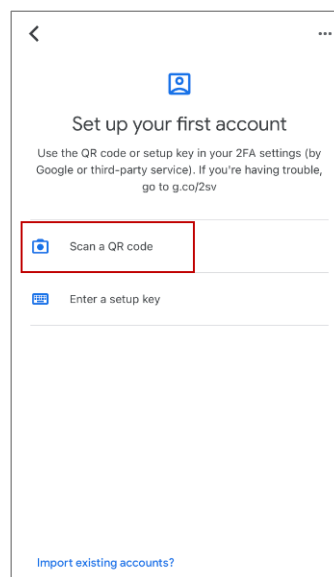
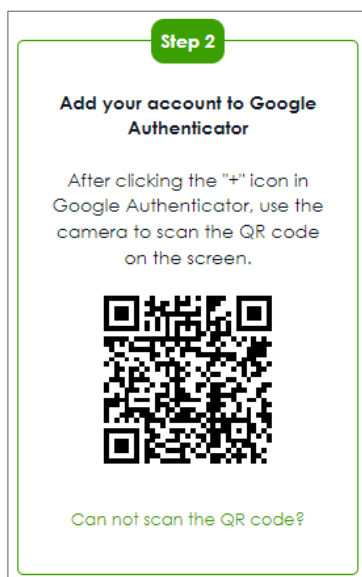
Apple Store



Google Play



- Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



7. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



Step 3

Verify your device

Enter code

754377

Verify code and finish

8. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.

View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

Download

81819556
70461950
51507415
38976818
39934997

Regenerate backup codes

Configure valid time and login service types

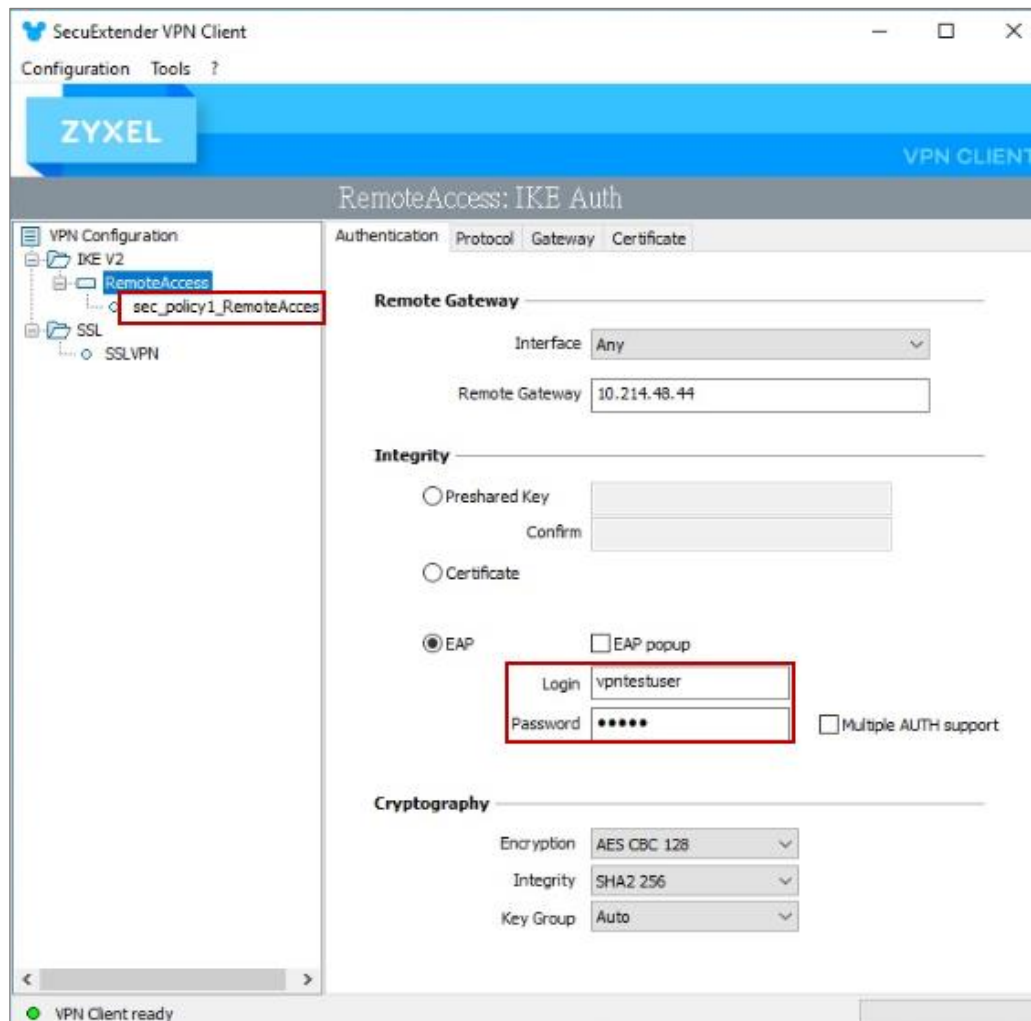
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes. The authentication page is working on specific service port. After building up VPN tunnel, user have to enter the code in the Web GUI.

AAA Server		Two-factor Authentication	
Admin Access			
Enable	<input checked="" type="checkbox"/>		
Valid Time	<input type="text" value="3"/>	(1-5 minutes)	
Two-factor Authentication for Services			
	<input type="checkbox"/> Web	<input type="checkbox"/> SSH	
VPN Access			
Enable	<input checked="" type="checkbox"/>		
Valid Time	<input type="text" value="3"/>	(1-5 minutes)	
Two-factor Authentication for Services			
	<input checked="" type="checkbox"/> SSL VPN Access	<input checked="" type="checkbox"/> IPSec VPN Access	
Delivery Settings			
Authorize Link URL Address	<input type="text" value="HTTPS"/>	<input type="text" value="From Interface"/>	<input type="text" value="ge3"/>
Authorized Port	<input type="text" value="8008"/>	(1-65535) ⓘ	

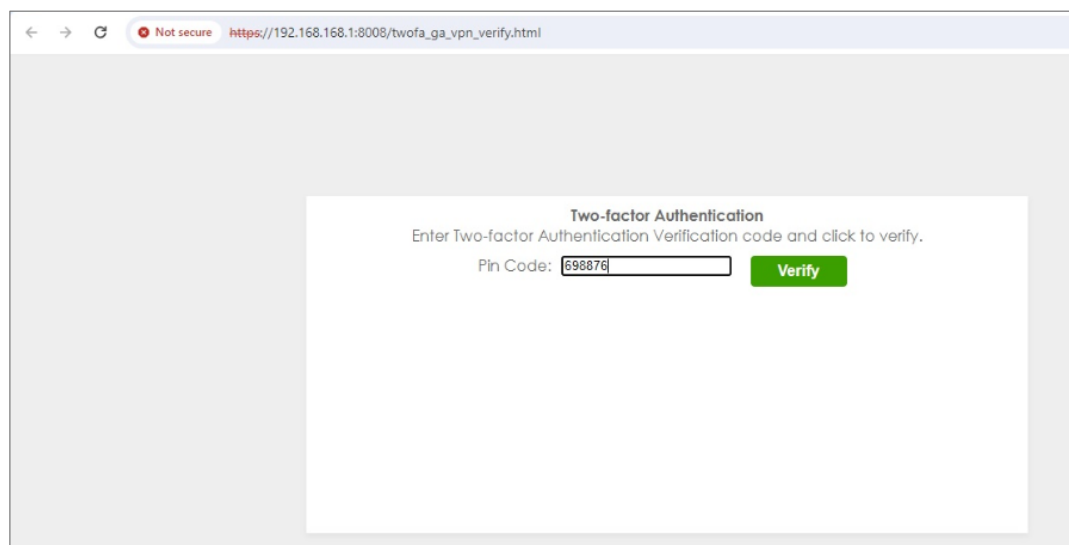
Test the Result

Remote Access VPN (IKEv2)

1. Open Remote Access VPN tunnel on SecuExtender VPN Client.



- The browser will pop up authentication page to enter the verification code. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.

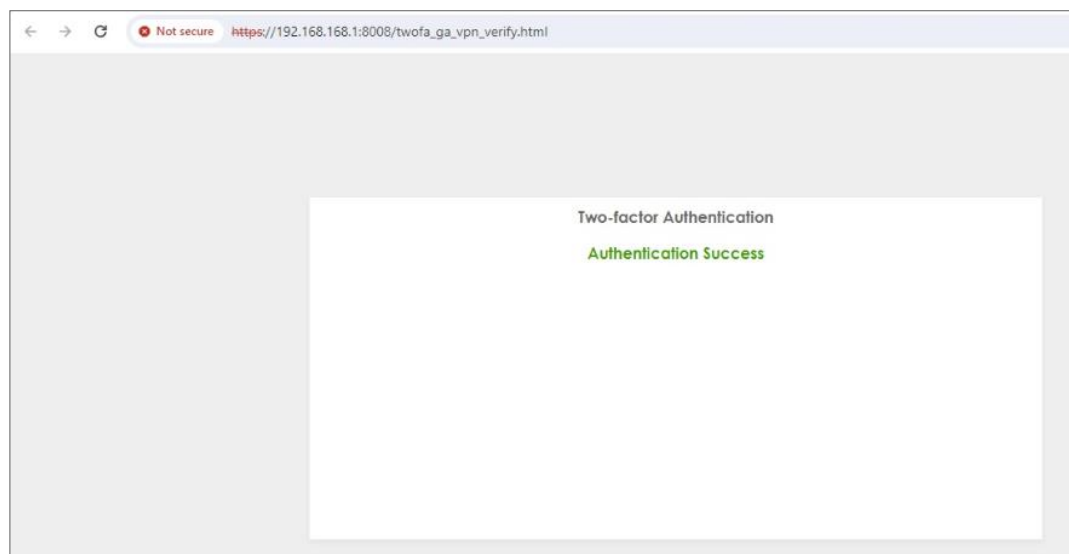


Two-factor Authentication

Enter Two-factor Authentication Verification code and click to verify.

Pin Code:

- Authorize with username, password and the token code successfully.



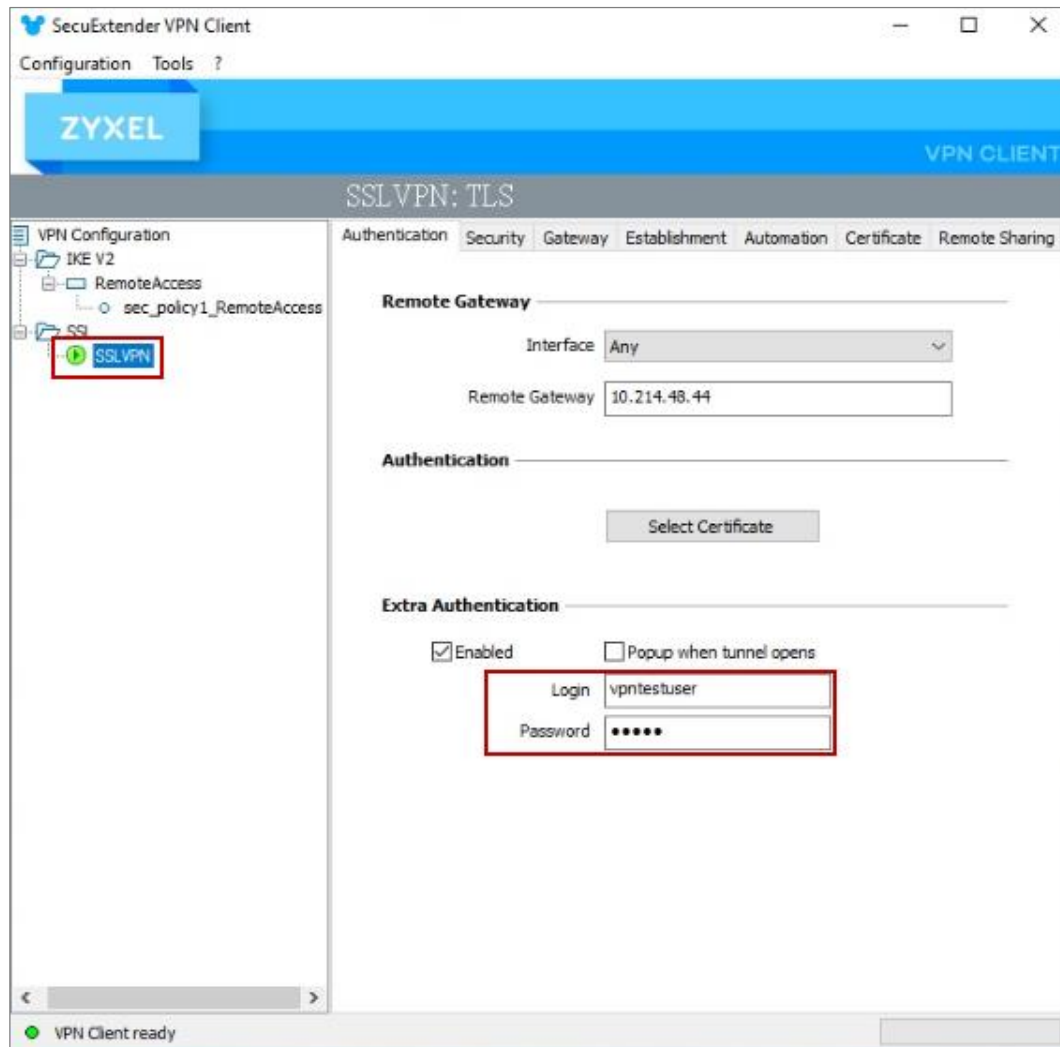
Two-factor Authentication

Authentication Success

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	user: vpntestuser(192.168.50.1) is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
67	2024-03-13 18:22:45	User	User vpntestuser(MAC=) from eap-cfg h as logged in Device	10.214.48.49	0.0.0.0	0	Account: vpntestuser
72	2024-03-13 18:22:45	IPSec VPN	assigning virtual IP 192.168.50.1 to peer 'vpntestuser'	10.214.48.44	10.214.48.49	500	

SSL VPN

1. Open SSL VPN tunnel on SecuExtender VPN Client.



- The browser will pop up authentication page to enter the verification code. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.

Two-factor Authentication

Enter Two-factor Authentication Verification code and click to verify.

Pin Code:

- Authorize with username, password and the token code successfully.

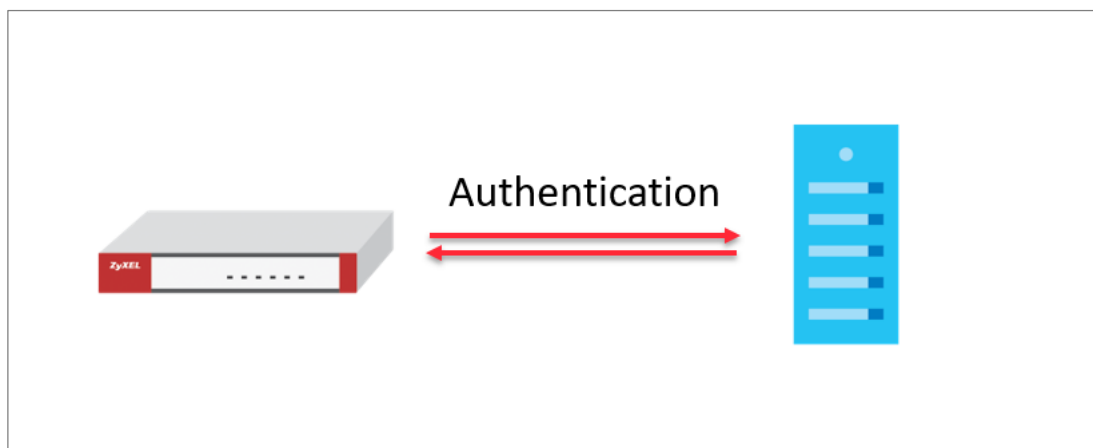
Two-factor Authentication

Authentication Success

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 18:19:57	User	user: vpntestuser[192.168.51.2] is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
2	2024-03-13 18:19:13	SSL VPN	SSL VPN client IP assigned 192.168.51.2	10.214.48.49	0.0.0.0	0	account vpntestuser
3	2024-03-13 18:19:13	SSL VPN	SSL VPN Tunnel established	10.214.48.49	0.0.0.0	0	account vpntestuser
4	2024-03-13 18:19:13	User	User vpntestuser(MAC=) from sslvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpntestuser
5	2024-03-13 18:19:13	SSL VPN	TLS: Username/Password authentication succeeded for username 'vpntestuser' [CN SET]	0.0.0.0	0.0.0.0	0	
6	2024-03-13 18:19:12	User	User vpntestuser(MAC=) from sslvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpntestuser

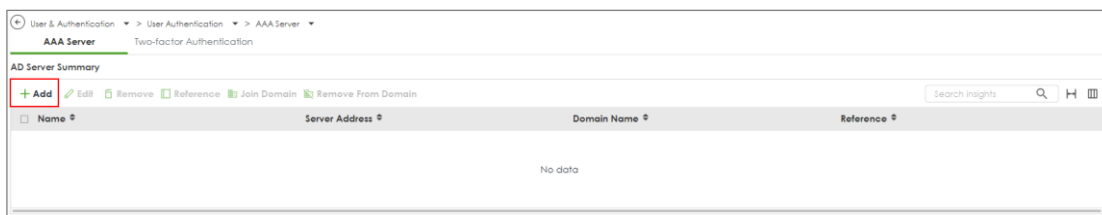
How to set up AD authentication with Microsoft AD

This is an example of using USG FLEX H to configure AD authentication with Microsoft Active Directory(AD). The article briefly explains the parameters for the AD configuration and guides how to join domain to the AD server.



Set Up a profile for AD server

Go to User & Authentication > User Authentication > AAA Server > AD. Click +Add to create a new profile



Enter the Server Address and port for Server settings. (10.214.48.XX:389 in this example). Enter the domain name and the credentials for logging into the AD server, and click Apply.

ZYXEL NETWORKS USG FLEX 100H

Search

Dashboard
Favorites
Traffic Statistics
Security Statistics
Network Status
VPN Status
Licensing
Network
VPN
Security Policy
Object
Security Services
User & Authentication
System
Log & Report
Maintenance

User & Authentication > User Authentication > AAA Server

Configuration

Name: Microsoft_AD
Description: (Optional)

Server Settings

Server Address: 10.214.48.XX (IP or FQDN)
Backup Server Address: (Optional) (IP or FQDN)
Port: 389 (1-65535)
☐ Use SSL
Search time limit: 5 (1-300 seconds)
☒ Case-sensitive User Names

Server Authentication

Domain Name: cso.com
User Name: Administrator
Password:
Retype to Confirm:

Advanced Settings

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

User Name: **Test**

Join Domain

After the profile is created, go to System > DNS & DDNS > DNS, create a domain zone forwarder, and configure the DNS server IP as the IP address for the domain controller.

Domain Zone Forwarder		
+ Add - Remove		
Domain	DNS Server	Query Via
<input type="checkbox"/> cso.com	10.214.48.20	ge1 (WAN)

After the action above, go back to the profile page, tick it and click **Join Domain**

User & Authentication > User Authentication > AAA Server			
AAA Server Two-factor Authentication			
AD Server Summary			
+ Add - Edit - Remove - Reference - Join Domain - Remove From Domain			
Name	Server Address	Domain Name	Reference
<input checked="" type="checkbox"/> Microsoft_AD	10.214.48.20	cso.com	0

Enter NetBIOS Domain Name, Username and Password, click Apply.

User & Authentication > User Authentication > AAA Server		Join AD Domain	
AAA Server Two-factor Authentication		Associated AD Server Object: Microsoft_AD	
AD Server Summary		AD Domain Name: cso.com	
+ Add - Edit - Remove - Reference - Join Domain - Remove From Domain		NetBIOS Domain Name: cso	
Name Server Address Domain Name		User Name: Administrator	
<input checked="" type="checkbox"/> Microsoft_AD 10.214.48.20 cso.com		Password: *****	
LDAP Server Summary		Retype to Confirm: *****	

After join domain successfully, you can see this icon.

User & Authentication > User Authentication > AAA Server			
AAA Server Two-factor Authentication			
AD Server Summary			
+ Add - Edit - Remove - Reference - Join Domain - Remove From Domain			
Name	Server Address	Domain Name	Join Domain
<input type="checkbox"/> Microsoft_AD	10.214.48.20	cso.com	<input checked="" type="checkbox"/>

Test the Result

Scroll down to the bottom of the profile, you will see the Configuration Validation section, using a user account from the server specified above to test if the configuration is correct.

← User & Authentication > User Authentication > AAA Server

Server Authentication

Domain Name	cso.com
User Name	Administrator
Password
Retype to Confirm

Advanced Settings ▾

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

User Name	stanley	Test
-----------	---------	------

Test Status

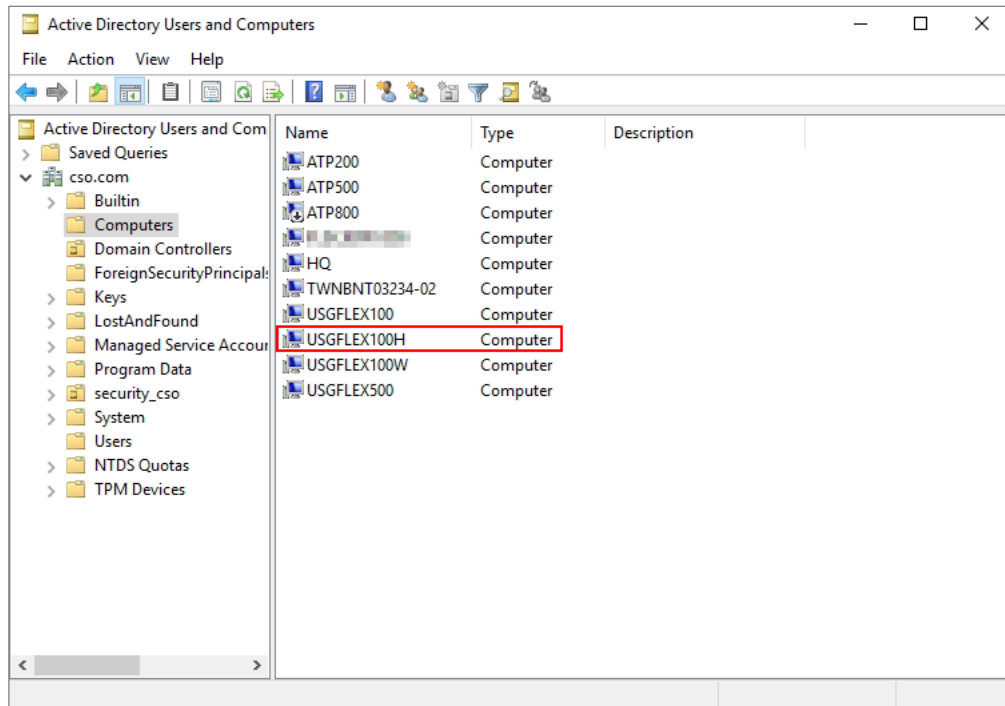
OK

Returned User Attributes

```

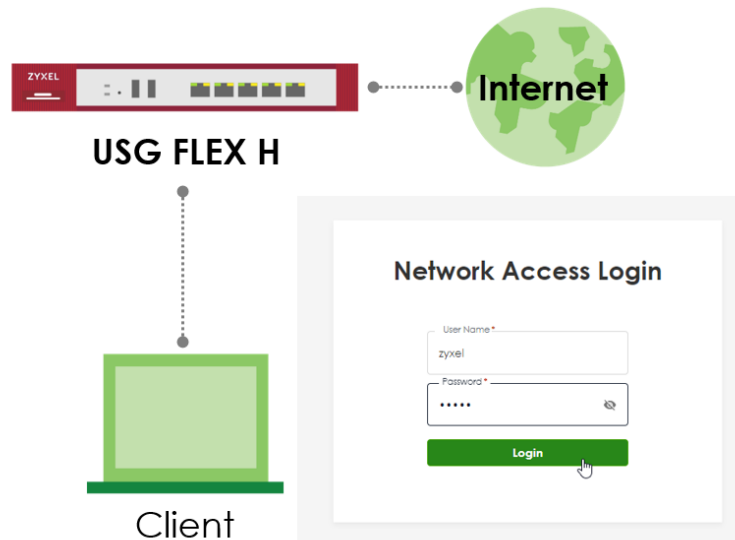
dn: CN=stanley,CN=Users,DC=cso,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: Stanley
distinguishedName: CN=stanley,CN=Users,DC=cso,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: Stanley
    
```


Check **computers** on Microsoft AD, you can see your firewall means join domain successfully.



How to Set Up Captive Portal?

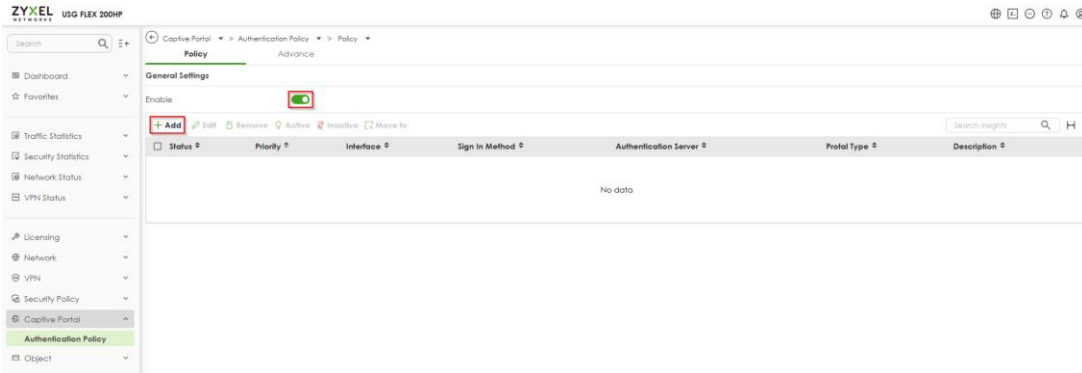
The Captive Portal feature provides functionality that requires LAN client users to complete the authentication procedure of Network Access Login page before accessing the internet. This article will guide users on how to set up and verify this feature.



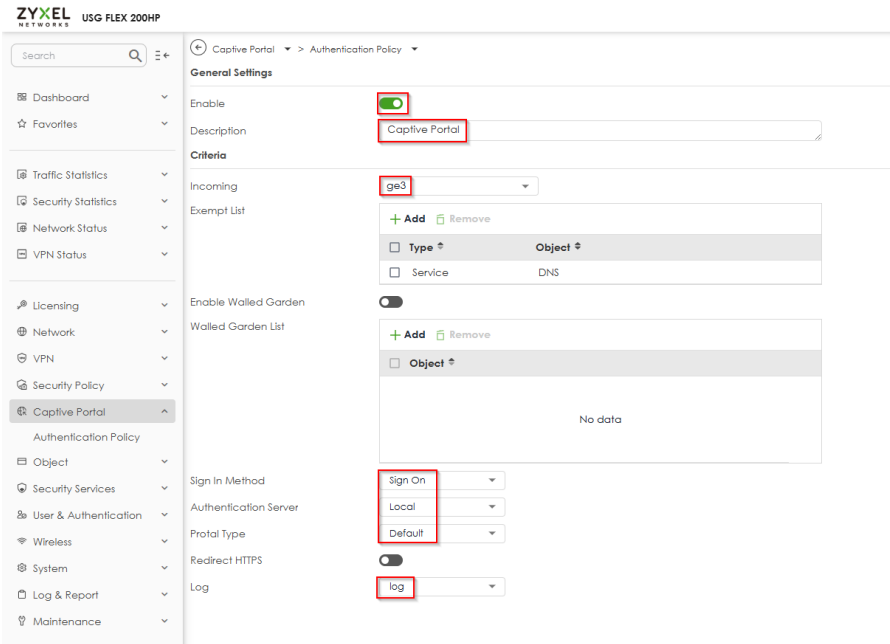
 Note: Captive Portal is supported on USG Flex 100H, USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.32).

Configure the Captive Portal via the Web-GUI

1. **Enable the Captive Portal and add a policy** - Navigate to the Web-GUI path Captive Portal > Authentication Policy > Policy > To enable the **Captive Portal** function and add a policy.



2. **Add an Authentication Policy** – Enable the Authentication Policy, provide a Description, select the Incoming interface, choose the Sign In Method, specify the Authentication Server and Portal Type, and enable Log.



3. **Check the settings** – Ensure the Captive Portal function and the Authentication Policy are enabled.

The screenshot shows the 'Captive Portal' configuration page, specifically the 'Policy' tab under 'Authentication Policy'. The 'General Settings' section has an 'Enable' toggle switch turned on. Below this is a table with columns: Status, Priority, Interface, Sign In Method, Authentication Server, Portal Type, and Description. A single entry is shown with Status 'On', Priority '1', Interface 'ge3', Sign In Method 'sign-on', Authentication Server 'local', Portal Type 'default', and Description 'Captive Portal'.

Status	Priority	Interface	Sign In Method	Authentication Server	Portal Type	Description
On	1	ge3	sign-on	local	default	Captive Portal

4. **Edit the Advance settings** – The default server address is 6.6.6.6, the default HTTP port is set to 1080, and the default HTTPS port is set to 1443.

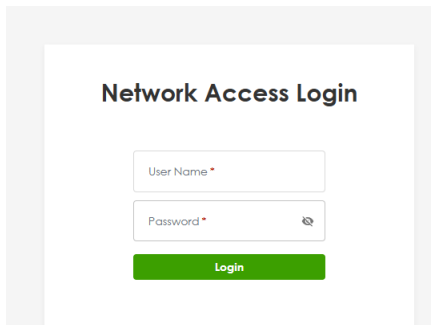
The screenshot shows the 'Captive Portal' configuration page, specifically the 'Advance' tab under 'Authentication Policy'. The 'General Settings' section includes the following fields:

- Server Address: 6.6.6.6 (highlighted with a red box)
- Redirect FQDN: (empty field)
- HTTP: Enabled (toggle switch), HTTP Port: 1080 (highlighted with a red box)
- Redirect HTTPS: Enabled (toggle switch)
- HTTPS: Enabled (toggle switch), HTTPS Port: 1443 (highlighted with a red box)
- Authenticate Client Certificates: Disabled (toggle switch)
- Server Certificate: default (dropdown menu)

Verify the Captive Portal function

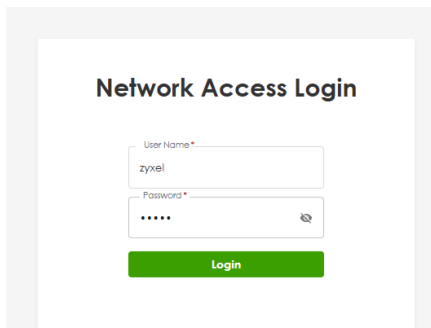
The PC client must complete the authentication process of the Captive Portal before gaining access to the internet.

1. The PC client connects to the LAN port and opens the browser, which will be redirected to the Network Access Login page.



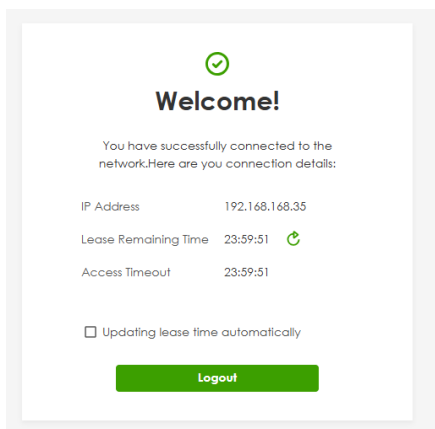
The image shows the 'Network Access Login' page. It has a title 'Network Access Login' at the top. Below the title are two input fields: 'User Name *' and 'Password *'. The 'Password *' field has a small eye icon to its right. Below these fields is a green 'Login' button.

2. Enter the login User Name and Password.




The image shows the 'Network Access Login' page with the 'User Name' field filled with 'zyxel' and the 'Password' field filled with six dots. The green 'Login' button is still visible at the bottom.

3. Once successfully logged into the Network Access Login page, the client will be redirected to the Welcome page, which displays the client's IP address, lease remaining time, and access timeout.

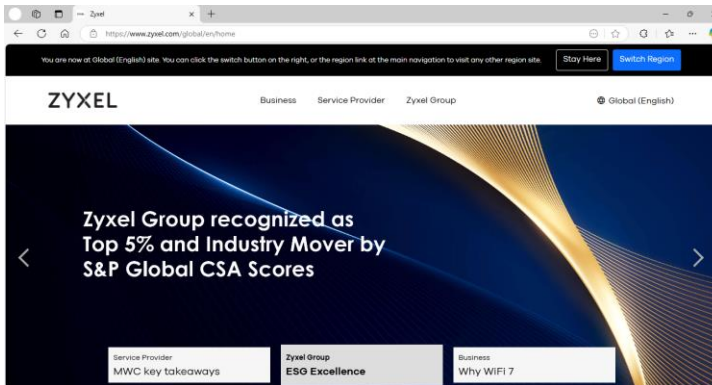


The image shows the 'Welcome!' page. At the top is a green checkmark icon and the text 'Welcome!'. Below this is a message: 'You have successfully connected to the network. Here are your connection details:'. A table follows with connection details:

IP Address	192.168.168.35
Lease Remaining Time	23:59:51 
Access Timeout	23:59:51

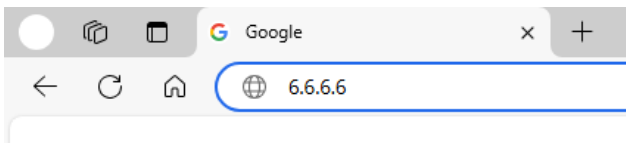
Below the table is a checkbox labeled 'Updating lease time automatically' which is currently unchecked. At the bottom is a green 'Logout' button.

4. Eventually, the client can access the internet normally.

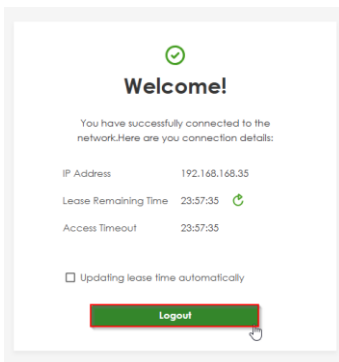


How to logout the Captive Portal?

1. Enter the defined server link. The default link is https://6.6.6.6.



2. Enter the Welcome page and click 'Logout'.



3. Redirect to the Network Access Login page. If the user needs to access the internet, they must re-enter the username and password to complete the Captive Portal authentication process.

Network Access Login

How to check the status?

When the user successfully logs into the Captive Portal page, they can navigate to the GUI path: Network Status > Login Users > Login Users, to check if the user account has already logged into the Captive Portal.

ZYXEL USG FLEX 200HP

Network Status > Login Users > Login Users

Force Log Out

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1	admin	admin	console	0:19:35	console	0.0.0.0	23:40:32	admin(admin)
2	admin	admin	192.168.169.33	0:00:13	http/https	0.0.0.0	23:59:59	admin(admin)
3	zyxel	user	192.168.168.35	0:01:23	captive portal	0.0.0.0	23:56:37	user(zyxel)

They can also navigate to the GUI path: Log & Report > Log / Events > System, to verify the log message indicating that they have successfully logged into the captive portal.

Log & Report > Log / Events > System

System

Category: All Log

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
4	2025-03-17 14:06:37	User	User zyxel(MAC=) from captive portal has logged in Device	192.168.168.35	192.168.168.1	0	Account: zyxel

When the user successfully logs out the Captive Portal page, they can navigate to the GUI path: Log & Report > Log / Events > System, to verify the log message indicating that they have successfully logged out the captive portal.


Log & Report > Log / Events > System

System

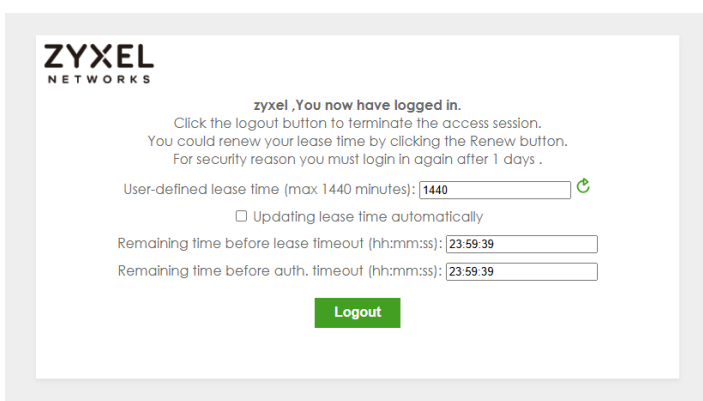
Category: User

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
59	2025-03-17 14:13:34	User	User zyxel from captive portal has logged out Device	192.168.168.35	192.168.168.1	0	Account: zyxel

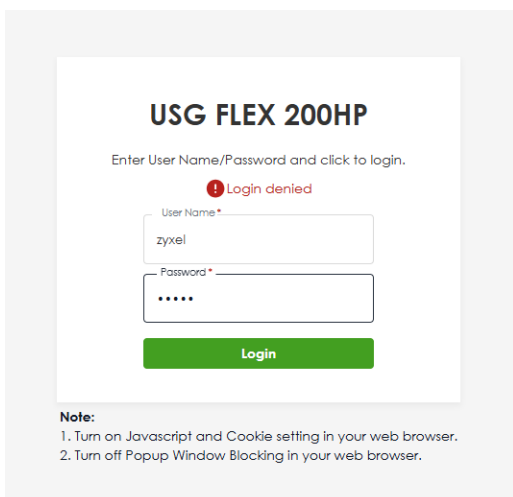
Feature Change:

 Starting from firmware version uOS 1.32, the user must log in to the Captive Portal before using the User Aware function for security policy or BWM policy utilization.

Prior to firmware version uOS 1.32, users were able to successfully log in to the device's GUI link to utilize security policies or BWM policies, as shown below:



Starting from firmware version uOS 1.32, if an account that does not belong to the Local Administrator attempts to log in to the Web-GUI page, access will be denied, as shown below:



Therefore, starting from firmware version uOS 1.32, if users wish to utilize security policies or BWM policies for login users, they need to enable the Captive Portal function. Users

must successfully log in to the Network Access Login page to activate the security or BWM policies, as show in below:

The user successfully logged in to the Network Access Login page.

The screenshot shows the 'Network Access Login' page. It has a 'User Name' field with 'zyxel' entered and a 'Password' field with masked characters. A green 'Login' button is at the bottom.

The screenshot shows the 'Welcome!' page with a green checkmark icon. It displays connection details: IP Address 192.168.168.35, Lease Remaining Time 23:57:35, and Access Timeout 23:57:35. There is a checkbox for 'Updating lease time automatically' and a green 'Logout' button.

They can then activate the security or BWM policies for the specific user account.

Security Policy

>

Policy Control

General Settings

Enable

Configuration

Allow Asymmetrical Route

+ Add

Edit

Remove

Active

Inactive

Move to

Copy to

Search insights

Status	Pri.	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Hits	Profile
<input type="checkbox"/>	1	For_The_User	LAN	any (Excluding ZyWALL)	any	any	any	zyxel	none	allow	no	3	

Network

>

BWM

General Settings

Enable

Configuration

+ Add

Edit

Remove

Active

Inactive

Move to

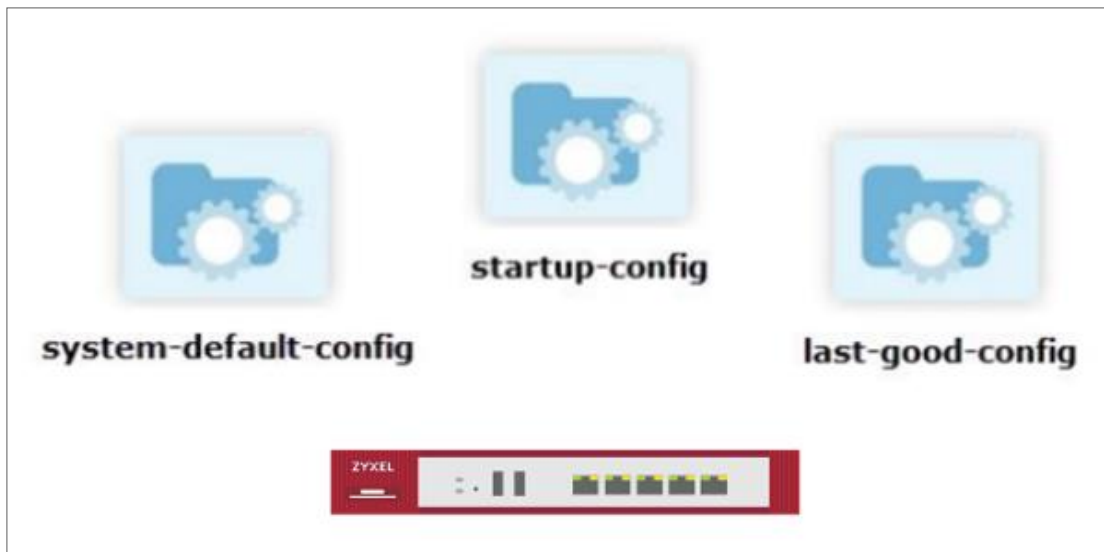
Search insights

Status	Pri.	Name	Description	User	Incoming Interface	Outgoing Interface	Source	Destination	Service	BWM Download/Upload/Pri
<input type="checkbox"/>		Default		any	any	any	any	any		no/no/7
<input checked="" type="checkbox"/>	1	For_The_User		zyxel	ge3	ge1	any	any	any	0/0/4

Chapter 4- Maintenance

How to Manage Configuration Files

This is an example of how to rename, download, copy, apply and upload configuration files. Once your USG FLEX H device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.



 **Note:** The **system-default.conf** file contains the ZyWALL default settings. This configuration file is included when you upload a firmware package.

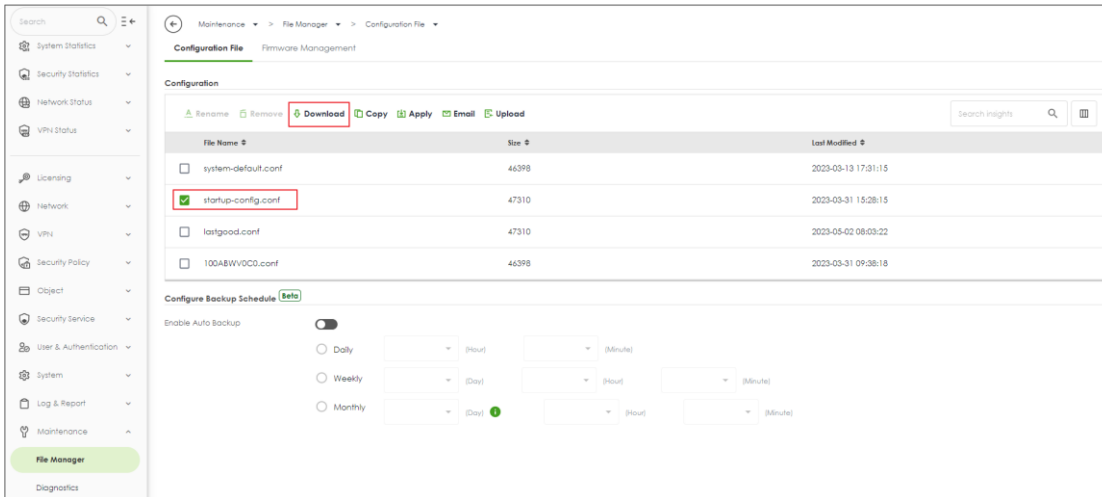
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

Download the Configuration Files

Maintenance > File Manager > Configuration File

Select the startup-config.conf and click "Download".

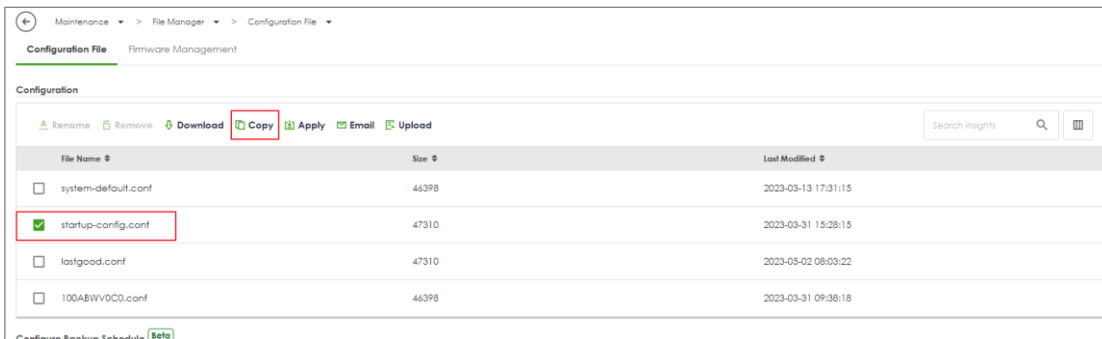


The screenshot shows the ZyXel File Manager interface. On the left is a sidebar with navigation options: System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, Log & Report, Maintenance, File Manager (highlighted), and Diagnostics. The main area is titled 'Configuration File' under 'Firmware Management'. It features a toolbar with icons for Rename, Remove, Download (highlighted in red), Copy, Apply, Email, and Upload. Below the toolbar is a table with columns 'File Name', 'Size', and 'Last Modified'. The table contains four rows: 'system-default.conf' (46398 bytes, 2023-03-13 17:31:15), 'startup-config.conf' (47310 bytes, 2023-03-31 15:28:15, selected with a green checkmark), 'lastgood.conf' (47310 bytes, 2023-05-02 08:03:22), and '100ABWVOC0.conf' (46398 bytes, 2023-03-31 09:38:18). Below the table is a 'Configure Backup Schedule' section with a 'Beta' tag and options for 'Enable Auto Backup' (Daily, Weekly, Monthly) with corresponding time settings.

Copy the Configuration Files

Maintenance > File Manager > Configuration File

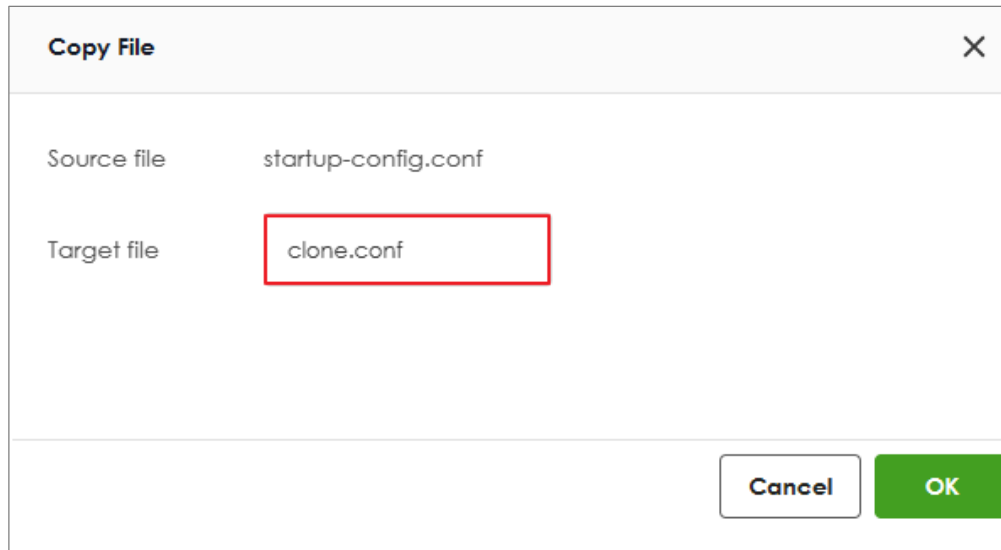
Select the file and click "Copy".



This screenshot is identical to the one above, showing the ZyXel File Manager interface. The 'Copy' button in the toolbar is highlighted in red, and the 'startup-config.conf' file in the table is selected with a green checkmark. The rest of the interface, including the sidebar and the 'Configure Backup Schedule' section, remains the same.

A pop-up screen will appear allowing you to edit the Target file name.

The file as format: [a-zA-Z0-9~_.-]{1,63}.conf

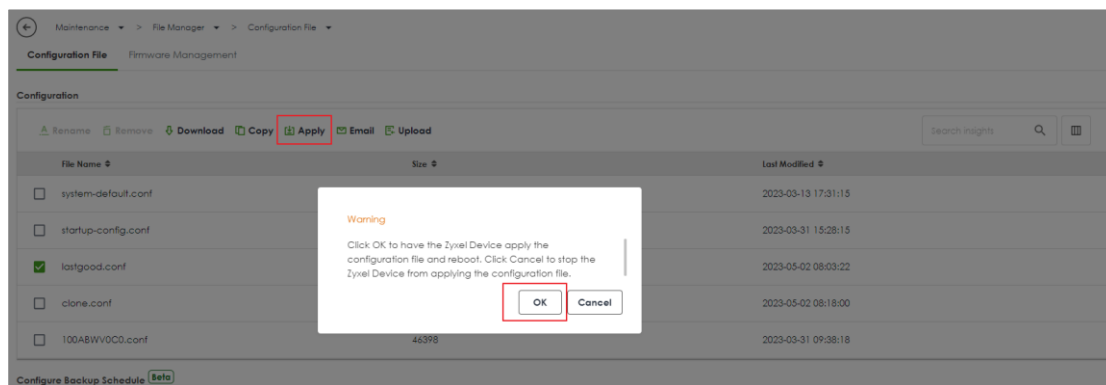


The image shows a 'Copy File' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Source file' with the value 'startup-config.conf' and 'Target file' with the value 'clone.conf'. The 'Target file' field is highlighted with a red rectangular border. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Apply the Configuration Files

Maintenance > File Manager > Configuration File

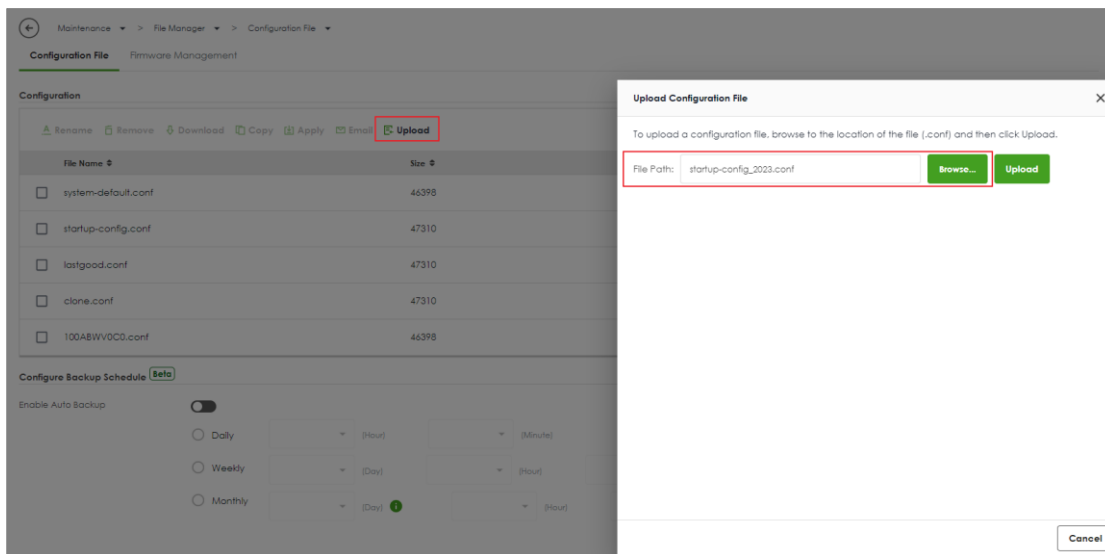
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when the device last restarted. If you uploaded and applied a configuration file with an error, select this file then click **Apply** to return the valid configuration. Click "OK", ZyWALL will reboot automatically.



Upload the Configuration Files

Maintenance > File Manager > Configuration File

Select Upload and Browse a new or previously saved configuration file from your computer to the USG FLEX H device. You cannot upload a configuration file which has the same name in the device.




How to Manage Firmware

For management convenience, administrators have the capability to upgrade the firmware effortlessly either from a PC or using the cloud firmware upgrade function. Additionally, the firmware upgrade can be scheduled to occur automatically within a preconfigured timeframe.

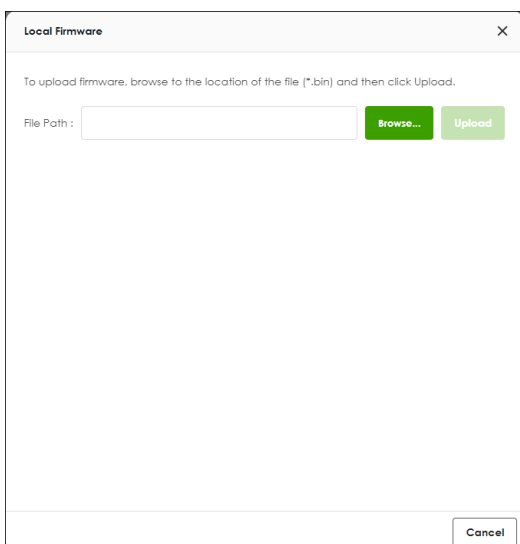
Local Firmware Upgrade

You can click the green button to upgrade firmware by browsing the .bin file from your PC.

 Note: You can download the latest firmware version from myZyxel.com portal.
(<https://portal.myzyxel.com/my/firmwares>)



Status	Model	Version	Release Date	Action
Running	USG FLEX 200H	V1.10(ABVV.0)	2023-05-05 20:01:57	



Local Firmware

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path : Browse... Upload

Cancel

Cloud Firmware Upgrade

The cloud firmware upgrade function allows you to verify the most recent firmware version by clicking the "Check New" button.

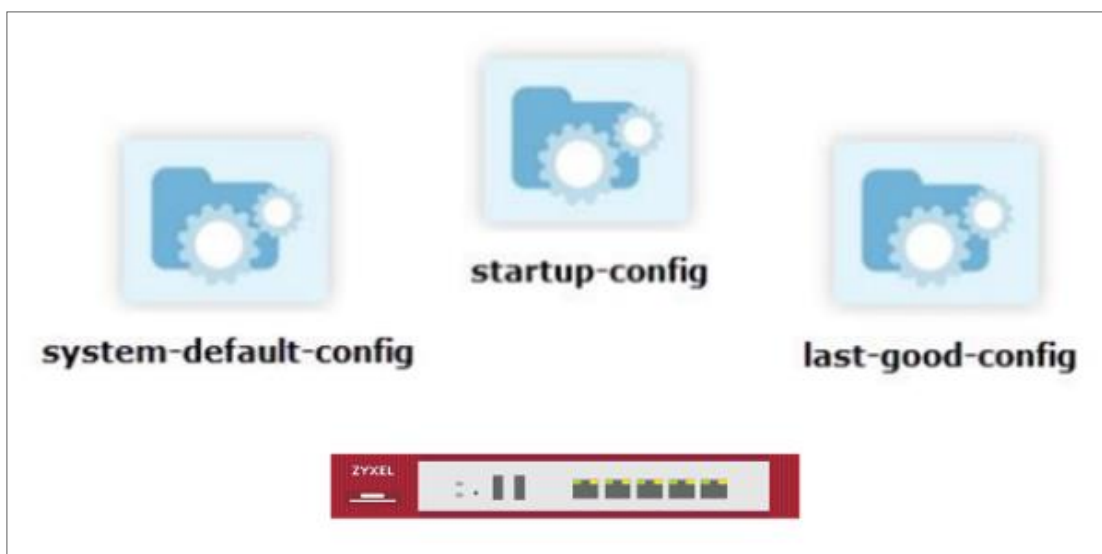
Furthermore, the "Auto Update" feature can be activated to automatically download firmware to your firewall first and reboot your device within a specified time frame.


Cloud Firmware Information

Latest Version	None	<div>Check Now</div>
Release Date	None	
Auto Update	<div> <input checked="" type="checkbox"/> </div> <div> <input type="radio"/> Daily <div> <div></div> <div></div> </div> <div>(Hour)</div> </div> <div> <input type="radio"/> Weekly <div> <div></div> <div></div> </div> <div>(Day)</div> <div> <div></div> <div></div> </div> <div>(Hour)</div> </div>	
<div>Auto Reboot</div> <div> <input type="checkbox"/> </div>		

How to set up configuration file backup rotation

In enterprise network environments, the integrity and availability of device configurations are critical to maintaining stable operations. To mitigate the risks associated with frequent configuration changes and human error, Zyxel uOS offers a Configuration Backup Rotation mechanism. This feature automatically retains the most recent configuration files while removing the oldest ones, enabling efficient storage management and reducing maintenance efforts. This document is intended to explain the principles, configuration methods, and limitations of the backup rotation function. It aims to assist network administrators in planning effective backup strategies and improving the automation and reliability of routine operations. With this feature, users can ensure that, even in the event of a misconfiguration or failure, the system can quickly revert to a known good state—minimizing downtime and maintaining a stable, resilient network infrastructure.

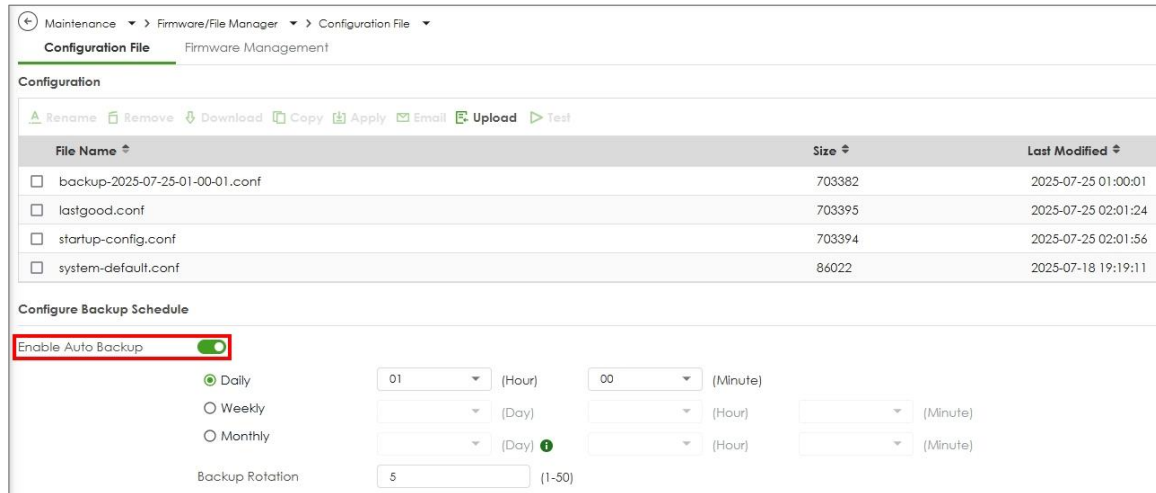


 **Note:** The **system-default.conf** file contains the default settings. This configuration file is included when you upload a firmware package.

The **startup-config.conf** file is the configuration file that the Firewall is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

Go to Configuration Backup Schedule section and enable “Enable Auto Backup”.



Maintenance > Firmware/File Manager > Configuration File

Configuration File Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

File Name	Size	Last Modified
<input type="checkbox"/> backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
<input type="checkbox"/> lastgood.conf	703395	2025-07-25 02:01:24
<input type="checkbox"/> startup-config.conf	703394	2025-07-25 02:01:56
<input type="checkbox"/> system-default.conf	86022	2025-07-18 19:19:11

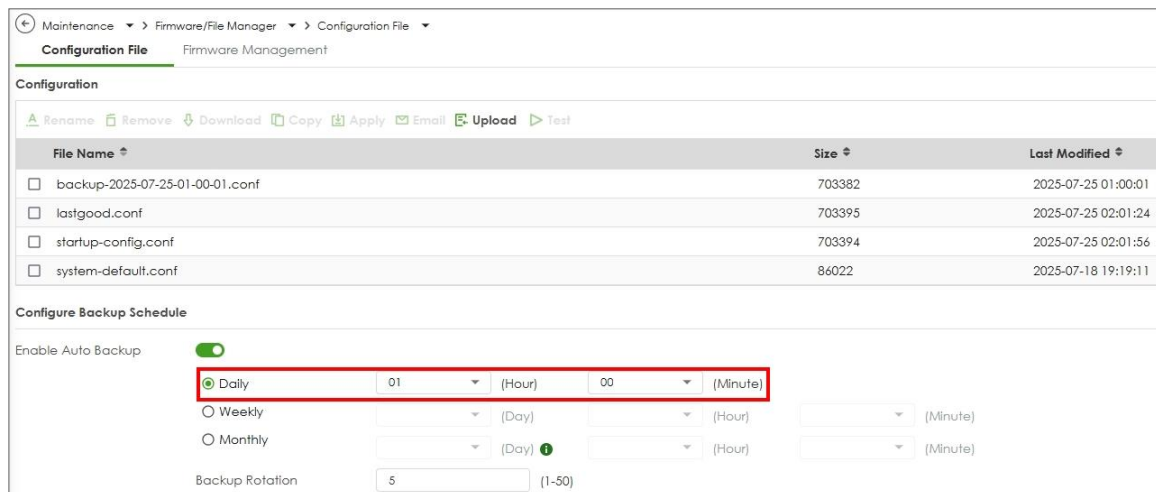
Configure Backup Schedule

Enable Auto Backup ☒

☒ Daily 01 (Hour) 00 (Minute)
☐ Weekly (Day) (Hour) (Minute)
☐ Monthly (Day) (Hour) (Minute)

Backup Rotation 5 (1-50)

You can select the backup cycle based on your requirements. In this guide, we select daily backup and set the time to 01:00.



Maintenance > Firmware/File Manager > Configuration File

Configuration File Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

File Name	Size	Last Modified
<input type="checkbox"/> backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
<input type="checkbox"/> lastgood.conf	703395	2025-07-25 02:01:24
<input type="checkbox"/> startup-config.conf	703394	2025-07-25 02:01:56
<input type="checkbox"/> system-default.conf	86022	2025-07-18 19:19:11

Configure Backup Schedule

Enable Auto Backup ☒

☒ Daily 01 (Hour) 00 (Minute)
☐ Weekly (Day) (Hour) (Minute)
☐ Monthly (Day) (Hour) (Minute)

Backup Rotation 5 (1-50)

After Enabling auto backup, the backup rotation feature becomes available. The maximum number of auto backup configuration files is 50. In this example, we set 5 for rotation.

Maintenance > Firmware/File Manager > Configuration File

Configuration File Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

File Name	Size	Last Modified
<input type="checkbox"/> backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
<input type="checkbox"/> lastgood.conf	703395	2025-07-25 02:01:24
<input type="checkbox"/> startup-config.conf	703394	2025-07-25 02:01:56
<input type="checkbox"/> system-default.conf	86022	2025-07-18 19:19:11

Configure Backup Schedule

Enable Auto Backup ☒

☒ Daily 01 (Hour) 00 (Minute)
☐ Weekly (Day) (Hour) (Minute)
☐ Monthly (Day) (Hour) (Minute)

Backup Rotation 5 (1-50)

Note: By default, the system allows up to 65 backup files, with a maximum total size of 200 MB.

Verification

Maintenance > File Manager > Configuration File

Five scheduled backup configurations are generated based on the scheduled backup settings. The firewall has automatically backed up five files, and it deletes the oldest file before performing an automatic backup.

Maintenance > Firmware/File Manager > Configuration File





Configuration File Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

File Name	Size
<input type="checkbox"/> backup-2025-07-25-01-00-01.conf	703382
<input type="checkbox"/> backup-2025-07-26-01-00-01.conf	703382
<input type="checkbox"/> backup-2025-07-27-01-00-01.conf	703382
<input type="checkbox"/> backup-2025-07-28-01-00-01.conf	703382
<input type="checkbox"/> backup-2025-07-29-01-00-01.conf	703382
<input type="checkbox"/> lastgood.conf	703395
<input type="checkbox"/> startup-config.conf	703473
<input type="checkbox"/> system-default.conf	86022

If the Auto Backup total size limit is reached, no new files will be generated, and backup rotation will not remove old files. The following event will be recorded in the Event log.

System		APC	AP				
Category System		Clear Log Export Refresh		<div>Search Insights</div> <div></div>			
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
11	2025-07-17 16:16:01	System	Configuration backup error: total size of all configuration files exceeds the maximum limit	0.0.0.0	0.0.0.0	0	
34	2025-07-17 15:48:16	System	Geo-IP country database version 20250713 update has succeeded.	0.0.0.0	0.0.0.0	0	

If the Auto Backup maximum file number is reached, no new files will be generated, and backup rotation will not remove old files. The following event will be recorded in the Event log.

System		APC	AP				
Category System		Clear Log Export Refresh		<div>Search Insights </div> <div> </div>			
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
0	2025-07-17 14:30:01	System	Configuration backup error: maximum number of configuration files exceed ed	0.0.0.0	0.0.0.0	0	

Chapter 5- Others

How to Setup and Configure Daily Report

Administrators can efficiently oversee gateway events by reviewing the Daily Report for management purposes. This example demonstrates how to set up the Daily Report, including the option to select specific log messages for inclusion. Once configured, you can utilize "Send Report Now" to assess your device's current status and establish a schedule for receiving the report.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Mail Server

Before setting up the Email Daily Report, we will be required to set up a mail server.

Navigate to the System > Notification > Mail Server. Input your Mail Server and port, and activate TLS Security and STARTTLS in their respective fields. Next, complete your account and password for SMTP Authentication as the Sender.

←

System > Notification > Mail Server

Mail Server

Alert

General Settings

Mail Server

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Port

587

(1-65535)

TLS Security

☒

STARTTLS

☒

Authenticate Server

☐

SMTP Authentication

☒

User Name

9@gmail.com

Password

.....

Retype

.....

Mail Server Test

Mail To

(Email Address)

Send From

(Email Address)

Mail Now

You can verify the correctness of the settings by using the Mail Server Test below. If it is successful, you will receive an email.

Mail Server Test

Mail To

gmail.com

(Email Address)

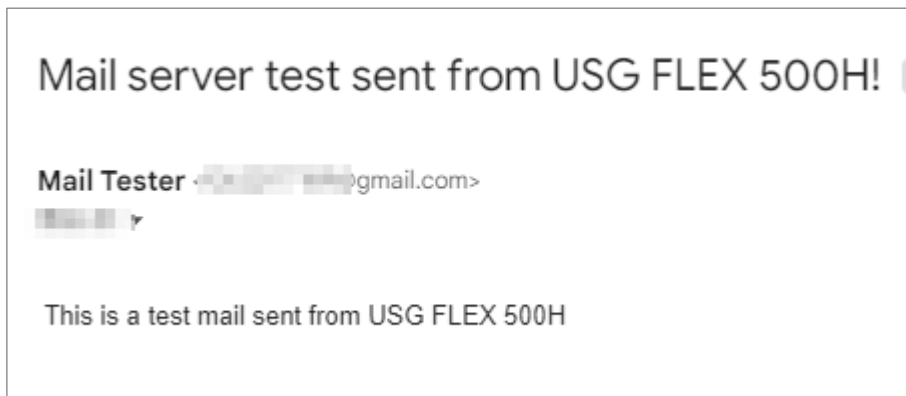
Send From

@gmail.com

(Email Address)

Mail Now

SUCCESS



Set Up Email Daily Report

Navigate to Log & Report > Email Daily Report. Enable your Email Daily Report

←

Log & Report ▾

>

Email Daily Report ▾


General Settings

Enable Email Daily Report

☒

Type your Email Subject and your Sender and Receiver in the field.

Email Settings

 **Note**
Please set up the **Mail Server** to send system statistics via email every day.

E-mail Subject

500H-Daily-Report

☒ Append system name
☒ Append date time

Email from

gmail.com

Email to

mail.com

(Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

Scroll down the page and go to Report Items to set up which messages you would like to include in the daily report

Report Items

System Resource Usage
☒ CPU Usage
☒ Interface Usage
☒ Memory Usage
☒ Port Usage
☒ Session Usage

Security Services
☒ Anti-Malware
☒ App Patrol
☒ Content Filter
☒ IPS
☒ Reputation Filter

System Information
☒ DHCP Table

You can set up a Schedule at the bottom of the page

Schedule

Time For Sending Report

04

(Hour)

00

(Minute)

Test the Email Daily Report

To confirm if the daily report has been set up successfully, click "Send Report Now."

Email Settings

Note

Please set up the **Mail Server** to send system statistics via email every day.

E-mail Subject

500H-Daily-Report

☒ Append system name

☒ Append date time

Email from

@gmail.com

Email to

@gmail.com (Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

Send Report Now

f

@gmail.com

下午3:41

ZYXEL NETWORKS

General

Model Name:

USG FLEX 500H

Firmware Version:

V1.10(AB2H.0)b7s1 | 2023-08-17 15:35:54

MAC Address Range:

08:00:27:00:00:00 - 08:00:27:00:00:00

System Uptime:

10 days, 22:37:53

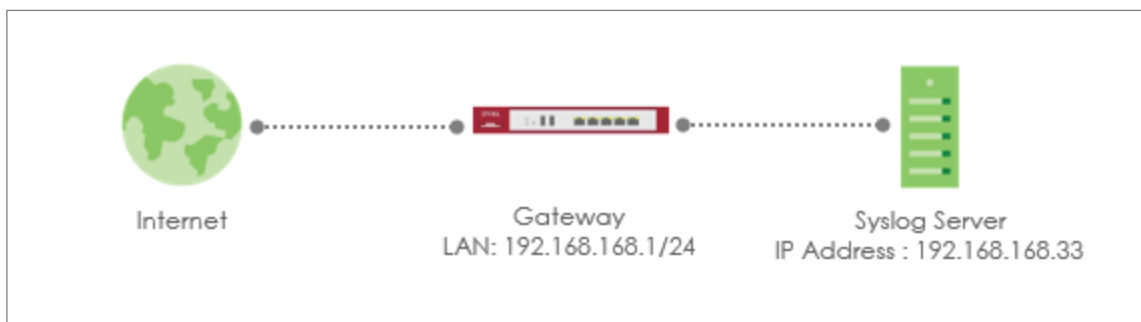
System Name:


usgflex500h

System Resource Usage

How to Setup and Send Logs to a Syslog Server

For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system logs.



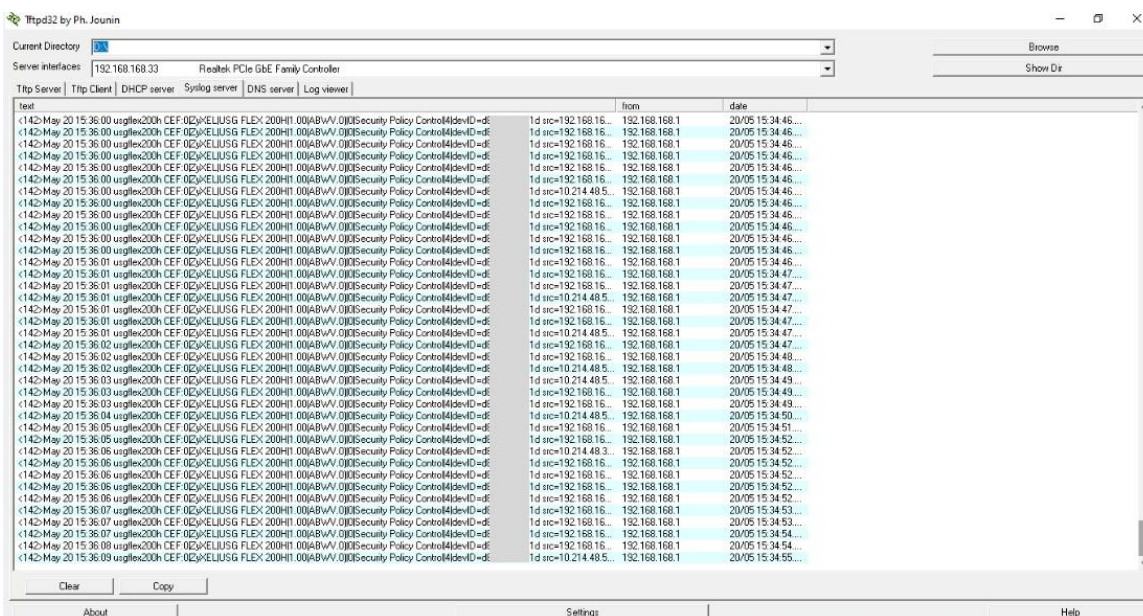
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Go to Log & Report > Log Settings > Remote Syslog Server. Set Log Format to be CEF/Syslog and type the server name or the IP address of the syslog server. Turn on "Active" to send log information to the server.

Remote Server 1	Remote Server 2	
Active	<input checked="" type="checkbox"/>	
Log Format	CEF/Syslog	
Server Address	192.168.168.33	(Server Name or IP Address)
Server Port	514	
Log Facility	Local 1	


Test the Remote Syslog Server

Check logs on the syslog server.



How to Setup and Send logs to the USB storage

The USG FLEX H Series device can use a connected USB device to store the system log and other diagnostic information. This example shows how to use the USB device to store the system log information.

 **Note:** The USB storage must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10). The USB port can provide max. 900mA output power. You might need to connect external power for the USB storage device.

USB Storage device

Plug in an external USB storage device. USB storage devices with FAT16, FAT32, EXT2, or EXT3 file systems are supported to be connected to the USB port of the gateway.

Set Up the USB storage on the Gateway

Go to Log & Report > Log Settings > Log Category Setting. Use the drop-down list to select what information you want to log from each log category.

Log Category Setting

Category	System Log			USB Storage			Remote Server 1			Remote Server 2			Count
<div><div></div><div></div></div>	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	
> Authenticate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	3
▼ Security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
Security Policy Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
DoS Prevention	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> Security Service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> VPN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> License	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0

Go to Log & Report > Log Settings > USB Storage. Turn on "Enable USB storage" to store the system logs on a USB device.

System Log

Log Consolidation ☐

Consolidation Interval (10 Seconds - 600 Seconds)

USB Storage

Enable USB storage ☒

Log Keep Duration ☐

Check the USG Log Files

Go to Maintenance > Diagnostics > System Log. Select a file and click "Download" to view the log.

System Log Archives in USB Storage

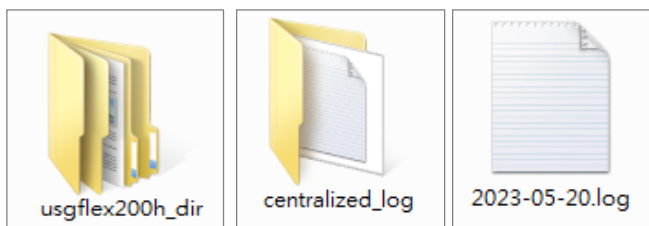
Remove Download Search insights

File Name	Size	Modified Time
2023-05-20.log	9708	May 20 16:47

You can also connect the USB storage to PC and find the files in the following path.


\\Model

Name_dir\centralized_log\YYYY-MM-DD.log



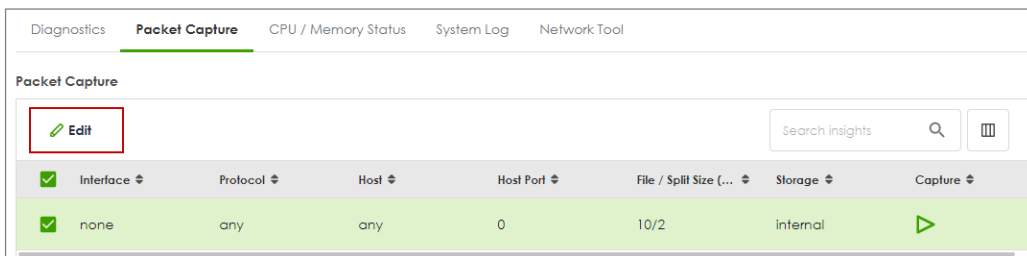
How to Perform and Use the Packet Capture Feature

This example shows how to use the Packet Capture feature to capture network traffic going through the device's interfaces. Studying these packet captures may help you analyze network problems.

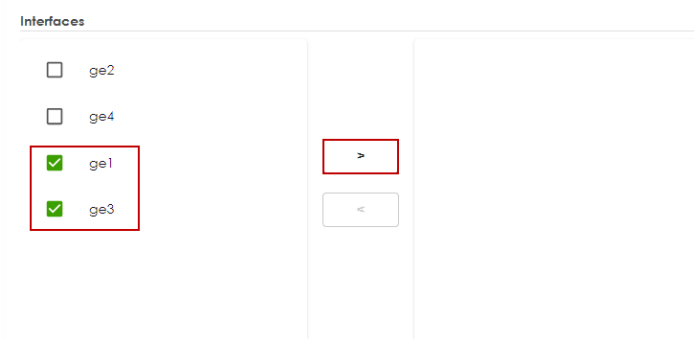
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the Packet Capture Feature

5. Go to Maintenance > Diagnostics > Packet Capture. Select "none" and click "Edit".



6. In Interfaces, select interfaces for which to capture packets and click the right arrow button to move them to the list.



7. In Filter, select IP Version for which to capture packets. Select any to capture packets for all IP versions.

Select the Protocol Type of traffic for which to capture packets. Select any to capture packets for all types of traffic.

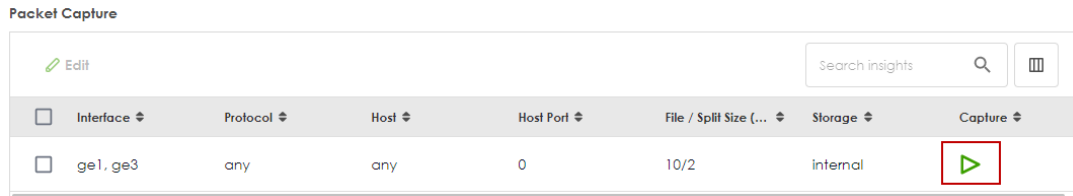
Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

Filter	
IP Version	any ▼
Protocol Type	any ▼
Host IP	any (IPv4 address or any)
Host Port	0 (0: any)

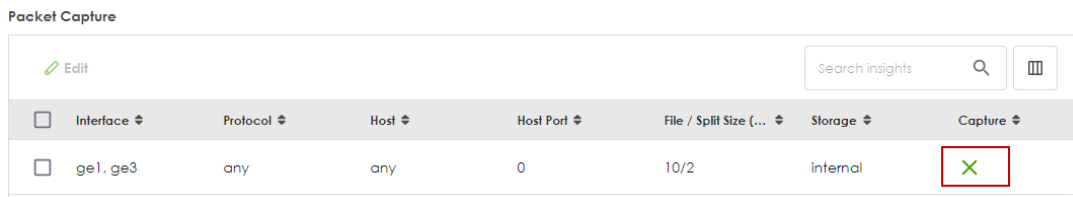
8. In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".

Misc setting	
Captured Packet Files	10 MB
Split threshold	2 MB
Duration	0 (0:unlimited)
File Suffix	-packet-capture
Number of Bytes to Capture (Per Pack...	1514 Bytes
<input checked="" type="radio"/> Save data to onboard storage only <input type="radio"/> Save data to USB storage <input type="radio"/> Save data to ftp server	

9. Click the icon to start capturing packets.

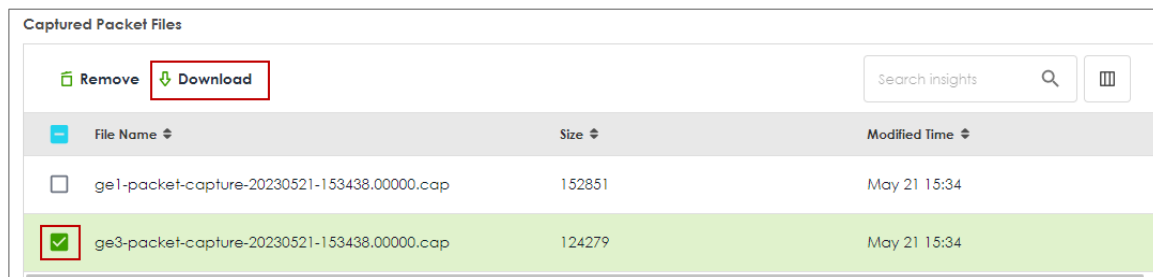


10. Click the icon to stop capturing packets.



Download the Captured Packet Files

In Captured Packet Files, select the file and click Download. You can download one file only at once. The captured files are named according to the date and time of capture, so new files will not overwrite existing ones.



Check Real-Time traffic using command

Traffic-capture is a CLI-based packet capturing tool on the device. It can be used to sniff and analyze network traffic by intercepting and displaying packets transmitted in the network interface.

Syntax:

cmd traffic-capture <interface name>

cmd traffic-capture <interface name> filter <icmp|tcp|udp|arp|esp>

cmd traffic-capture <interface name> filter "src <ip address>"

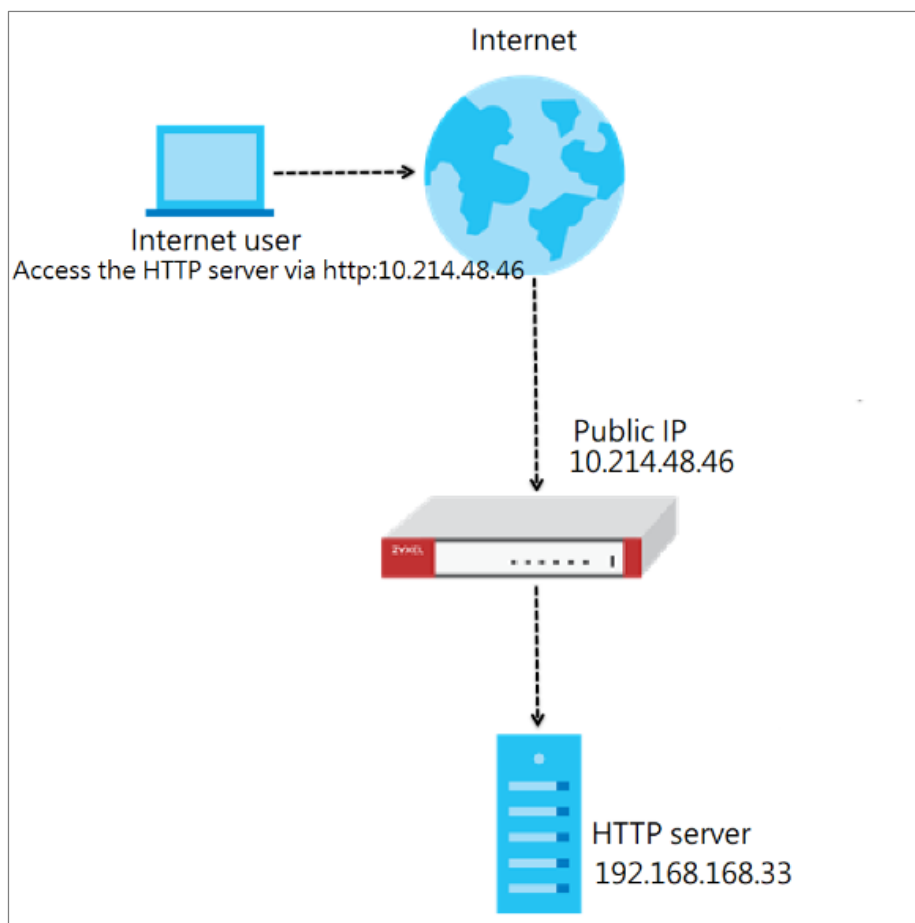
cmd traffic-capture <interface name> filter "port <port number>"

cmd traffic-capture <interface name> filter "host <ip address> and port <port number>"

```
usgflex200h> cmd traffic-capture ge3 filter "src 192.168.168.33"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:07:36.738176 [redacted] > [redacted], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.738249 [redacted] > [redacted], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.739617 [redacted] > [redacted], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.lo
cal. (35)
16:07:36.739654 [redacted] > [redacted], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.lo
cal. (35)
16:07:37.066145 [redacted] > [redacted], ethertype IPv4 (0x0800),
length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 478, length
40
^CNetconf RPC interrupted.
```


How to Allow Public Access to a Server Behind USG FLEX H

Here is an example of allowing access to the internal server behind a USG FLEX H device with network address translation (NAT). Internet users can access the server directly by its public IP address and a NAT rule will forward traffic from the internet to the local server in the intranet.



Set Up the NAT

Go to Network > NAT, and click +Add to create a NAT rule.

- Input the rule name
- select Virtual Server
- Incoming Interface: ge1
- Configure the Source IP to limit the access by the Source IP. You may select Any
- Configure the External IP. Select Any to choose the ge1 interface IP as the external IP.
- Configure the internal IP. Click +Add Object to create an address object as a host 192.168.168.33 which is the IP address of the internal server.

The screenshot shows the ZyXel NAT configuration interface. The 'Mapping Rule' section is active, with the 'Virtual Server' classification selected. The 'Incoming Interface' is set to 'ge1'. The 'Source IP' is set to 'any'. The 'External IP' is set to 'any'. The 'Internal IP' is set to 'user defined', and a red box highlights the '+ Add Object' button in the 'Select Address' dialog. The 'Port Mapping Type' is set to 'any'. The 'Related Settings' section shows 'Enable NAT Loopback' as a toggle switch.

- Port Mapping Type: Select HTTP for both external and internal service.

←
Network
>
NAT
▼

General Settings

Enable Rule ☒


Rule Name internal_server


Port Mapping Type


Classification ☒ Virtual Server ☐ 1:1 NAT ☐ Many 1:1 NAT

Mapping Rule

Incoming Interface ge1 ▼

Source IP any 

External IP user defined  10.214.48.46

Internal IP internal_server 

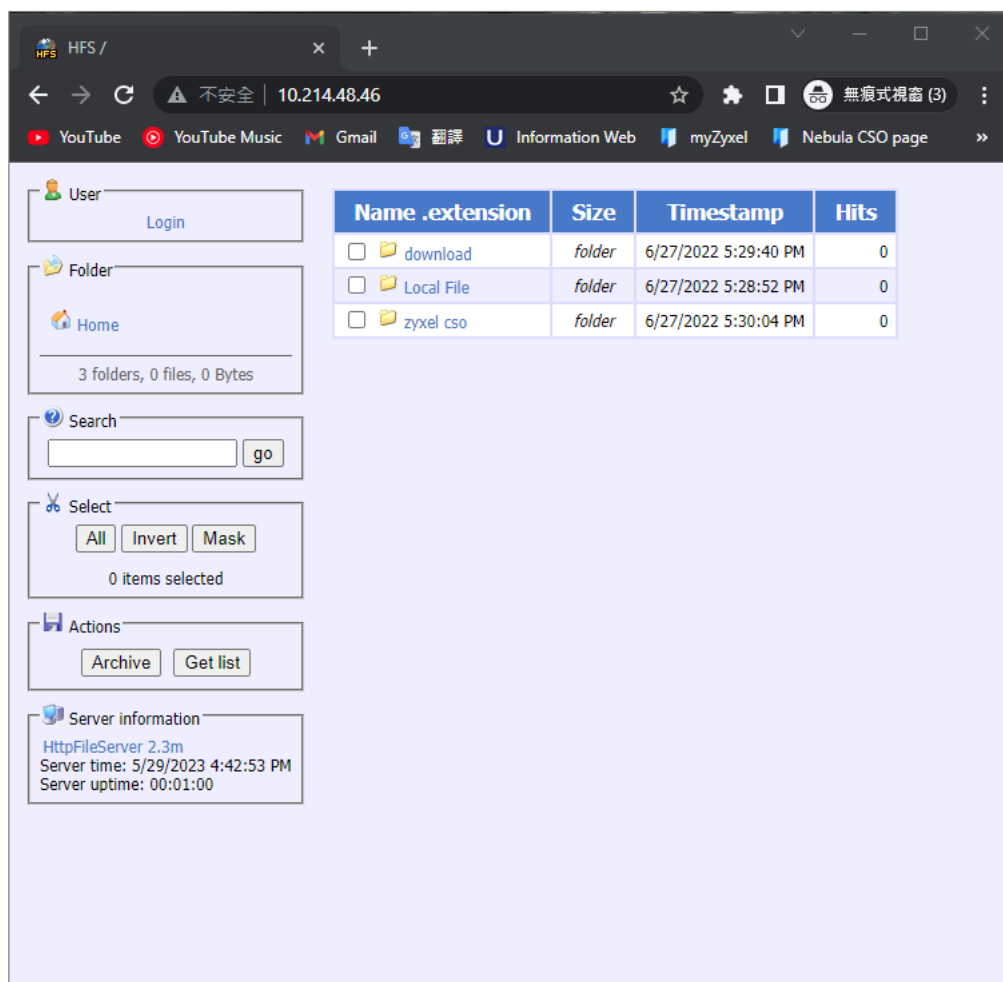
Port Mapping Type Service ▼

External Service HTTP ▼

Internal Service HTTP ▼

Test the Result

Type `http://10.214.48.46` into the browser, and it display the HTTP service page.



The screenshot shows a web browser window with the address bar displaying `10.214.48.46`. The page title is "HFS /". The interface is divided into a sidebar on the left and a main content area on the right.

Sidebar:

- User:** Login
- Folder:** Home (3 folders, 0 files, 0 Bytes)
- Search:** Search bar with a "go" button.
- Select:** All, Invert, Mask (0 items selected)
- Actions:** Archive, Get list
- Server information:**
 - HttpFileServer 2.3m
 - Server time: 5/29/2023 4:42:53 PM
 - Server uptime: 00:01:00

Main Content Area:

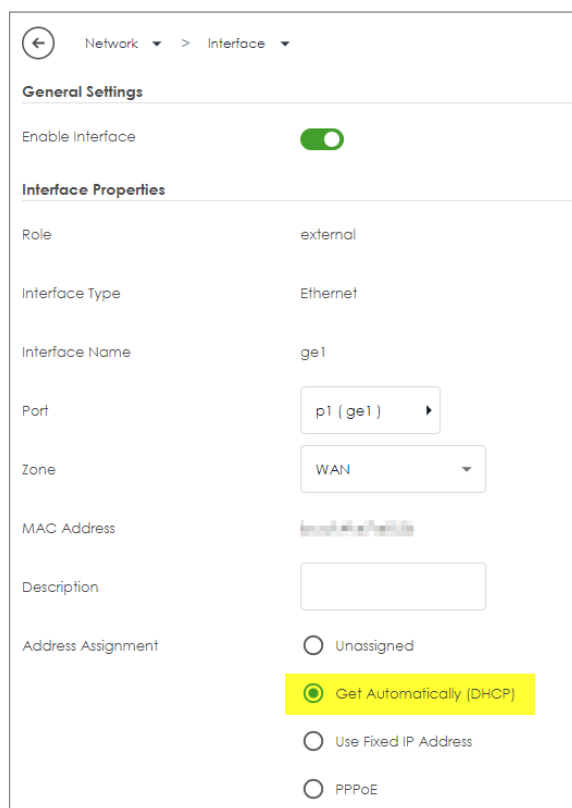
Name	.extension	Size	Timestamp	Hits
<input type="checkbox"/>	download	folder	6/27/2022 5:29:40 PM	0
<input type="checkbox"/>	Local File	folder	6/27/2022 5:28:52 PM	0
<input type="checkbox"/>	zyxel cso	folder	6/27/2022 5:30:04 PM	0

How to Configure DHCP Option 60 – Vendor Class Identifier

USG FLEX H series supports DHCP option 60. By VCI string matching, a DHCP client can select a specific DHCP server within the WAN network. This feature proves beneficial in network environments where multiple DHCP servers offer services. Clients that need Internet service can be directed to the DHCP server that provides corresponding Internet connection details via the identical option 60 string. On the other hand, IPTV clients can relay to another DHCP server for obtaining IPTV service information.

Set Up DHCP 60 on the USG FLEX H

1. Go to Network > Interface > External, and edit the WAN interface.
2. Make sure the WAN interface is set as a DHCP client. Select **Get Automatically (DHCP)** for Address Assignment.



The screenshot shows the configuration page for the WAN interface. The breadcrumb navigation at the top indicates the path: Network > Interface > External. The page is divided into two main sections: 'General Settings' and 'Interface Properties'.

General Settings:

- Enable Interface:** A toggle switch is turned on (green).

Interface Properties:

- Role:** external
- Interface Type:** Ethernet
- Interface Name:** ge1
- Port:** p1 (ge1)
- Zone:** WAN
- MAC Address:** [Randomly generated MAC address]
- Description:** [Empty text box]
- Address Assignment:**
 - ☐ Unassigned
 - ☒ Get Automatically (DHCP)
 - ☐ Use Fixed IP Address
 - ☐ PPPoE

3. Scroll down and expand the Advanced Settings: DHCP Option 60
4. Enter the VCI string in the field of DHCP Option 60, and click **Apply**

Advanced Settings

DHCP Option 60

CSO-FAQ

MTU

Default SNAT

☒

Test DHCP Option 60

To check the functionality of DHCP Option 60, we can use packet capture software to check if option 60 string exists in the DHCP discover message that is sent from the USG FLEX H.

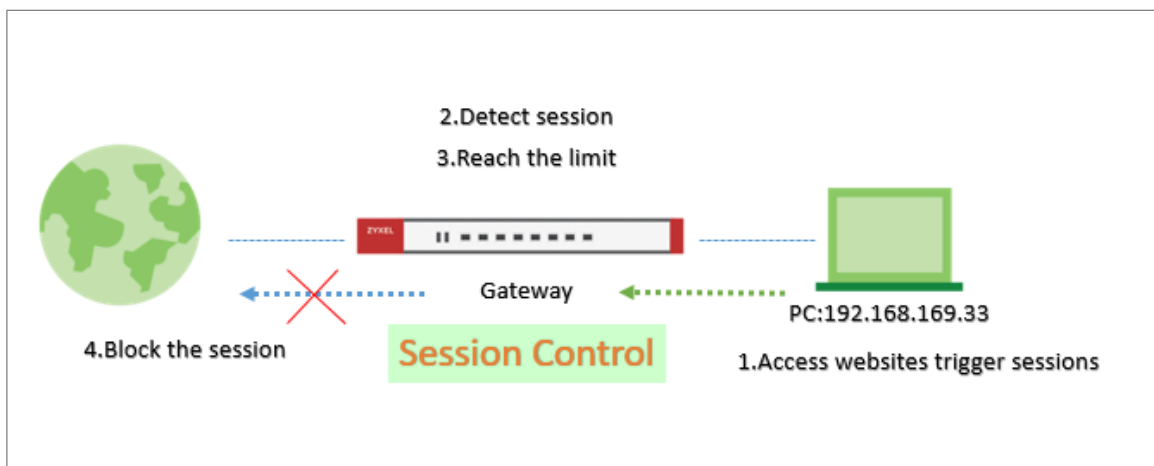
```

77 15.048707 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xee96c336
> Frame 77: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A6AF40E6-CF63-4365-AF89-...}, id 0
> Ethernet II, Src: ZyxelCom_e7:e8:36 (...), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xee96c336
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: ZyxelCom_e7:e8:36 (...)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
    Length: 7
    Vendor class identifier: CSO-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
  Padding: 0000000000

```

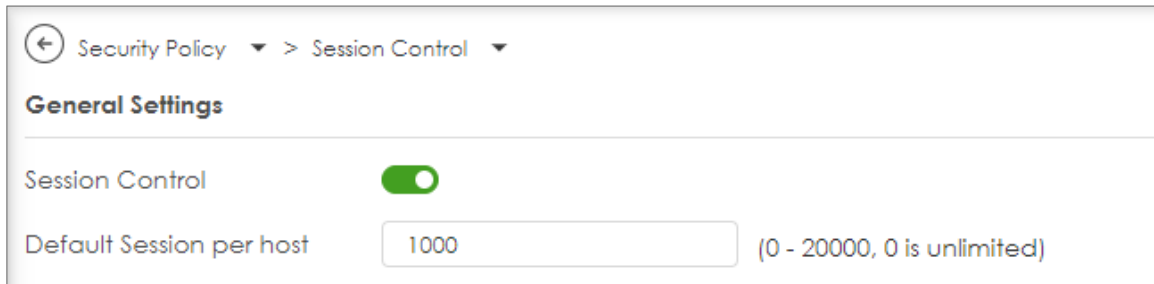
How to Configure Session Control

Session control can address abnormal user behavior. By monitoring session activities, the firewall can detect deviations from normal usage, such as sudden traffic spikes or unauthorized access attempts. This proactive approach enables prompt action to be taken to investigate and mitigate potential security threats .



Set Up the Session Control

Go to Security Policy > Session Control. Turn on this feature.



Security Policy > Session Control

General Settings

Session Control ☒

Default Session per host (0 - 20000, 0 is unlimited)

You can field in the value of the Session per hosts you would like to limit.

The field here is for the client who is not in the rule under the list

Configuration

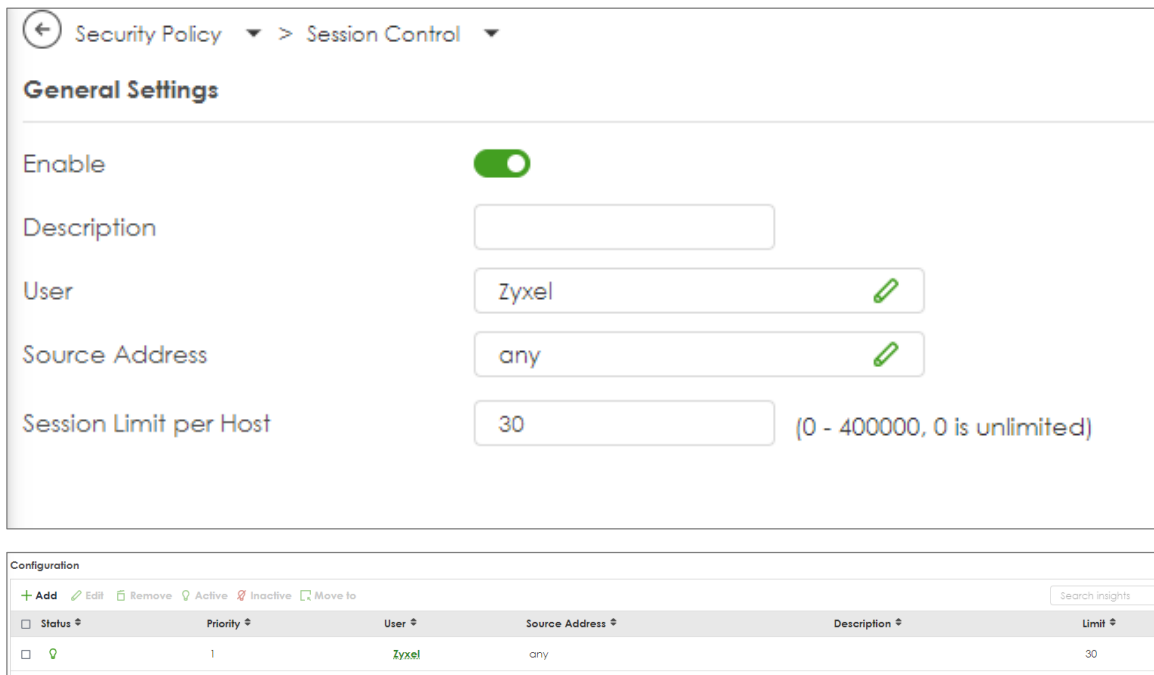
+ Add Edit Remove Active Inactive Move to

Search Insights

Status	Priority	User	Source Address	Description	Limit
--------	----------	------	----------------	-------------	-------

To limit a user's session. You can set up specific rules for each user

Click Add > Select one of the user and field in the Session limit for the user and click save.



Security Policy > Session Control

General Settings

Enable ☒

Description

User

Source Address

Session Limit per Host (0 - 400000, 0 is unlimited)

Configuration


+ Add Edit Remove Active Inactive Move to

Search Insights

Status	Priority	User	Source Address	Description	Limit
<input checked="" type="checkbox"/>	1	Zyxel	any		30


Test the Result

Log in as User: Zyxel



Zyxel ,You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 1 days .

User-defined lease time (max 1440 minutes): 

☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss):

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

Logout

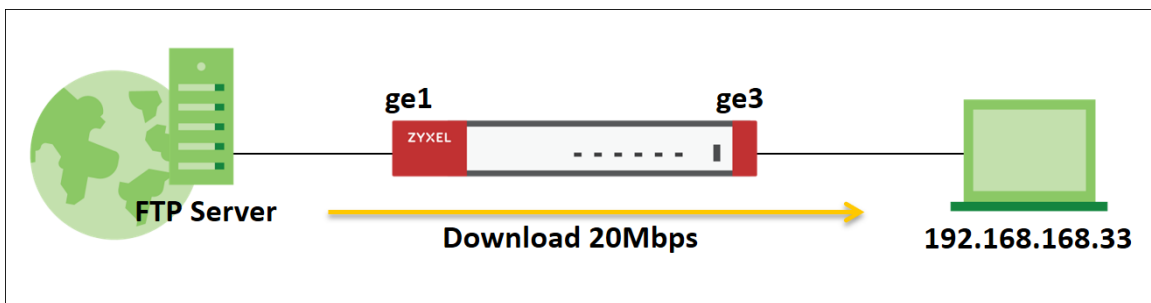
Try to access web browser to hit the session limit


Go to Log & Report > Log/Events and select Session Control to check the logs.

Session Control	Maximum sessions per host (30) was exceeded.	192.168.169.33	172.23.5.1	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.169.33	172.23.5.2	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.169.33	172.25.5.210	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.169.33	172.21.5.1	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.169.33	172.24.78.18	0	ACCESS BLOCK

How to Configure Bandwidth Management for FTP Traffic

This example illustrates how to use USG Bandwidth Management (BWM) for controlling FTP traffic bandwidth allocation. By specifying criteria such as incoming interface, outgoing interface, source address, destination address, service objects, application group, and user, you can create a sequence of conditions to allocate bandwidth for packets that match these criteria. Once BWM is set up, it allows you to limit bandwidth for high-consumption services like FTP, ensuring bandwidth guarantees. This is a practical example of implementing BWM for FTP traffic with a USG device.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 5Mbps. This example was tested using USG FLEX 500H

Set Up the BWM rule for FTP download

Go to Network > BWM scan. Click on "Add" button to create a new BWM rule.

Network > BWM

Configuration

Enable ☒

Name BWM_Per-IP

Description

BWM Type ☒ Shared ☐ Per user ☐ Per-Source-IP ⓘ

Criteria

Incoming Interface ge3 (LAN)

Outgoing Interface ge1 (WAN)

Source LAN1_SUBNET

Destination any

Service Type ☒ Service Object ☐ Application Group

Service Object FTP

User any

Schedule none

Traffic Shaping

Download Limit ☐ Unlimited ☒ Limit 20 Mbps

Upload Limit ☒ Unlimited ☐ Limit 0 Mbps

Priority Medium(4)

Related Setting

Log log

Incoming Interface: ge3

Outgoing Interface: ge1

Source: LAN1 IP Subnet

Application Group: FTP

Traffic Shaping: Download Limit 20 Mbps.



Note: The terms "incoming interface" and "destination interface" indicate the direction of traffic that the client initiates during a session. The term "Source IP information" denotes the initial IP address. Furthermore, the Application Group function identifies client traffic types based not only on the service port but on other criteria as well.

Different Scenarios:

(1) Shared

If you select the "Shared" setting in the BWM rule, the selected IP addresses will share the configured bandwidth.

e.g. Limit the maximum FTP download bandwidth to 20 Mbps for whole of LAN1 PCs.

(2) Per User

If you select the "Per User" setting in the BWM rule, each user will have a limited bandwidth.

e.g. Limit the maximum FTP download bandwidth to 20 Mbps for each user.

(3) Per-Source-IP

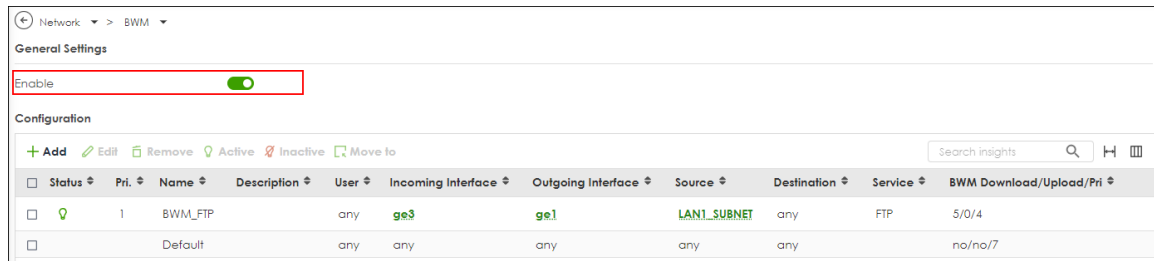
If you select the "Per-Source-IP" setting in the BWM rule, each selected IP address will have a limited bandwidth.

e.g. Limit the FTP download bandwidth for each LAN1 PC to 20 Mbps.



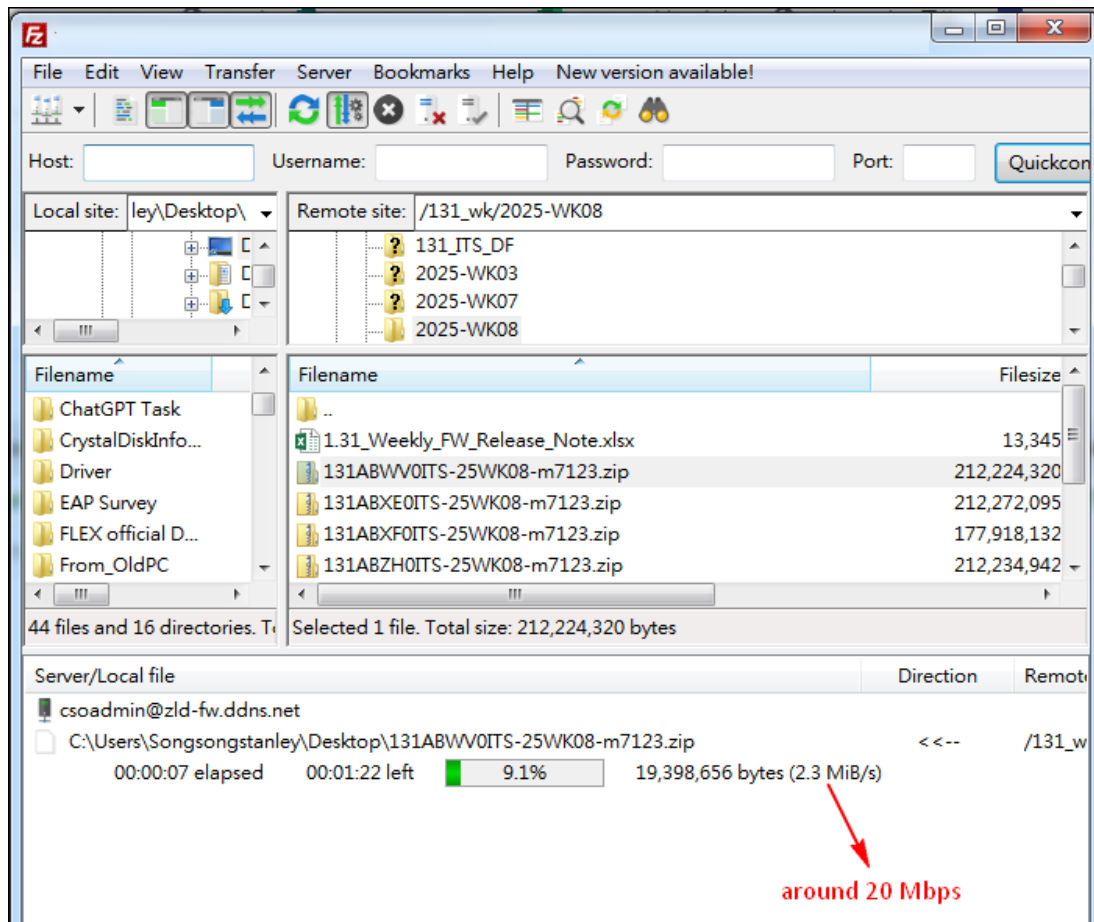
Note: If you select the "Per User" option or configure "User" as a condition, the Captive Portal service must be enabled, and the PC must be authenticated by the firewall first.

Turn on this feature. It will enable BWM function to allowing the rules to be effectively applied.



Test the Result

The PC connect to LAN1 and download file by FTP. the download speed is around 20 Mbps.

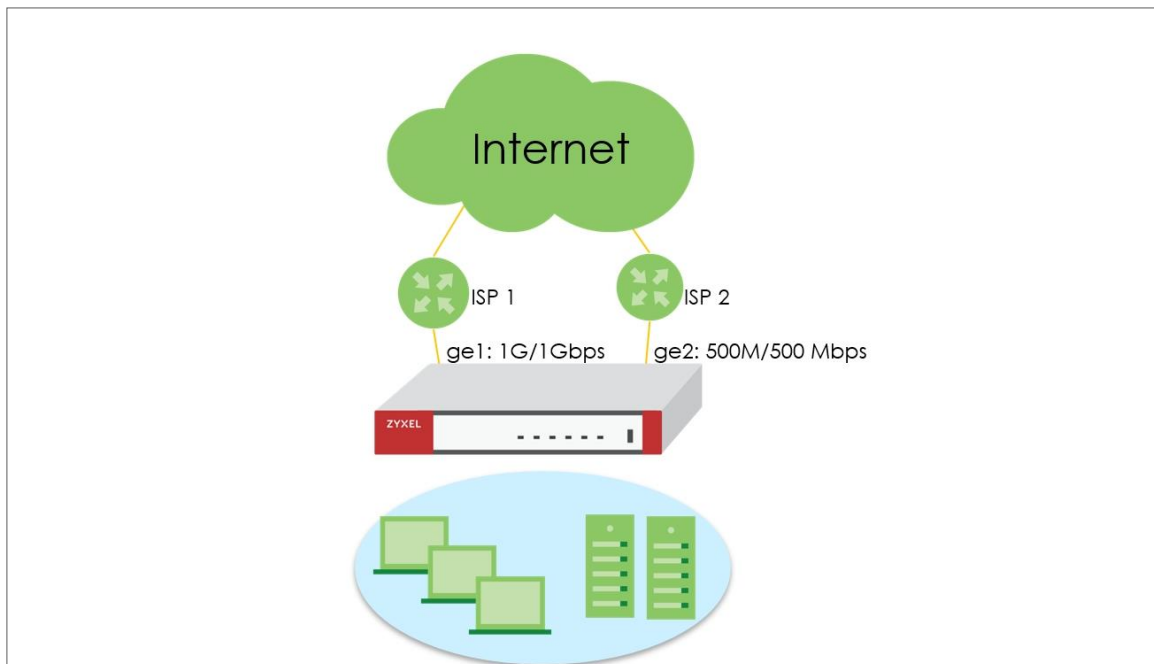



Go to Log & Report > Log/Events and select BWM to check the logs.

Log & Report > Log / Events > System						
System APC AP						
Category All Log Clear Log Export Refresh						
#	Time	Category	Message	Src. IP	Dst. IP	
1	2025-03-27 18:34:15	BWM	Mode=port-base rule_name=BWM_Per-IP user=admin matched	192.168.168.33	59.115.140.38	
2	2025-03-27 18:34:00	BWM	Mode=port-base rule_name=BWM_Per-IP user=admin matched	192.168.168.33	59.115.140.38	

How to Configure WAN trunk for Spillover and Least Load First

In the realm of network management, WAN trunk spillover and the Least Load First (LLF) algorithm are vital for optimizing resource utilization and enhancing network performance. WAN trunk spillover ensures seamless connectivity by distributing traffic across multiple WAN connections, preventing bottlenecks, and maximizing bandwidth usage. The LLF algorithm intelligently balances traffic load by prioritizing the least loaded WAN links, minimizing latency, and improving overall network efficiency. This is an example of using the FLEX H series for two spillovers and the Least Load First configuration. The following example is based on GE1 1G/1G and GE2 500/500 Mbps for illustration.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.20).

Least Load First

The “Least Load First” algorithm allocates new session traffic based on the current outbound bandwidth utilization of each trunk member interface. This utilization, measured as outbound throughput over available bandwidth, serves as the load balancing index. For instance, if WAN 1 has a throughput of 1000K and WAN 2 has 5K, the ZyXel Device calculates the load balancing index accordingly. With WAN 2 showing a lower utilization, indicating lesser utilization compared to WAN 1, subsequent new session traffic is routed through WAN 2 for optimal load distribution.

Spillover

The “Spillover” load balancing algorithm prioritizes the first interface in the trunk member list until its maximum load capacity is reached. Any excess traffic from new sessions is then directed to subsequent interfaces in the list, continuing until all member interfaces are utilized or traffic demands are met. For example, if the first interface offers unlimited access while the second incurs usage-based billing, the algorithm only activates the second interface when traffic surpasses the threshold of the first. This approach optimizes bandwidth usage on the first interface, minimizing Internet fees and preventing overload situations on individual interfaces.

Set Up the User-Defined Trunk

Spillover and Least Load First

Go to Network > Interface > Trunk page, and click **Add** button to create user-defined Trunk. In the general settings, we can configure the following settings;

Name: Least Load First (Enter a descriptive name for this trunk)

Algorithm: LLF

Load Balancing Index: Outbound

Note: This field is available if you selected to use the **Least Load First** or **Spillover** method.

Network > Interface > Trunk

General Settings

Name: LLF

Load Balancing Setting

Algorithm: Least Load First

Load Balancing Index(es): Outbound

+ Add - Remove

Interface	Mode	Limit (Kbps)
No data		

Click **Add** to add a member interface to the trunk, in this scenario, we have ge1, and ge2 for Internet access.

Member: ge1(Wan)

Mode: Active

Limit(Kbps): 1024000

Member: ge2(Wan)

Mode: Active

Limit(Kbps): 512000

+ Add - Remove

Interface	Mode	Limit (Kbps)		
ge1 (WAN)	Active	1024000	✓	✗
ge2 (WAN)	Active	512000	✓	✗

Click **Apply** to save changes.

Some changes were made

What do you want to do then?

Cancel Apply

After the Trunk LLF is created, let's create a second WAN trunk for spillover testing, click **Add** button to create 2nd user-defined Trunk.

Name: Spillover (Enter a descriptive name for this trunk)

Algorithm: Spillover

Load Balancing Index: Outbound

The screenshot shows the 'General Settings' for a new Trunk. The 'Name' field is set to 'Spillover'. Under 'Load Balancing Setting', the 'Algorithm' is set to 'Spillover' and the 'Load Balancing Index(es)' is set to 'Outbound'. Below these settings is a table for adding member interfaces. The table has columns for 'Interface', 'Mode', and 'Limit (Kbps)'. The 'Add' button is highlighted with a red box.

Interface	Mode	Limit (Kbps)
No data		

Click **Add** to add a member interface to the trunk.

Member: ge1(Wan)

Mode: Active

Limit(Kbps): 819200

Member: ge2(Wan)

Mode: Active

Limit(Kbps): 512000

The screenshot shows the 'General Settings' for a new Trunk. The 'Name' field is set to 'Spillover'. Under 'Load Balancing Setting', the 'Algorithm' is set to 'Spillover' and the 'Load Balancing Index(es)' is set to 'Outbound'. Below these settings is a table for adding member interfaces. The table has columns for 'Interface', 'Mode', and 'Limit (Kbps)'. The 'Add' button is highlighted with a red box.

Interface	Mode	Limit (Kbps)
ge1 (WAN)	Active	819200
ge2 (WAN)	Active	512000

Click **Apply** to save changes.

The screenshot shows a confirmation dialog box with the text 'Some changes were made' and 'What do you want to do then?'. There are two buttons: 'Cancel' and 'Apply'. The 'Apply' button is highlighted with a red box.

Go to Default WAN Trunk section, select User-Defined Trunk and select the newly created (LLF or Spillover) Trunk from the list box. Click **Apply** to save changes.

Network > Interface > Trunk

Interface **Trunk** Port

Default WAN Trunk

Trunk Selection

☐ Default Trunk

☒ User-Defined Trunk LLF

User-Defined Trunk

+ Add Edit Remove Reference Search insights

Name	Algorithm	Members
<input type="checkbox"/> LLF	llf	ge1, ge2
<input type="checkbox"/> Spillover	spill-over	ge1, ge2

Default Trunk

Edit Search

Some changes were made

What do you want to do then?

Cancel **Apply**

Test the Result

Spillover

- 1) Apply Spillover in User-Defined Trunk.
- 2) Connect two hosts on the LAN side. Host A upload a large file to an FTP server.
- 3) Go to Traffic Statistics > Port to check interface utilization. Upload traffic should go to ge1 as this interface is the first member interface in Trunk Spillover. Check if maximum load capacity 819200bps is reached. Any excess traffic from new sessions is then directed to subsequent interfaces in the list
- 4) Host B generates ICMP traffic to 8.8.8.8.
- 5) Capture packets on the interface ge2 to see if new sessions are captured on ge2.

Least Load First

- 1) Apply LLF in User-Defined Trunk
- 2) Connect two hosts on the LAN side. Host A upload a large file to an FTP server.
- 3) Go to Traffic Statistics > Port to check interface utilization.
- 4) Host B generates ICMP traffic to 8.8.8.8.
- 5) Capture packets on the interface with lower traffic load to verify if the ICMP traffic is routed through the less congested interface.

How Does SIP ALG Function Work on USG FLEX H?

SIP ALG consists of two key services for managing traffic on firewalls: SIP transformation and SIP pinholes.

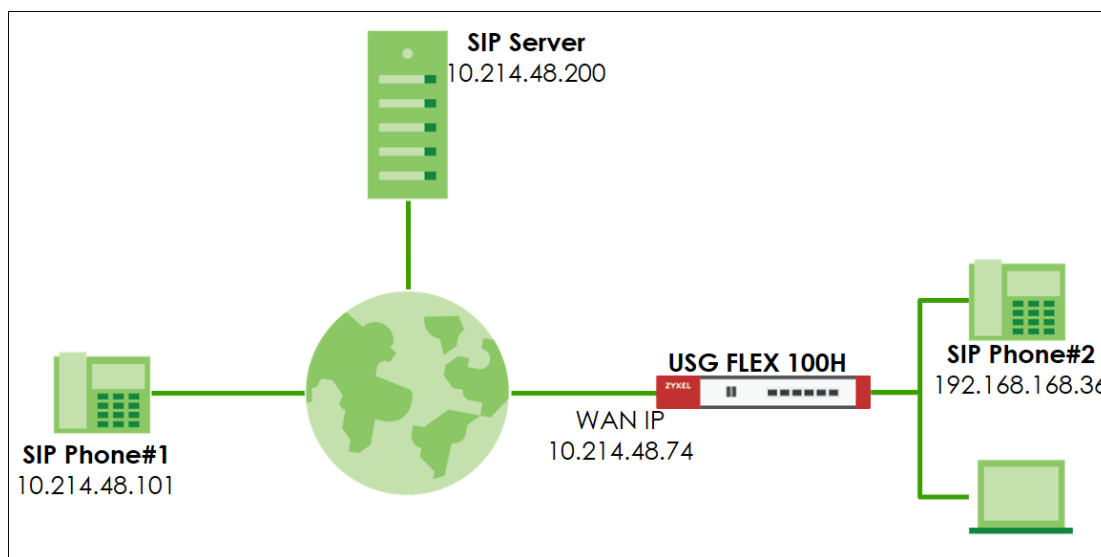
SIP Transformation

The SIP transformation function modifies SIP header information, facilitating SIP signaling traffic over NAT operations. This enables seamless communication between private IP addresses and public IP addresses.

SIP Pinholes

SIP pinholes ensure the persistence of registered SIP sessions and RTP sessions during NAT operations. This prevents issues such as dropped calls or non-functioning phone calls caused by expired SIP/RTP sessions on the firewall.

Cloud-based SIP servers are typically sophisticated enough to distinguish between a client's local (private IP) and public IP, making SIP transformation unnecessary in most scenarios. However, the SIP pinhole feature remains essential for proper NAT operations. The SIP ALG feature on H Series firewalls focuses on supporting SIP pinholes. This ensures that SIP and RTP sessions are managed effectively, maintaining reliable communication across firewalls.



SIP ALG Feature for Keep SIP/RTP Activity Sessions on Firewall

Go to Network > ALG > SIP ALG feature.

Network > ALG

FTP ALG

Enable ☒

Enable FTP Transformations ☒

FTP Signaling Port (1-65535)

Additional FTP Signaling Port (1-65535) (Optional)

SIP ALG

Enable ☒ ←

SIP Signaling Port

+ Add - Remove

☐ Port ↕

☐ 5060

SIP Inactivity Timeout ☒

Media Inactivity Timeout seconds

Signaling Inactivity Timeout seconds

Restrict Peer to Peer Media Connection ☒ i

Restrict Peer to Peer Signaling Connection ☒

SIP Signaling port:

Default SIP service port is 5060. You can configure to other ports to fulfil your network environment.

SIP Inactivity timeout:

In firewall default setting, general UDP session timeout is 300 seconds, and UDP stream timeout is 60 seconds. (System > Advanced)

System Parameters		
Name ↕	Description ↕	Value ↕
UDP Timeout (seconds)	The timeout for initial UDP packets in a connection. (seconds)	300 (seconds)
UDP Timeout Stream (seconds)	The timeout values of the UDP streams once they have sent enough packets. (seconds)	60 (seconds)
ICMP Timeout (seconds)	The timeout for ICMP connection. (seconds)	5 (seconds)

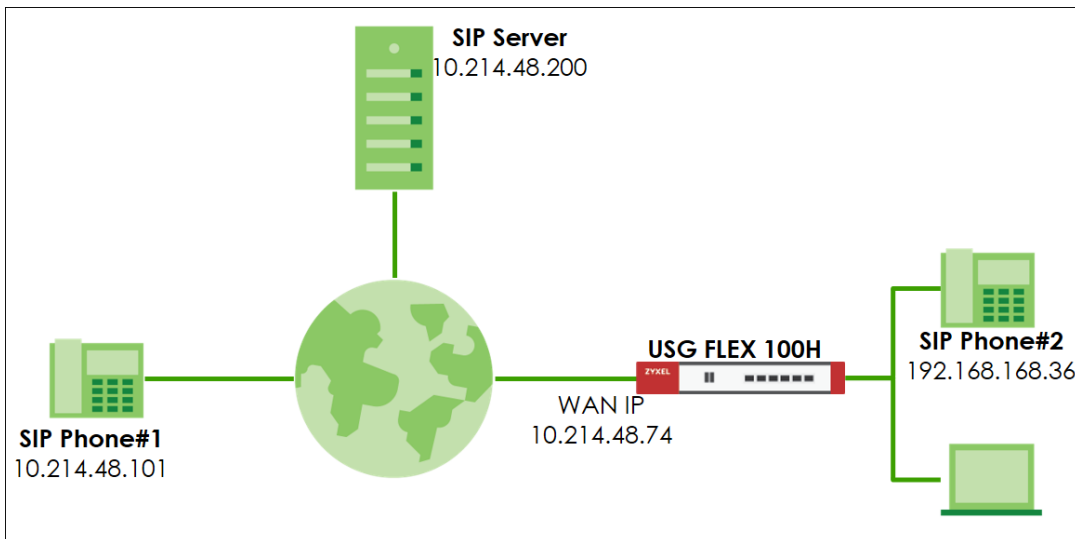
You can configure Media(RTP) and Signaling(SIP) timeout for your SIP phone, it could keep the sessions on firewall to prevent lost incoming phone call due to session expired.

Peer to Peer connection restriction:

It is for incoming STP/RTP traffic. If the source IP address doesn't match to exist sessions, then firewall will drop the incoming traffic.

Test the Result

Dial the SIP phone call from SIP Phone#1 to SIP Phone#2.



Turn on SIP ALG feature and enable "SIP Inactivity Timeout" service, also have an extend Signaling(SIP) and Media(RTP) inactivity timeout as 3000 seconds.

Network > ALG

FTP ALG

Enable ☒

Enable FTP Transformations ☒

FTP Signaling Port (1-65535)

Additional FTP Signaling Port (1-65535)(Optional)

SIP ALG

Enable ☒ ←

SIP Signaling Port

+ Add - Remove

☐ Port

☐ 5060

SIP Inactivity Timeout ☒

Media Inactivity Timeout seconds

Signaling Inactivity Timeout seconds

Restrict Peer to Peer Media Connection ☒ ⓘ

Restrict Peer to Peer Signaling Connection ☒

Use CLI command to check exist sessions has been extended successfully.

CLI> show conntracks | match "<IP address>"

Before enabling the SIP ALG feature, system will use the default UDP timeout.

```
usgflex100h> show conntracks | match "192.168.168.36"
udp      17 294 src=192.168.168.36 dst=10.214.48.200 sport=10007 dport=11015 packets=1 bytes=92 [UNREPLIED]
src=10.214.48.200 dst=10.214.48.74 sport=11015 dport=10007 packets=0 bytes=0 mark=0 use=1
RTP session

udp      17 55 src=192.168.168.36 dst=10.214.48.200 sport=10006 dport=11014 packets=2 bytes=400
src=10.214.48.200 dst=10.214.48.74 sport=11014 dport=10006 packets=1 bytes=200 [ASSURED] mark=16777216 use=1

udp      17 55 src=192.168.168.36 dst=10.214.48.200 sport=5061 dport=5060 packets=2 bytes=1178
src=10.214.48.200 dst=10.214.48.74 sport=5060 dport=5061 packets=1 bytes=556 [ASSURED] mark=16777216 use=1
SIP session

usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
```

After enabling the SIP ALG feature, system will extend the timeout value.

```
usgflex100h> show conntracks | match "192.168.168.36"
udp      17 2999 src=192.168.168.36 dst=10.214.48.200 sport=10002 dport=10254 packets=9513 bytes=1902600
src=10.214.48.200 dst=10.214.48.74 sport=10254 dport=10002 packets=18665 bytes=3733000 [ASSURED] mark=0 helper=RTP use=1
RTP Session

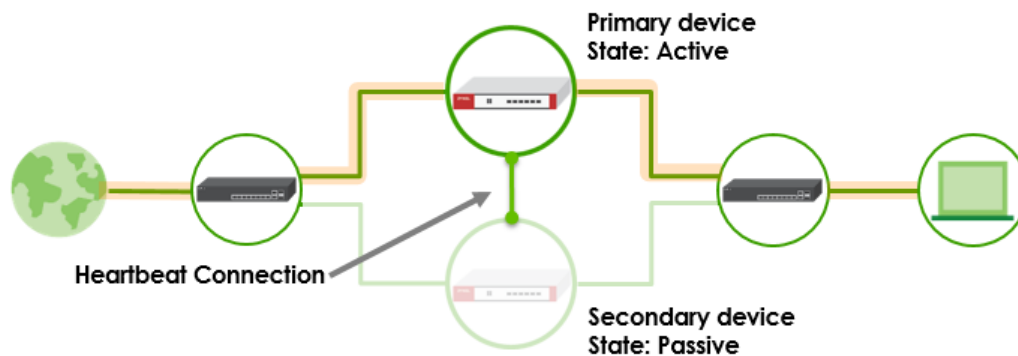
udp      17 2995 src=192.168.168.36 dst=10.214.48.200 sport=10003 dport=10255 packets=36 bytes=3312
src=10.214.48.200 dst=10.214.48.74 sport=10255 dport=1025 packets=73 bytes=6716 [ASSURED] mark=0 helper=RTP use=1


udp      17 2946 src=192.168.168.36 dst=10.214.48.200 sport=5061 dport=5060 packets=38 bytes=4235
src=10.214.48.200 dst=10.214.48.74 sport=5060 dport=5061 packets=5 bytes=2986 [ASSURED] mark=0 helper=sip use=3
SIP Session

usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
```


How to Deploy Device HA

The Device HA feature acts as a failover when one of the devices in the network fails or can't access the Internet. Device HA uses a dedicated heartbeat link between an active device and a passive device for status syncing and backup to the passive device. On the passive device, all ports are disabled except for the port with the heartbeat link. This example illustrates how to deploy the Device HA in your network.

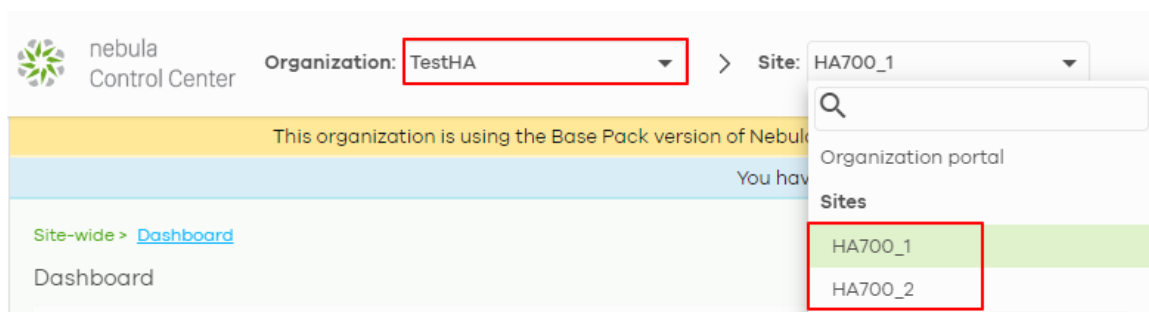


 Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.35).

Prerequisites for Device HA

The primary and secondary devices in Device HA mode must meet the following requirements:

1. **The same model** - Both devices must be of the same hardware model. In this example, both devices must be USG FLEX 200H. You cannot set up Device HA between different models, USG FLEX 200H and USG FLEX 200HP.
2. **The same firmware version** - Both devices must be running the same firmware version (uOS 1.31 or later versions).
3. **The same Organization on Nebula** - Both devices must be registered to the same Organization on Nebula.
 - Assign the primary USG FLEX H to the first site
 - Assign the secondary USG FLEX H to the second site



4. **Synchronization Port** - The port 49058 is reserved for the Device HA synchronization. Users cannot modify this port or assign it to other services.
5. **WAN connection of the active device** - Ensure that the active device has normal WAN connectivity to the internet and is connected to Nebula.



Note: It is highly recommended to complete device registration steps on Nebula before pairing HA.

Configuration on the primary device

1. Set up with your desired configuration and networking settings.
2. The highest-numbered copper Ethernet port is reserved for heartbeat communication. Make sure the heartbeat port is not assigned to any interface. In this example, P8 is the heartbeat port on USG FLEX 200H. **Remove** P8 from interface ge4.

General Settings

Enable Interface

☒

Interface Properties

Role

internal

Interface Type

Ethernet

Interface Name

ge4

Port

p7 (ge4) ✕

p8 (ge4) ✕

▼

Zone

LAN ▼

 Note: Heartbeat port for HA synchronization

USG FLEX 200H/200HP: P8

USG FLEX 500H/700H: P12

Go to Network > Interface and make sure p8 doesn't belong to any interface.

Network

>

Interface

>

Interface

Interface

Trunk

Port

External

<div> <div>+ Add</div> <div>✎ Edit</div> <div>✕ Remove</div> <div>🔗 Reference</div> <div>💡 Active</div> <div>🚫 Inactive</div> <div>🔄 Connect</div> <div>🔌 Disconnect</div> <div>Search insights</div> <div>🔍</div> <div>🔍</div> <div>🔍</div> </div>								
Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input type="checkbox"/> 💡	ge1	WAN		10.214.48.99/255.255.255.0		Ethernet	p1	3
<input type="checkbox"/> 💡	ge2	WAN		0.0.0.0/0.0.0.0		Ethernet	p2	1

Internal

<div> <div>+ Add</div> <div>✎ Edit</div> <div>✕ Remove</div> <div>🔗 Reference</div> <div>💡 Active</div> <div>🚫 Inactive</div> <div>Search insights</div> <div>🔍</div> <div>🔍</div> <div>🔍</div> </div>								
Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input type="checkbox"/> 💡	ge3	LAN		192.168.168.1/255.255.255.0		Ethernet	p3,p4,p5,p6	2
<input type="checkbox"/> 💡	ge4	LAN		192.168.169.1/255.255.255.0		Ethernet	p7	2

3. Go to **System > Device HA > HA Configuration**.

- Select Primary role.
- Select HA MAC address.

If Virtual MAC Address is selected, the MAC address of each interface will be replaced as follows.

D8:EC:E5:XX:XX:1D -> D6:EC:E5:XX:XX:1D

- Configure Management IP for active and passive role. The two management IPs must be different but in the same subnet.
- Select monitor interfaces. HA failover will be triggered when monitored interface is down. Turn on **"Enable"** to enable Device HA and Apply.

HA Status	HA Configuration	HA Log
General Settings		
Enable	<input checked="" type="checkbox"/>	
Management Configuration		
Initial Role	<input checked="" type="radio"/> Primary (License Controller)	
HA MAC address	<input type="radio"/> Physical MAC address <input checked="" type="radio"/> Virtual MAC address	
	<input type="radio"/> Secondary	
Active Node Management IP	<input type="text" value="10.10.10.1"/>	
Passive Node Management IP	<input type="text" value="10.10.10.2"/>	
Management IP Subnet Mask	<input type="text" value="255.255.255.0"/>	
Monitor Interface		
Member	<input type="text" value="ge3"/>	
Failover on Monitored Interface Link Down	<input checked="" type="checkbox"/>	
Failover on Monitored Connectivity Check Failure	<input type="checkbox"/>	

Configuration on the secondary device

1. Make sure the secondary device is reset to default settings. Follow the wizard to register it to Nebula and it to the same organization as the primary device.
2. After the secondary device is registered to Nebula successfully, remove wan connection from the secondary device and login to the device via lan interface to configure HA.
3. Make sure the heartbeat port is not assigned to any interface. In this example, P8 is the heartbeat port on USG FLEX 200H. **Remove** P8 from interface ge4.

General Settings

Enable Interface ☒

Interface Properties

Role: internal

Interface Type: Ethernet

Interface Name: ge4

Port: p7 (ge4) ✕ **p8 (ge4) ✕** ▼

Zone: LAN ▼

4. Go to **System > Device HA > HA Configuration**. Select Secondary role. Turn on "Enable" to enable Device HA and Apply. Logout from the secondary device and unplug all Ethernet cables of wan and lan interfaces.

HA Status **HA Configuration** HA Log

General Settings

Enable ☒

Management Configuration

Initial Role: ☐ Primary (License Controller) ☒ **Secondary**

HA MAC address: ☒ Physical MAC address ☐ Virtual MAC address


Active Node Management IP:

Passive Node Management IP:

Management IP Subnet Mask:

Connect the heartbeat ports

Connect the heartbeat ports of the primary and secondary device directly and avoid putting a device in between such as a switch.

 Note: The heartbeat port of the primary and secondary device must be connected directly to each other (not through a switch).

Check HA status

Login to the primary device and go to **System > Device HA > HA Status**. Make sure the heartbeat link status is connected. You can also use the [SYS LED](#) on the active device to check the pairing status.


Pairing status: Paired

Last Full Sync Status: Success

HA Status
HA Configuration
HA Log

Status

Active



Passive

Primary

S 5009

Secondary

S 3298

Device HA Status

Pairing Status

Synchronization Status

Enabled

Paired

Success

Last Full Sync Status

Last Full Sync Time

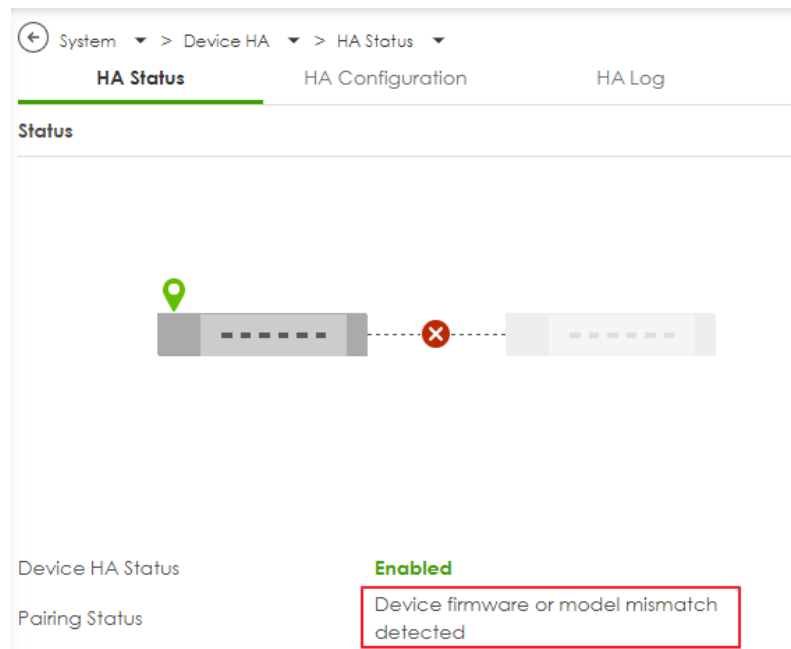
2024-12-25 14:09:39


You can also enter the command on the primary device to check HA status. ***usgflex200h> show state vrf main device-ha status***

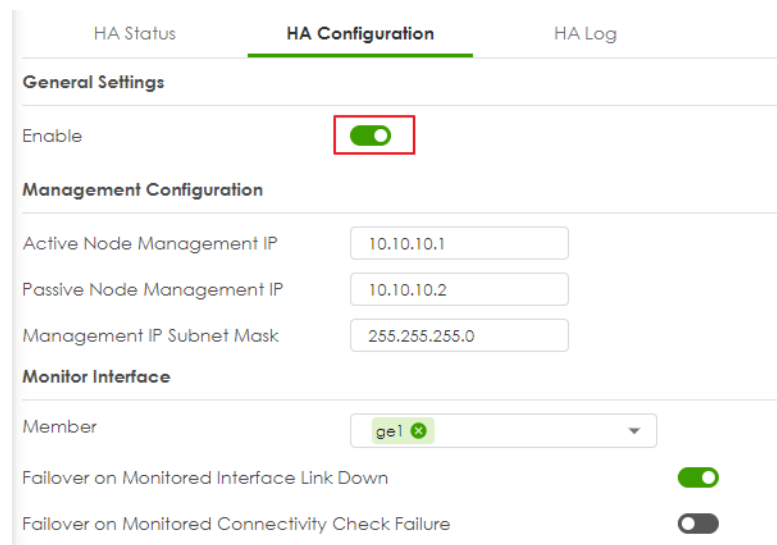
Synchronization can take up to 5 minutes or so. Once it has finished synchronizing, you can verify if the settings are synchronized by accessing the passive device through Passive Node Management IP. Once pairing is complete, the secondary device's license will automatically be transferred to the primary device and you will receive an email notification.

```
usgflex200h0325> show state vrf main device-ha status
status
  enabled true
  initial-role primary
  pairing-state paired
  pairing-msg Paired
  ha-health-state connected
  local-state active
  local-role primary
  active
    role primary
    sn S21[REDACTED]5009
    icon-color on
    ..
  passive
    role secondary
    sn S22[REDACTED]3298
    icon-color on
    ..
  ..
```

If Pairing Status is not "Paired", check what the error message is and resolve the error. In this example, the error is "Device firmware mismatch". Check the firmware version on primary and secondary again and make sure firmware version on both devices are identical.



 Note: After the error is resolved (Upgrade two devices to the same firmware version), you can keep the heartbeat port connected on both devices, and disable and enable HA on the **primary** device to trigger pairing again.



HA Synchronization

- Full Synchronization: Full Sync will be performed under the following conditions. You can also use [SYS LED](#) on the passive device to check the status of HA synchronization.
 - After device reboot
 - After firmware update
 - After turning off Pause Device HA
 - After heartbeat connection is restored
 - After performing CLI on active device to manually force a full synchronization

usgflex200h> cmd device-ha force-sync full
- Incremental Synchronization: This happens automatically when changes are made to the active firewall. The updates are synced to the passive firewall within 5 seconds. It is important to only make configuration changes on the active device.



Note: All configuration changes must be made on the active device. Do NOT manually configure the passive device.


Connect the network cables to the secondary device

Once the devices have been properly synchronized, connect all network cables to wan and lan interfaces of the secondary devices.

Test HA Failover

1. In this example, ge1 is the monitored interface. Unplug the Ethernet cable of ge1 interface from the primary device to trigger HA failover.

Monitor Interface

Member ge1 

Failover on Monitored Interface Link Down ☒

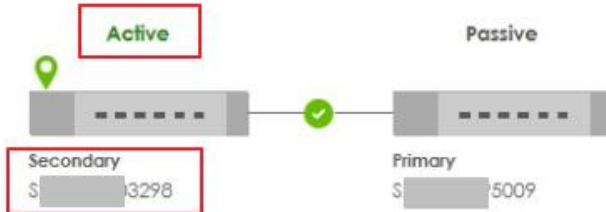
Failover on Monitored Connectivity Check Failure ☐

2. Check HA Status and HA log by accessing Active Node Management IP <https://10.10.10.1>. In HA Status, the secondary device becomes Active role.

Active Node

System > Device HA > HA Status

HA Status HA Configuration HA Log



Device HA Status **Enabled**

Pairing Status **Paired**

Synchronization Status

Last Full Sync Status Success

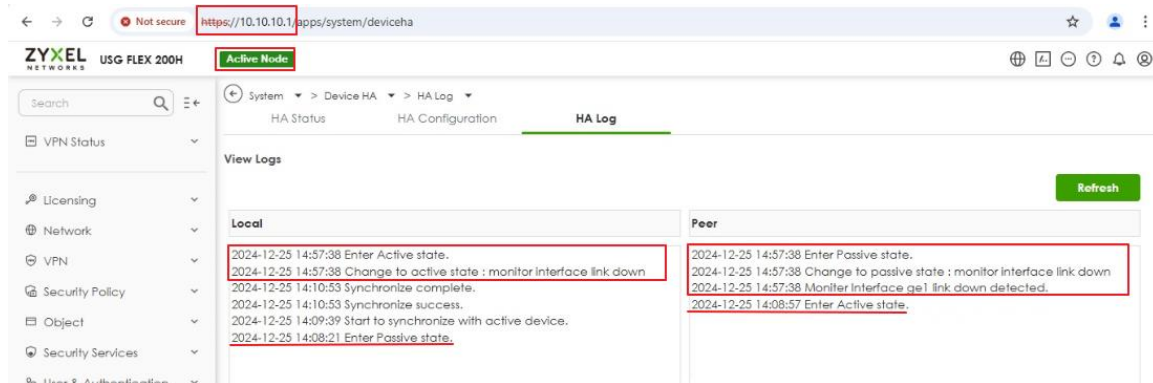
Last Full Sync Time 2024-12-25 14:10:53

Failover Status

Failover Reason Monitor interface link down

Last Failover Time 2024-12-25 14:57:38

In HA Log, the secondary device (Local) changes the state from Passive to Active.



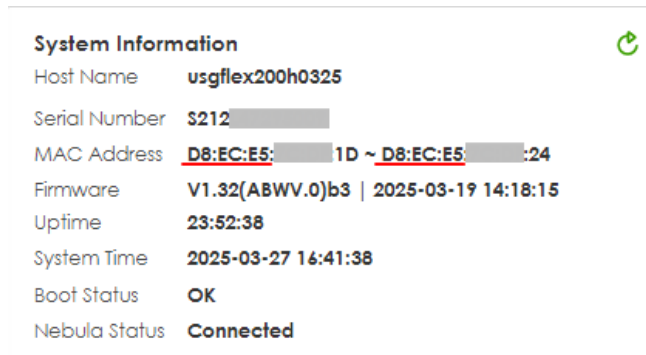
- To prevent excessive failover flapping, the firewall includes a mechanism. By default, the Device HA failover count limit is 5. When this failover count reaches limitation, failover will be stopped. The failover count automatically resets every 5 days. You can use the command to check the failover count.

usgflex200h> show state vrf main device-ha summary

Check Virtual MAC Address

Active Device

On Dashboard > System Information, MAC address is the physical MAC address.



In Network > Interface, it shows the Virtual MAC address.












Interface Properties

Role	external
Interface Type	Ethernet
Interface Name	ge1
Port	p1 (ge1) ✕
Zone	WAN
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <u>d6:ec:e5:</u> 1d <input type="radio"/> Overwrite Default MAC Address auto1

Interface Properties

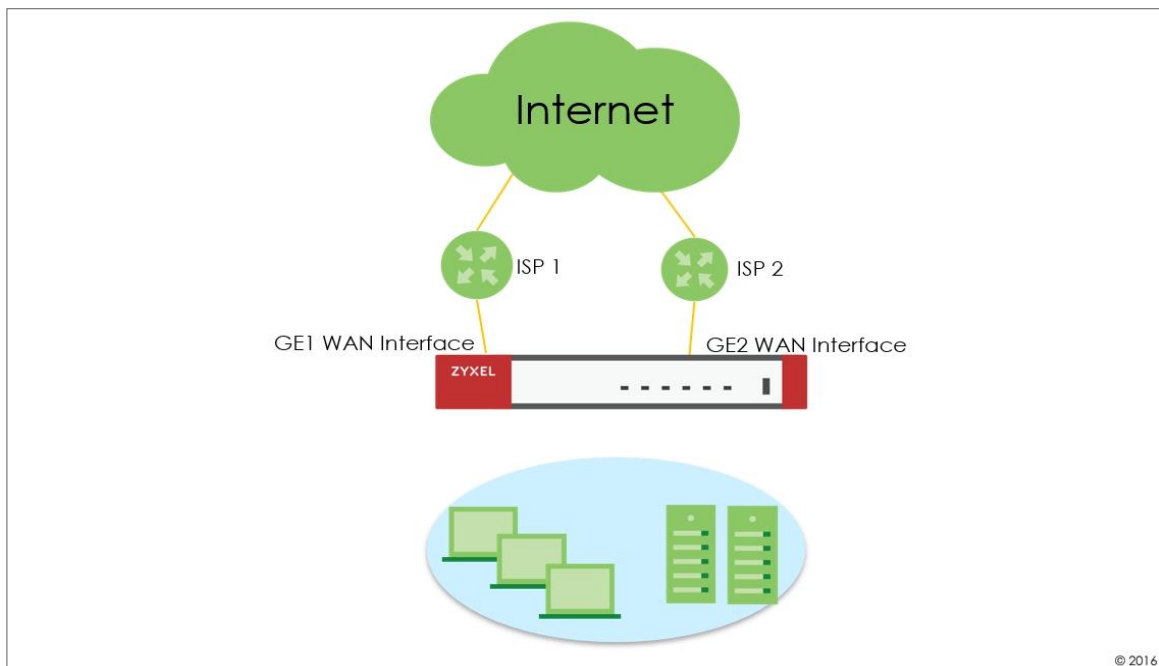
Role	internal
Interface Type	Ethernet
Interface Name	ge3
Port	p3 (ge3) ✕ p4 (ge3) ✕ p5 (ge3) ✕ p6 (ge3) ✕
Zone	LAN
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <u>d6:ec:e5:</u> 1f <input type="radio"/> Overwrite Default MAC Address auto3


SYS LED Status

State	SYS LED on Active Device	SYS LED on Passive Device
Pairing in Progress	Alternating Green on: 500ms, Red on: 500ms  	Green Solid 
Pairing fail	Red Blinking (1sec) 	Green Solid 
Sync. in Progress	Green Solid 	Amber Blinking (500ms) 
Sync. Completed	Green Solid 	Amber Solid 
Active Node Running	Green Solid 	Amber Solid 

How to check Packet Flow Explorer

The Packet Flow Explorer is a powerful tool for analyzing and understanding routing-related issues. When used correctly, it offers a basic overview of your firewall's configuration without requiring an in-depth examination. This example demonstrates how to check the routing and SNAT status using the Packet Flow Explorer.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.31).

Scenario and Requirement

1. Dual WAN interfaces are in the default WRR mode, and both WANs are active.

Name

Default

Load Balancing Setting

Algorithm

wrr

Interface	Mode	Parameter
ge1	Active	1
ge2	Active	1


2. A static route is configured to route traffic to 8.8.8.8 from the GE2 WAN interface.


Policy Route


Static Route

Configuration


+ Add


 Edit


 Remove


 Refresh

Search insights







<input type="checkbox"/>	Status ▾	Name ▾	Destination ▾	Next Hop ▾	Description ▾	Metric ▾
<input type="checkbox"/>		Google_DNS	8.8.8.8/32	ge2		0

3. A policy route is configured to route all internet traffic through the GE1 WAN interface when source is LAN1 subnet.

Policy Route

Static Route

Configuration

+ Add

 Edit

 Remove

 Active

 Inactive

 Move to

 Refresh

Search insights









<input type="checkbox"/>	Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits
<input type="checkbox"/>		1	any	none	ge3	LAN1_SUBNET	any	any	any	any	ge1	preserve	outgoing-interface	0

Based on the configuration above, we expect that if a host is placed in the LAN 1 subnet, all traffic will be routed through the GE1 WAN interface, except for traffic to 8.8.8.8, which will be routed through the GE2 WAN interface.

Verification

1. Place a host in the LAN1 subnet, then run the command **ping 8.8.8.8 -t** in the Windows Command Prompt to check for ICMP response from 8.8.8.8.

```
C:\Users\NT122546>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=9ms TTL=57
Reply from 8.8.8.8: bytes=32 time=8ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=7ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
```

The host receives ICMP response.

2. Confirm that the traffic is being sent out through the GE2 WAN interface, as per the static route configuration.

Type the command **cmd traffic-capture ge2 filter "host 8.8.8.8"** to capture packets on the GE2 WAN interface and verify that the traffic is being sent out through the GE2 WAN interface.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
█
```

We're unable to see packets to 8.8.8.8. Let's capture the packets on the GE1 WAN interface instead.

cmd traffic-capture ge1 filter "host 8.8.8.8"

```
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:59:42.856370 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34317, length 74
09:59:42.862565 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34317, length 74
09:59:43.869372 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34318, length 74
09:59:43.874648 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34318, length 74
09:59:44.882064 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34319, length 74
09:59:44.886659 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34319, length 74
09:59:45.895564 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34320, length 74
09:59:45.898654 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34320, length 74
```

Traffic to 8.8.8.8 is being sent out through the GE1 WAN interface, indicating that the static route is not working as expected.

3. Go to **"Maintenance > Packet Flow Explorer > Routing Status"** to check for possible issues.

Maintenance > Packet Flow Explore > Routing Status

Routing Status SNAT Status

Routing Flow

In Dynamic/SiteTo Site VPN Direct Route **Policy Route** Static Route Nebula Static Route 1-1 SNAT Default WAN Trunk Main Route

Search insights

#	Destination	Gateway	Interface	Metric
1	8.8.8.8	10.214.36.254	ge2	0

As we can see, the policy route has a higher priority than the static route, causing traffic to 8.8.8.8 to be affected by the policy route.

Maintenance > Packet Flow Explore > Routing Status

Routing Status SNAT Status

Routing Flow

In Dynamic/SiteTo Site VPN Direct Route **Policy Route** Static Route Nebula Static Route 1-1 SNAT Default WAN Trunk Main Route

Search insights

#	User	Incoming Interface	Source	Destination	Service	Source Port	DSCP Code	Next Hop Type	Next Hop Info	Policy Route Priority
1	any	ge3	LAN1_SUBNET	any	any	any	any	Interface/GW	ge1:default	1

We can try temporarily disabling the policy route to see if traffic to 8.8.8.8 goes through the GE2 WAN interface.

cmd traffic-capture ge2 filter "host 8.8.8.8"

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
10:40:33.037025 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36708, len 74
10:40:38.034168 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36709, len 74
10:40:43.036771 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36710, len 74
10:40:48.033310 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36711, len 74
10:40:53.035280 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36712, len 74
```

Now we can see the traffic to 8.8.8.8 appearing on the GE2 WAN interface. However, there is no ICMP response from the uplink router. Upon checking the source IP, it is the LAN host's IP, but it should be the GE2 WAN interface IP. The result shows that the firewall GE2 WAN interface does not have source NAT.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
10:40:33.037025 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36708, len 74
10:40:38.034168 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36709, len 74
10:40:43.036771 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36710, len 74
10:40:48.033310 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36711, len 74
10:40:53.035280 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36712, len 74
```

4. Go to **"Maintenance > Packet Flow Explorer > SNAT Status"** to check for possible issues.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP
2	Remote Access VPN	External Interface	Outgoing Interface IP

Mouse over the External interface. It indicates that SNAT is off on the GE2 WAN interface. This would be a misconfiguration on the GE2 WAN interface.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP
2	Remote Access VPN	External Interface	Outgoing Interface IP

We can go to **"Network > Interface > Interface"**, and double click ge2 to tick SNAT.

DHCP Option 60

MTU Bytes

Default SNAT ☒

Change to a Different ISP ☐

The above scenario is a simple example for checking routing and SNAT status in Packet Explorer.

Test the Result

Generate ICMP traffic from LAN hosts to 8.8.8.8 and confirm if the traffic is sent out through the GE2 WAN interface.

1. Run the command ***ping 8.8.8.8 -t*** in the Windows Command Prompt to check if it has an ICMP response from 8.8.8.8.

```
C:\Users\NT122546>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=3ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
```

2. Type the command ***cmd traffic-capture ge2 filter "host 8.8.8.8"*** to capture packets on the GE2 WAN interface and check if the traffic is sent out through the GE2 WAN interface.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
15:51:47.733935 d8:ec:e5:7c:df:de > d2:ec:30:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26449, length 60
15:51:47.738151 d2:ec:30:78:al:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26449, length 60
15:51:48.747899 d8:ec:e5:7c:df:de > d2:ec:30:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26450, length 60
15:51:48.751677 d2:ec:30:78:al:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26450, length 60
15:51:49.773147 d8:ec:e5:7c:df:de > d2:ec:30:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26451, length 60
15:51:49.777218 d2:ec:30:78:al:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26451, length 60
15:51:50.780712 d8:ec:e5:7c:df:de > d2:ec:30:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26452, length 60
15:51:50.784007 d2:ec:30:78:al:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26452, length 60
15:51:51.789695 d8:ec:e5:7c:df:de > d2:ec:30:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26453, length 60
15:51:51.793041 d2:ec:30:78:al:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26453, length 60
```

How to set up a Link Aggregation Group (LAG) interface

A Link Aggregation Group (LAG) combines multiple Ethernet ports into a single logical link, LAG interface, between network devices. It helps to increase bandwidth and provide link redundancy.

The LAG interface of ZyXel USG FLEX H firewalls combines multiple Ethernet interfaces as members and supports three types of modes, Active-Backup, LACP (802.3ad), and Static.

Prerequisites of Ethernet interface member

To be a member of LAG interface, the Ethernet interface must Meet all of the following conditions:

1. The Ethernet interface can only bind to one port. And the port cannot be used by other VLAN interface.
2. The Ethernet interface cannot be a member of other bridge, or LAG interface.
3. It does not have an IP address (must be set to unassigned).
4. It cannot have MAC address overwrite settings, must use default MAC address.
5. The interface must not be referenced by any other configurations except the Zone.

Create a LAG interface

1. Edit the member Ethernet interfaces and make sure the MAC address is set to use default MAC address and the Address Assignment is set to unassigned.

← Network > Interface > Interface

General Settings

Enable Interface ☒

Interface Properties

Role: internal

Interface Type: Ethernet

Interface Name: ge5

Port: p8 (ge5)

Zone: LAN

MAC Address: ☒ Use Default MAC Address fc:22:f4:f6:91:4c
☐ Overwrite Default MAC Address auto8

Description:

Address Assignment: ☒ Unassigned ☐ Use Fixed IP Address
 IP/Network Mask:

2. Click +Add to create an interface and select the Interface Type as LAG.

← Network > Interface > Interface

General Settings

Enable Interface ☒

Interface Properties

Role: internal

Interface Type: LAG

Name:

Zone:

MAC Address:

Ethernet
VLAN
Bridge
LAG

characters. The valid characters are [a-z][A-Z]+[0-9][a-z][A-Z][_-].



Note:

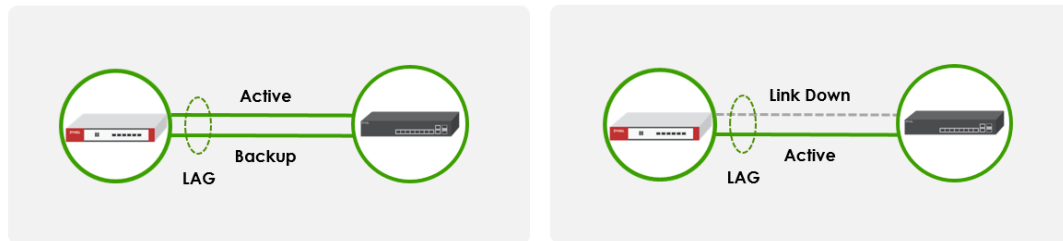
- LAG support interface Role: **External**, **Internal** and **General**
- When the interface role is external, the LAG IP address does not support PPPoE or PPPoE with a static IP

3. Select the LAG mode

Name	<input type="text" value="LAG-ge-5-6"/>	
Zone	<input type="text" value="LAN"/>	
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <input type="radio"/> Overwrite Default MAC Address <input type="text"/>	
Description	<input type="text"/>	
Address Assignment	<input type="radio"/> Unassigned <input checked="" type="radio"/> Use Fixed IP Address IP/Network Mask <input type="text" value="172.198.1.1/24"/>	
Secondary IP	<div> <div>+ Add <input type="checkbox"/> Remove</div> <div> <input type="checkbox"/> IP/Netmask <input type="text"/> </div> <div>No data</div> </div>	
Members	<input type="text" value="ge5"/> <input type="text" value="ge6"/>	
Mode	<div> <div>static</div> <div>active-backup</div> <div>lacp (802.3ad)</div> </div>	
Mii Monitoring Interval	<input type="text" value="(1-1000)ms"/>	
Primary		

LAG mode: Active-Backup

Provides automatic link failover by keeping backup ports not transmitting traffic until the primary port experiences a link-down event.



Mii Monitoring Interval: Defines how frequently the system checks if a LAG member interface is active or down

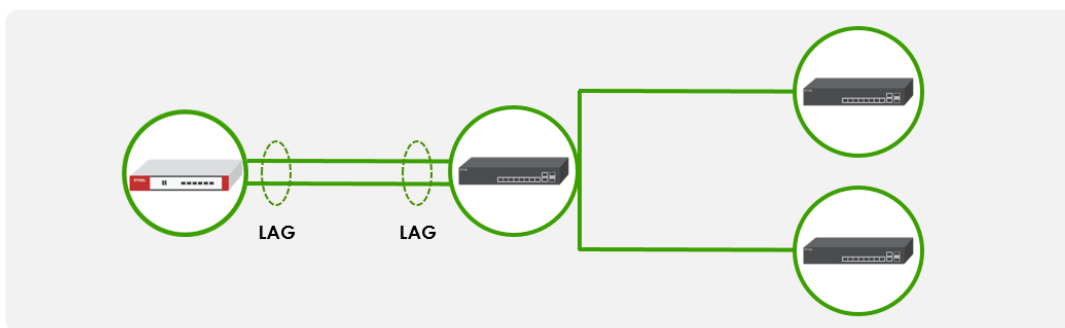
Primary: Allows you to specify which member interface should be preferred as the active link

Members ⓘ	ge5 x ge6 x
Mode	active-backup
Mii Monitoring Interval	100 (1-1000)ms
Primary	ge5




LAG mode: LACP (802.3ad)

Provides automatic link failover and load sharing by allowing all ports in the LAG group to transmit traffic. The LACP messages will be periodically sent.

When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall.






Transmit Hash Policy: Determine how outgoing traffic is distributed across the aggregated links. The default option is **src-dst-ip-mac**. Select **src-dst-ip-mac** to distribute traffic more efficiently by considering both source-destination IP and MAC.

Members 	ge5  ge6 	
Mode	lACP (802.3ad) ▼	
Mii Monitoring Interval	100	(1-1000)ms
Transmit Hash Policy	src-dst-ip-mac ▼	

LAG Mode: Static

All ports in the LAG group will be always active for link failover and load balancing. The use case is when using legacy networking equipment that doesn't support LACP. When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall. When in Static mode, the connected Switch must also configure Static Trunk mode for the physical ports that connect to the USG FLEX H Firewall.

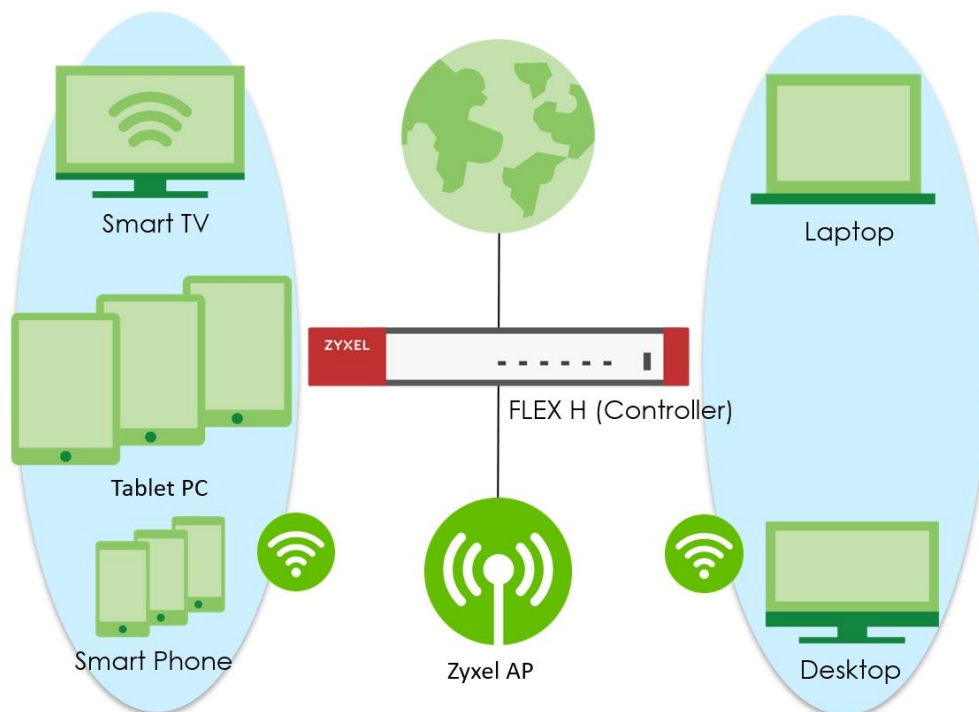
Members 	ge5  ge6 	
Mode	static ▼	
Mii Monitoring Interval	100	(1-1000)ms
Transmit Hash Policy	src-dst-ip-mac ▼	


Checked by CLI: show state vrf main interface lag

```
usgflex500h> show state vrf main interface lag
lag LAG-ge-5-6
  mtu 1500
  promiscuous false
  enabled true
  ethernet
    mac-address fc:22:f4:f6:91:4d
  ..
  ipv4
    address 172.198.1.1/24
    primary-address 172.198.1.1/24
  ..
  network-stack
    ipv4
      send-redirects true
      accept-redirects false
      accept-source-route false
      arp-announce any
      arp-filter false
      arp-ignore any
      arp-proxy false
      log-invalid-addresses false
    ..
    ipv6
:....skipping...
lag LAG-ge-5-6
  mtu 1500
  promiscuous false
  enabled true
  ethernet
    mac-address fc:22:f4:f6:91:4d
  ..
  ipv4
    address 172.198.1.1/24
    primary-address 172.198.1.1/24
  ..
  network-stack
    ipv4
      send-redirects true
      accept-redirects false
      accept-source-route false
      arp-announce any
      arp-filter false
```

How to Set Up AP Control Service for Zyxel APs

In today's digital landscape, wireless networks have become a critical infrastructure for businesses and organizations. As the number of connected devices continues to rise and network demands grow, managing and optimizing wireless environments has become increasingly challenging. Serving as the backbone of centralized Wi-Fi management, wireless controllers play a vital role in enhancing network stability, security, and operational efficiency. This article delves into the key functions of wireless controllers, their application scenarios, and their importance in enterprise network architecture. This is an example of using USG FLEX H series to manage the Zyxel Access Points (APs) and allow wireless access to the network.

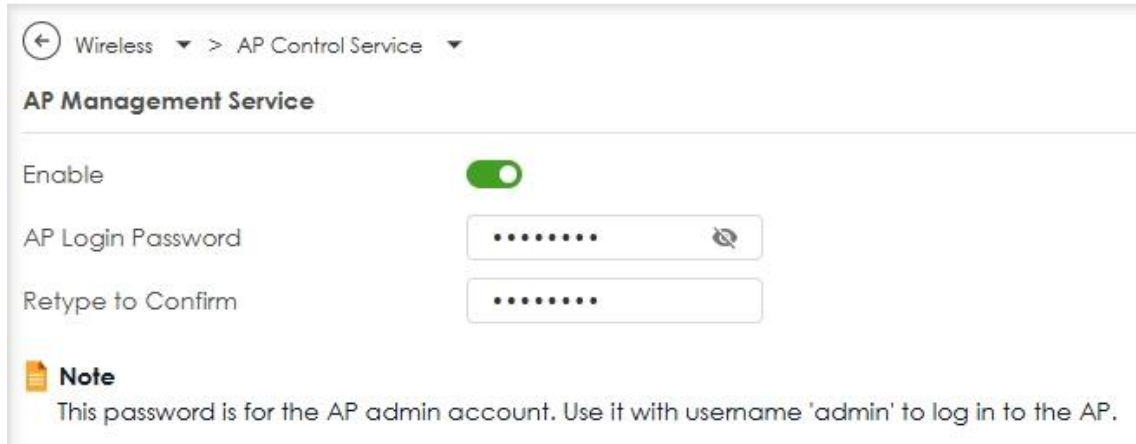


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).

Set Up the AP Management on the FLEX H series

In the USG FLEX H, go to Wireless > AP Control Service, enable the AP Management Service, and set the AP login password.

Wireless > AP Control Service



Wireless > AP Control Service

AP Management Service

Enable ☒

AP Login Password

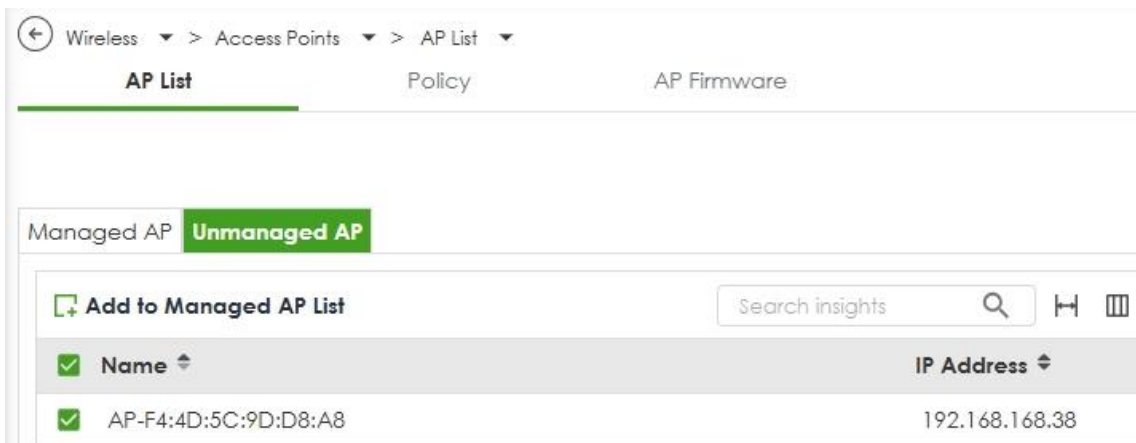
Retype to Confirm

Note
This password is for the AP admin account. Use it with username 'admin' to log in to the AP.

Connect the Zyxel AP unit to the lan interface.

Go to Wireless > Access Points > AP List. The Zyxel AP will be listed under Unmanaged AP tab. Tick the AP and click "Add to Managed AP List."

Wireless > Access Points > AP List > Unmanaged AP



Wireless > Access Points > AP List

AP List Policy AP Firmware

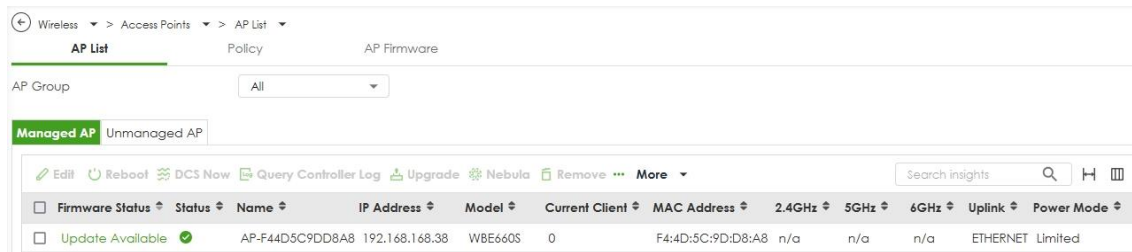
Managed AP **Unmanaged AP**

[Add to Managed AP List](#)

<input checked="" type="checkbox"/> Name	IP Address
<input checked="" type="checkbox"/> AP-F4:4D:5C:9D:D8:A8	192.168.168.38


Once the actions above are completed, the AP will be listed in the Managed AP tab.

Wireless > Access Points > AP List > Managed AP



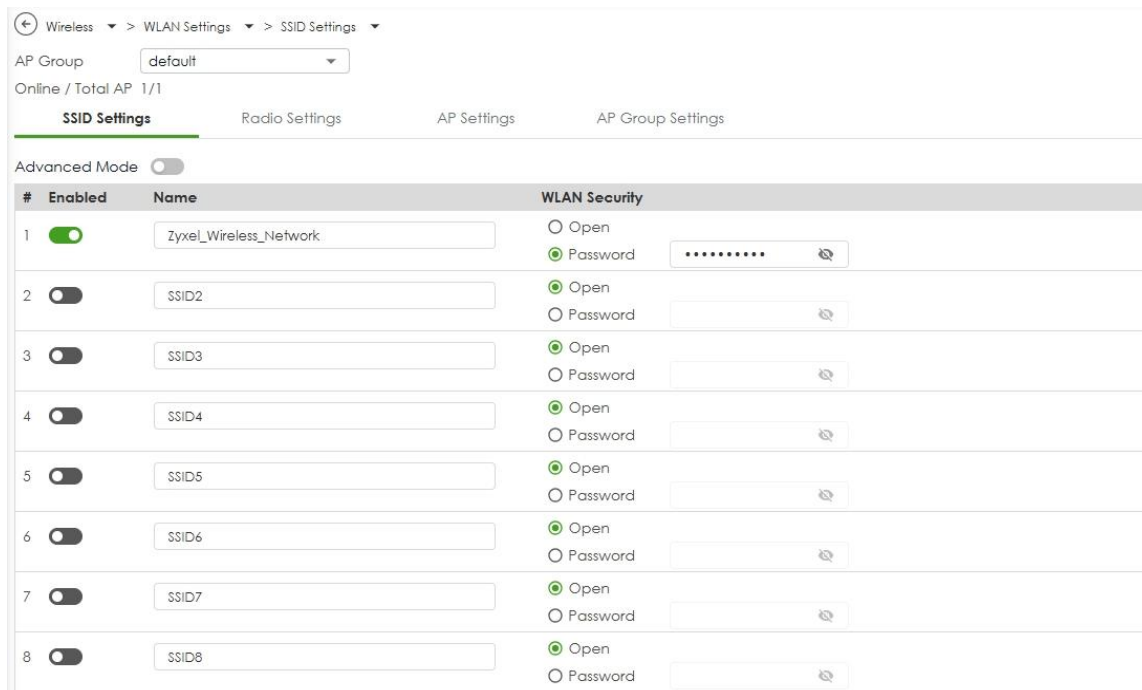
The screenshot shows the 'Managed AP' tab in the 'AP List' section. It includes a table with columns for Firmware Status, Status, Name, IP Address, Model, Current Client, MAC Address, 2.4GHz, 5GHz, 6GHz, Uplink, and Power Mode. A single AP is listed with the name 'AP-F44D5C9DD8A8' and status 'Update Available'.

Firmware Status	Status	Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	Uplink	Power Mode
Update Available	✓	AP-F44D5C9DD8A8	192.168.168.38	WBE660S	0	F4:4D:5C:9D:D8:A8	n/a	n/a	n/a	ETHERNET	Limited

 Note: The APs may take few minutes to appear in the Managed AP List.

Go to Wireless > WLAN Settings > SSID Settings to configure a name for the SSID and set a password for WLAN security.

Wireless > WLAN Settings > SSID Settings



The screenshot shows the 'SSID Settings' page with a table of SSIDs. The first SSID, 'ZyXel_Wireless_Network', is enabled and has 'Password' security selected. The other SSIDs (SSID2 through SSID8) are disabled and have 'Open' security selected.

#	Enabled	Name	WLAN Security
1	<input checked="" type="checkbox"/>	ZyXel_Wireless_Network	<input checked="" type="radio"/> Password
2	<input type="checkbox"/>	SSID2	<input checked="" type="radio"/> Open
3	<input type="checkbox"/>	SSID3	<input checked="" type="radio"/> Open
4	<input type="checkbox"/>	SSID4	<input checked="" type="radio"/> Open
5	<input type="checkbox"/>	SSID5	<input checked="" type="radio"/> Open
6	<input type="checkbox"/>	SSID6	<input checked="" type="radio"/> Open
7	<input type="checkbox"/>	SSID7	<input checked="" type="radio"/> Open
8	<input type="checkbox"/>	SSID8	<input checked="" type="radio"/> Open

Test the Result

Go to Wireless > Access Points > AP List > Managed AP tab. You can check the list of APs currently connected, along with detailed information such as IP address, model name, current clients, MAC address, and radio information.

Wireless > Access Points > AP List > Managed AP

Firmware Status	Status	Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	Uplink	Power Mode
Update Available	✓	AP-F44D5C9DD8A8	192.168.168.38	WBE660S	0	F4:4D:5C:9D:D8:A8	n/a	n/a	n/a	ETHERNET	Limited

Go to the Wireless > WLAN clients, you can check the list of wireless stations associated with a managed AP and the details information such as SSID Name, Security, IPv4 Address, and association time.

Wireless > WLAN clients

MAC Address	Host Name	Connected to	AP Group	SSID	Security	IPv4 Address	Association time
E0:D0:45:6B:3F:69	NT122546-NB01	AP-F44D5C9DD8A8	default	Zyxel_Wireless_Network	WPA2-PSK	192.168.168.39	2025/03/26 17:08:11

Using a laptop to connect to SSID: Zyxel_Wireless_Network and type the password for authentication. Go to the Log & Report > Log / Events > APC, you will see WLAN Station Info as shown below.

Log & Report > Log / Events > APC

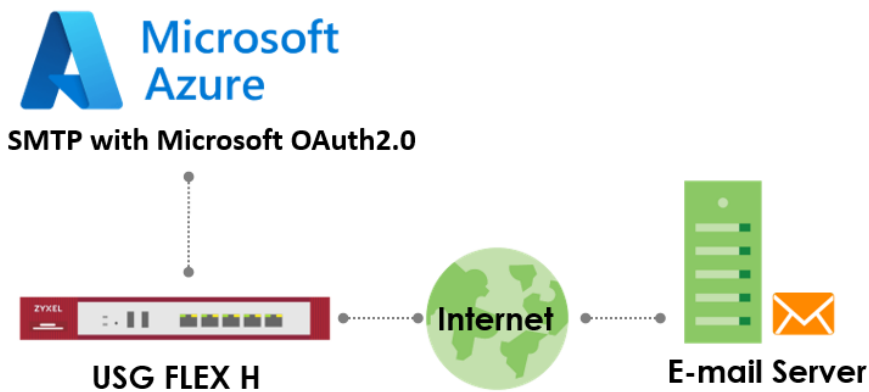
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2025-03-26 17:17:25	Wlan Station Info	STA connected, MAC:E0:D0:45:6B:3F:69, AP:AP-F44D5C9DD8A8, interface:wlan-2-1, SSID: Zyxel_Wireless_Network. Signal: -20dBm	0.0.0.0	0.0.0.0	0	


What Could Go Wrong?

If you can't see AP information in the AP List, please check the number of APs connected to the USG FLEX H firewall has exceeded the maximum Managed AP number it can support. If your mobile device can't access to the Internet via AP connects to the USG FLEX H firewall, please check if the LAN outgoing security policy allow access to the Internet.

How to set up SMTP with Microsoft OAuth2.0?

This guide explains how to configure your gateway to send emails using **SMTP with Microsoft OAuth 2.0** authentication through a Microsoft 365 account. OAuth 2.0 provides secure, token-based authentication, replacing less secure basic authentication methods. Follow these steps to register an application in Microsoft Azure and configure your gateway for SMTP.



 Note: SMTP with Microsoft OAuth 2.0 is supported on USG Flex H series. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.35).

Prerequisites

1. A Microsoft 365 account with a licensed Exchange Online mailbox.
2. Administrative access to the Microsoft Azure Portal (<https://portal.azure.com>).
3. SMTP AUTH is enabled for the mailbox (see Step 3 below).
4. Your gateway device with SMTP configuration access (firmware version uOS1.35 or above).

Step 1: Register an Application in Azure Portal

1. **Sign in to Azure Portal** - Navigate to <https://portal.azure.com> and sign in with an account that has administrative privileges for Microsoft Entra ID.
2. **Navigate to App Registrations** - In the left-hand menu, select **Microsoft Entra ID** > **App registrations** > **New registration**.
3. **Configure the Application** –

Name: Enter a descriptive name (e.g., "Gateway SMTP App").

Supported account types: Select **Accounts in this organizational directory only** (Single tenant) for most cases.

Redirect URI: The redirect URI specifies where the authorization server should send the user back after successfully authenticating to return an access token to their email account.

Type: Select **"Web"**.

URI: Enter [https://\[device fqdn or ip\]/cgi-bin/msoauth2.cgi](https://[device fqdn or ip]/cgi-bin/msoauth2.cgi). Replace [Device FQDN or IP] with the actual fully qualified domain name or IP address of an internal interface that the administrator computer can connect to. (Note: Redirect URI must begin with the scheme **https**). Finally, click **Register**.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

All services > App registrations >

Register an application

Name

The user-facing display name for this application (this can be changed later).

SMTP

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Zyxel Group Corporation only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://192.168.0.81/cgi-bin/msoauth2.cgi

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

4. **Copy Application IDs** – On the app's **Overview** page, copy the **Application (client) ID** and **Directory (tenant) ID**. These are required for your gateway configuration.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

All services > App registrations >

SMTP

Search Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
- Support + Troubleshooting

Essentials

Display name : SMTP

Application (client) ID : 27cba1b2-4a02-463a-969b-893384237a82

Object ID : 52960d2c-971d-409b-a643-5d714087f423

Directory (tenant) ID : d44c31fd-3801-477b-9157-475a43d895a8

Supported account types : My organization only

Client credentials : 0 certificate_1_secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in L... : SMTP

5. **Create a Client Secret** – Navigate to **Certificates & secrets > Client secrets > New client secret**. Add a description (e.g., "SMTP Secret") and select an expiration period (e.g., 24 months). Click **Add**, then immediately copy the **Value** of the client secret. **Note: This value is only shown once**, and you will not be able to retrieve it after leaving

this page. If you lose it, you'll need to generate a new one. This is your "Client Secret". Store it securely, as it grants access to your application.

Home > SMTP

SMTP | Certificates & secrets

Search Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
SMTP Secret	7/2/2027	cpb*****	6a6a8b7c3b-1a2b-4d5e-af5f2-bcd8a4c71f9b2

Step 2: Grant API Permissions

Add Permissions:

- o From the left-hand navigation of your application's overview page, click on **API permissions > +Add a permission**.
- o Select **Microsoft Graph**
- o Choose **Delegated permissions** > Search for **offline_access**
- o Click **Add permissions**.
- o Add 2nd permissions. Click **+Add a permission**
- o Select **Microsoft Graph**
- o Choose **Delegated permissions** > select **SMTP.Send**
- o Click **Add permissions**.

Home > App registrations > test0616

test0616 | API permissions

Search Refresh Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

You are editing permission(s) to your application, users will be notified.

Granting tenant-wide consent may revoke permissions that were previously granted. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about permissions](#)

[+ Add a permission](#) Grant admin consent for Zyxel

API / Permissions name	Type	Description
Microsoft Graph (2)		
offline_access	Delegated	Maintain access to data you have given it access to
User.Read	Delegated	Sign in and read basic profile

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Cosmos DB

Fast NoSQL database with open APIs for any scale.

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps server

Home > App registrations > test0616

test0616 | API permissions

Search Refresh Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

You are editing permission(s) to your application, users will be notified.

Granting tenant-wide consent may revoke permissions that were previously granted. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about permissions](#)

[+ Add a permission](#) Grant admin consent for Zyxel

API / Permissions name	Type	Description
Microsoft Graph (2)		
offline_access	Delegated	Maintain access to data you have given it access to
User.Read	Delegated	Sign in and read basic profile

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

off

The "Admin consent required" column shows the default value for an organization, how the permission, user, or app. This column may not reflect the value in your organization, or [learn more](#)

Permission

OpenId permissions (1)

☒ offline_access Maintain access to data you have given it access to

[Add permissions](#) Discard

Home > App registrations > test0616

test0616 | API permissions

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request

You are editing permission(s) to your application, users will be affected.

Granting tenant-wide consent may revoke permissions that were previously granted. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about permissions](#)

[+ Add a permission](#)

API / Permissions name	Type	Description
Microsoft Graph (2)		
offline_access	Delegated	Maintain session state
User.Read	Delegated	Sign in and read user profile

To view and manage consented permissions for individual users, go to the [Users](#) blade.

Request API permissions

9 **Delegated permissions**
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

10 **SMTP**

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization. [Learn more](#)

Permission

11 **SMTP (1)**

☒ SMTP.Send
Send emails from mailboxes using SMTP AUTH.

12 **Add permissions** Discard

Step 3: Enable SMTP AUTH for the mailbox

1. **Sign in to Microsoft 365 admin center** - Navigate to **Users > Active users** > click the user's mailbox > Select **Mail** tab.

Microsoft 365 admin center

Home > Active users

Active users

Recommended actions (1)

[Add a user](#) [Multi-factor authentication](#)

☒ Display name ↑

Mail

Account Devices Licenses and apps **Mail** OneDrive

Mailbox storage

Learn more about mailbox storage quotas

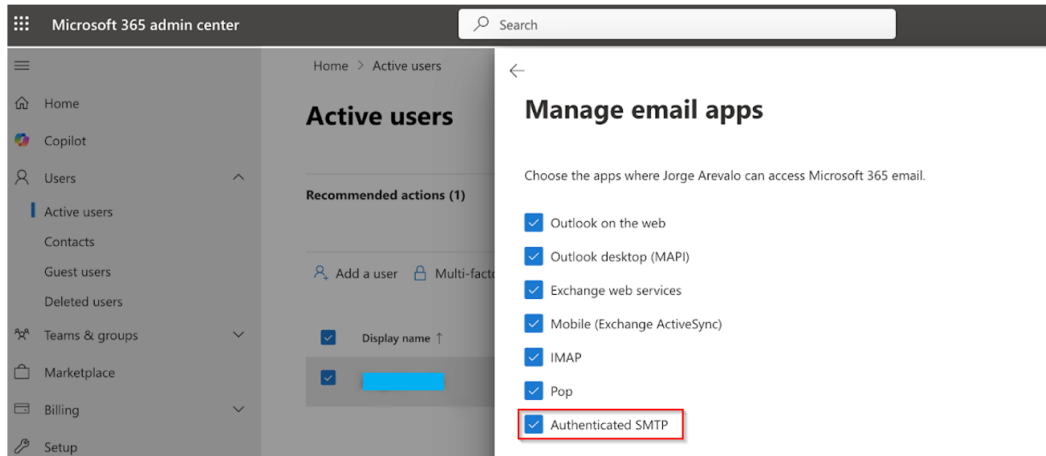
Mailbox permissions

Read and manage permissions (0)
Send as permissions (0)
Send on behalf of permissions (0)

Email apps

All apps allowed
[Manage email apps](#)

2. Ensure that the checkbox option "Authenticated SMTP" is selected.



Step 4: Configure SMTP in Your Gateway

1. **Access the Gateway GUI**
 - o Log in to your device's configuration interface from internal interface (LAN side).
 - o Navigate to **System > Notification > Mail Server**
2. **Enter SMTP Settings**
 - o **Mail Server:** smtp.office365.com
 - o **Port:** 587 (recommended, supports STARTTLS).
 - o **Encryption:** Enable **TLS Security** and **STARTTLS**
 - o **Authentication Method:** Select **Microsoft OAuth2.0**.
 - o **Sender Email Address:** Enter the Microsoft 365 email address (e.g., sender@yourdomain.com).
 - o **Client ID:** Paste the Application (client) ID from Step 1-4.
 - o **Client Secret:** Paste the client secret value from Step 1-5.
 - o **Tenant ID:** Paste the Directory (tenant) ID from Step 1-4.
3. **Apply Configuration**
 - o You must click **Apply** before requesting a token.
 - o Click **Apply** to save the configuration on your gateway.

System > Notification > Mail Server

Mail Server Alert

General Settings

Mail Server: smtp.office365.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (1-65535)

TLS Security: ☒

STARTTLS: ☒

Authenticate Server: ☐

Authentication Method: Microsoft OAuth2.0 [How to set up SMTP with Microsoft OAuth2.0](#)

Sender Email Address: jeff.lin@zyxel.com.tw

Client ID: 27cba1b2-fad2-4c0e-9ee9-d93d4c33a082

Client Secret:

Tenant ID: d44c31fd-3401-417a-f157-d70de43e956d

Token Status: No token available – click "Get New Token"

Get New Token **Refresh Token Status**

Default Sender and Recipient

Recipient: Email Address

Send Test Email

4. Obtain OAuth 2.0 Token

- o After applying the configuration, click **"Get New Token"** button.
- o This will **open a new browser tab** to the Microsoft Azure sign-in page.
- o Sign in with the Microsoft 365 account associated with the sender email address (e.g., [sender@yourdomain.com](#)).
- o Grant permissions when prompted
- o The browser will close automatically upon successful authentication, and your gateway will have securely obtained an authentication token from Microsoft.
- o The **Token Status** field will update. (e.g., "Valid").
- o **If the browser does not open:** Click the **"Refresh Token Status"** button to check if the token was successfully obtained or to retry the token retrieval process.

System > Notification > Mail Server

Mail Server Alert

General Settings

Mail Server: smtp.office365.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (1-65535)

TLS Security: ☒

STARTTLS: ☒

Authenticate Server: ☒

Authentication Method: Microsoft OAuth2.0 [How to set up SMTP with Microsoft OAuth2.0](#)

Sender Email Address: jerry@zyxel.com.tw

Client ID: 27cba1b2-fad2-4c0e-9a67-8f3d94235a82

Client Secret:

Tenant ID: d44c31fd-3401-4c79-f137-d73e45a9f8a8

Token Status: No token available – click "Get New Token"

Get New Token **Refresh Token Status**

Default Sender and Recipient

Recipient: Email Address

Send Test Email

Verify the SMTP with Microsoft OAuth2.0 function

1. Ensure token is successfully acquired.

System > Notification > Mail Server

Mail Server Alert

General Settings

Mail Server: smtp.office365.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (1-65535)

TLS Security: ☒

STARTTLS: ☒

Authenticate Server: ☒

Authentication Method: Microsoft OAuth2.0 [How to set up SMTP with Microsoft OAuth2.0](#)

Sender Email Address: jerry@zyxel.com.tw

Client ID: 27cba1b2-fad2-4c0e-9a67-8f3d94235a82

Client Secret:

Tenant ID: d44c31fd-3401-4c79-f137-d73e45a9f8a8

Token Status: **Valid**

Get New Token **Refresh Token Status**

Default Sender and Recipient

Recipient: Email Address

Send Test Email

Fill in the recipient email address and send a test email.

Navigate to **Log & Report > Log/Events > System** and check for the successful token-retrieval log message.

Log & Report > Log / Events > System							
System		APC	AP				
Category		All Log	Clear Log		Export	Refresh	Search insights
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
63	2025-07-02 20:56:47	System	[Notification][Mail Server]Get OAuth2.0 refresh token success!	0.0.0.0	0.0.0.0	0	

- Navigate to **Log & Report > Email Daily Report > Send Report Now** to send an email through your firewall.

Log & Report > Email Daily Report

General Settings

Enable Email Daily Report

Reset All Counters

Email Settings

Note
Please set up the Mail Server to send system statistics via email every day.

Email Subject

Email from

Recipients

Send Report Now

Reset counters after sending report successfully.

Report Items

System Resource Usage

Traffic Statistics

Security Services

Ensure that the email is successfully received in the mailbox.

E-mail Report usgflex200hp 2025-07-02 21:01 +08:00

usgflex200hp@zyxel.com.tw

General

Model Name: USG FLEX 200HP
Firmware Version: V1.35(ABXE.0)4 | 2025-06-25 06:26:12
MAC Address Range: 08:00:27:0C:00:00-08:00:27:0C:00:08
System Uptime: 2 days, 7:06:20
System Name: usgflex200hp

Licensing

License Status

Signature Status

Service Name	Status	Service Type
Web Filtering	Activated	standard
Secure WIFI	Activated	standard
Security Profile Sync	Activated	standard
SecuReporter	Activated	standard
Application Patrol	Activated	standard
Anti-Malware	Activated	standard
Device Insight	Activated	standard
IPS	Activated	standard
Sandboxing	Activated	standard

Troubleshooting

1. **Authentication Failed:**

- o Double-check credentials: Ensure that the Client ID, Tenant ID, and Client Secret are copied precisely without any extra spaces.
- o Ensure admin consent was granted for API permissions
- o Check that the sender email address exists in your Microsoft 365 tenant

2. **Permission Denied:**

- o Confirm API permission is granted (Step2-1).
- o Verify the application has admin consent
- o Check that the sender email account is active

3. **Client Secret Expired:**

Generate a new client secret in Azure Portal and update it in the gateway settings.

4. **Connection Issues:**

- o Verify SMTP server settings (smtp.office365.com:587). Ensure port 587 is unblocked.
- o Ensure STARTTLS encryption is enabled
- o Check firewall/network connectivity

5. **Browser Issues:**

- o **Browser doesn't open:** Check if pop-up blockers are enabled and allow pop-ups for the gateway
- o **Browser opens but shows error:** Verify the Azure application redirect URI configuration. And make sure the administrator's PC located in the network that can access the URI (Located in LAN side of gateway is recommend).
- o **Token not acquired after sign-in:** Click "Refresh Token Status" button to check token status
- o **Multiple browser tabs open:** Close extra tabs and try again
- o **Browser doesn't close automatically:** Manually close the tab after successful sign-in

6. **Token Issues:**

- o **Token acquisition failed:** Verify internet connectivity and try clicking "Get New Token" again
- o **Token expires quickly:** This is normal - the gateway will automatically refresh tokens
- o **"Refresh Token Status" button shows no token:** Repeat the "Get New Token" process
- o **Token status not updating:** Wait 10-15 seconds then click **"Refresh Token Status"** again

Security Best Practices

1. **Secret Management:**

- o Store client secrets securely
- o Rotate secrets before expiration
- o Use different applications for different purposes

2. **Access Control:**

- o Grant minimum required permissions only
- o Regularly review application permissions
- o Monitor application usage through Azure logs

3. **Monitoring**

- o Enable audit logging in Microsoft Entra ID
- o Monitor for unusual authentication patterns
- o Set up alerts for failed authentication attempts

Additional Information

1. **Token Lifecycle:**

- o Access tokens expire after 1 hour
- o Your gateway automatically handles token refresh
- o Initial token must be acquired through browser sign-in
- o Subsequent token renewals happen automatically in the background
- o No user interaction required for token renewal after initial setup

2. **Supported Email Types:**

- o Plain text emails
- o HTML formatted emails
- o Emails with attachments
- o Bulk email sending (within Microsoft limits)

3. **Rate Limits** – Microsoft imposes sending limits

- o 30 messages per minute
- o 10,000 messages per day (default)
- o Higher limits available through Microsoft support

4. **Support** – If you encounter issues:

- o Verify all steps were completed correctly
- o Check Microsoft Entra ID audit logs for authentication errors
- o Contact your system administrator for Azure access issues
- o Refer to Microsoft's official OAuth 2.0 documentation


For technical support with your gateway device, contact our support team with your configuration details (never share client secrets).

Chapter 6- Nebula

How to Set Up Nebula site-to-site VPN on the USG FLEX H?

This example shows how to use Nebula VPN to establish Site to Site VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Site-to-Site VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



 **Note:** Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

Set Up the Site-to-Site VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Site-to-Site VPN topology.

USG FLEX/ATP site

The screenshot shows the Nebula Control Center interface for a USG FLEX/ATP site. The top navigation bar includes the Nebula logo, Organization dropdown, and Site dropdown (set to ATP200). The breadcrumb trail is Site-wide > Configure > Firewall > Site-to-Site VPN.

Site-to-Site VPN Configuration:

- Primary interface:** wan1
- Secondary interface:** wan2
- Local networks:**

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

Nebula VPN Configuration:

- Enabled:** ☒
- VPN Area:** Default
- VPN topology:** Split tunnel (send only site-to-site traffic over the VPN)
 - Site-to-Site:** ☒
- ADVANCED OPTIONS:**
 - Area communication:** ☐
 - NAT traversal:**
 - ☐ None
 - ☒ Custom NAT traversal
- Peer VPN networks:**

Network	Subnet(s)
USG Flex 200HP	192.168.168.1/24

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestration](#) to save your time.

USG FLEX H site

Organization: [J&J Enterprises, Inc.](#) > Site: USG Flex 200HP

Site-wide > Configure > Firewall > [Site-to-Site VPN](#)

Site-to-Site VPN

Primary interface: ge1_ppp

Secondary interface: ge2

Local networks

Name	Subnet	Use VPN
ge3	192.168.168/24	<input checked="" type="checkbox"/>
ge4	192.168.169/24	<input type="checkbox"/>

Nebula VPN

Enabled: ☒

VPN Area: Default

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)
Site-to-Site

Area communication: ☐

NAT traversal: ☐ None ☒ Custom NAT traversal IP

Peer VPN networks

Network	Subnet(s)
ATP200	192.168.66.0/24

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

Verify the VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

Organization: [J&J Enterprises, Inc.](#) > Site: ATP200

Site-wide > Monitor > Firewall > [VPN connections](#)

VPN connections

Connection status
 Configuration: This security gateway is exporting 1 subnet over the VPN 192.168.66.0/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168/24	connected	25.50 KB	33.26 KB	1038	2025-01-07 14:52:01

Organization: [J&J Enterprises, Inc.](#) > Site: USG Flex 200HP

Site-wide > Monitor > Firewall > [VPN connections](#)

VPN connections

Connection status
 Configuration: This security gateway is exporting 1 subnet over the VPN 192.168.168/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66/24	connected	109.38 KB	109.38 KB	879	2025-01-07 14:46:19

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

ZYXEL USG FLEX 200HP

VPN Status > IPsec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh


	#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
Nebula VPN										
	1	SA_BCP118028	111.243.200.200	5182L372000	59.115.115.115	0.0.0.0 <-> 0.0.0.0	2544	24987	2623 (157.38K bytes)	2600 (156K bytes)

VPN Status
IPsec VPN
SSL VPN

How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)?

This example shows how to establish Hub-and-Spoke VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



 **Note:** Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke VPN topology and ensure that the USG FLEX H is set as the Hub site.

USG FLEX H site

Organization: [\[Organization\]](#) > Site: USG Flex 200HP

Site-wide > Configure > Firewall > [Site-to-Site VPN](#)

Site-to-Site VPN

Primary interface: [ge1_PPP](#)

Secondary interface: [ge2](#)

Local networks

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>

Nebula VPN

Enabled: ☒

VPN Area: [Default](#)

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)
[Hub-and-Spoke](#)

Hubs (peers connect to)

SiteName
1 USG Flex 200HP

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

USG FLEX/ATP site

nebulas Control Center Organization: [Organization] Site: ATP200

Site-wide > Configure > Firewall > Site-to-Site VPN

Site-to-Site VPN

Primary interface: wan1

Secondary interface: wan2

Local networks

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

Nebula VPN

Enabled: ☒

VPN Area: Default

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke: Hub-and-Spoke

Hubs (peers connect to)

SiteName
1 USG Flex 200HP

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

Verify The VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

nebulas Control Center Organization: [Organization] Site: USG Flex 200HP

Site-wide > Monitor > Firewall > VPN connections

VPN connections

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN 192.168.66.0/24

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.0/24	connected	0/42 KB	105.47 KB	437	2025-01-07 16:06:26

nebulas Control Center Organization: [Organization] Site: ATP200

Site-wide > Monitor > Firewall > VPN connections

VPN connections

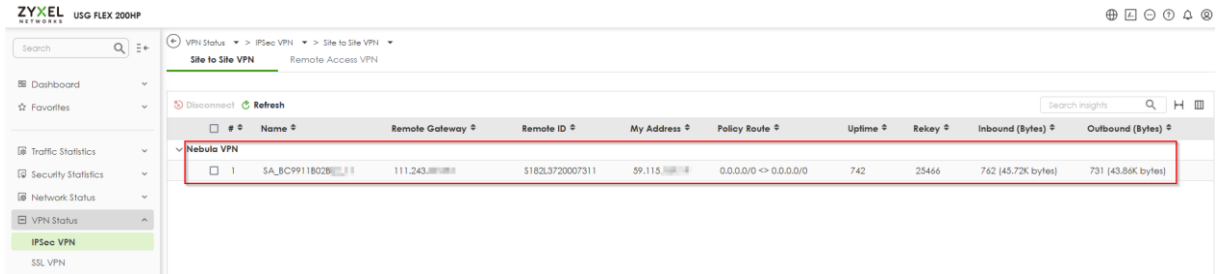
Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN 192.168.66.0/24

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.66.0/24	connected	13.25 KB	19.10 KB	316	2025-01-07 16:04:09

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.




	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
▼	Nebula VPN								
<input type="checkbox"/>	1 SA_B09911802B	111.243.	51823720007311	59.115.	0.0.0.0/0 <> 0.0.0.0/0	742	25466	762 (45.72K bytes)	731 (43.86K bytes)

How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)?

This example shows how to use Nebula VPN to establish Hub-and-Spoke VPN tunnel between USG FLEX/ATP and USG FLEX H. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.

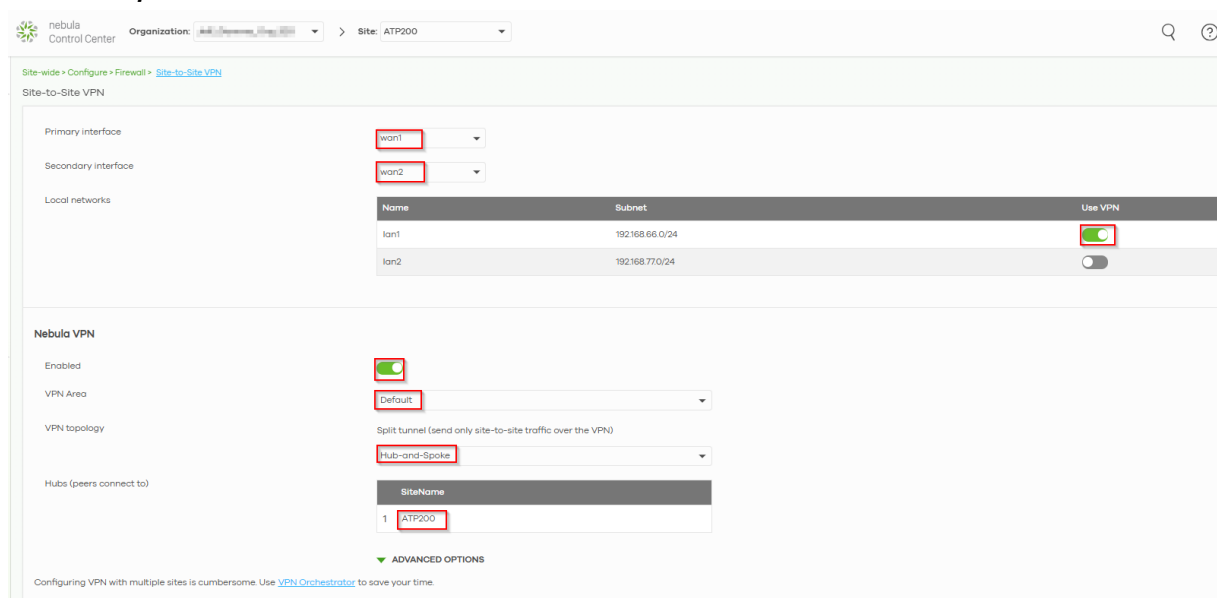


 Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke VPN topology and ensure that the USG FLEX H series is set as the Spoke site.

USG FLEX/ATP site



The screenshot shows the Nebula Control Center interface for configuring Site-to-Site VPN. The breadcrumb trail is: Site-wide > Configure > Firewall > Site-to-Site VPN. The current site is ATP200.

Site-to-Site VPN Configuration:

- Primary interface: wan1
- Secondary interface: wan2
- Local networks:

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

Nebula VPN Configuration:

- Enabled: ☒
- VPN Area: Default
- VPN topology: Split tunnel (send only site-to-site traffic over the VPN). Selected: Hub-and-Spoke
- Hubs (peers connect to):

SiteName
1 ATP200

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

USG FLEX H site

Organization: [jedi-systems,org,1001](#) > Site: USG Flex 200HP

Site-wide > Configure > Firewall > [Site-to-Site VPN](#)

Site-to-Site VPN

Primary interface:

Secondary interface:

Local networks

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>

Nebula VPN

Enabled: ☒

VPN Area:

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hubs (peers connect to)

SiteName
1 <input type="text" value="ATP200"/>

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

Verify The VPN connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

Organization: [jedi-systems,org,1001](#) > Site: ATP200

Site-wide > Monitor > Firewall > [VPN connections](#)

VPN connections

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.66.0/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168.1/24	connected	26.71 KB	34.84 KB	869	2025-01-07 17:46:52

Organization: [jedi-systems,org,1001](#) > Site: USG Flex 200HP

Site-wide > Monitor > Firewall > [VPN connections](#)

VPN connections

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.168.1/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.1/24	connected	93.05 KB	89.77 KB	439	2025-01-07 16:36:32

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

ZYXEL USG FLEX 200HP

VPN Status > IPsec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BC9911802888	111.243.208.101	182L372000	1.161.1.101	0.0.0.0/0 <- 0.0.0.0/0	140	27197	139 (8.34K bytes)	143 (8.58K bytes)

Search insights

How to Onboard Firewall to Nebula within Initial Setup Wizard

In the initial setup wizard, there are 2 ways to onboard your firewall to Nebula. One is started by Web Configurator (Local configure first), and the other one is started from Nebula CC (Cloud configure first). A brand new firewall with version 1.35 and default configuration will start with the Initial Setup Wizard. You can follow these steps to onboard your firewall, no matter whether it's started by Web Configurator or Nebula CC.

Onboarding via Web Configurator (Local Configuration First)

You can choose to onboard your firewall locally by selecting Web Configurator.

Do you want to use Nebula or the Web Configurator for initial configuration?



Nebula

First, register your Device in the next screen, then Nebula will send the initial configuration to your Device. (If you have already set up Nebula.)



Web Configurator

Continue with the local wizard.

☐ Restore from a file
Import configuration (.conf) or Recovery Manager backup file (.rbf).

Next

In Step 3, The Web GUI will prompt you to register your firewall.

Device Registration

If you have activated licenses on another Zyxel portal like myZyxel.com, you can use all Zyxel Device services except SecuReporter and remote support through Nebula.

Create an Organization and Site on Nebula to be able to use SecuReporter and remote support.

Registration Status: **Incomplete**

Back Next

Click **Next** to proceed. The browser will redirect you to the Nebula Control Center (NCC), where you must assign the firewall to an existing Organization and Site or create a new one.

01

With Nebula Control Center, you can efficiently manage multiple USG FLEX H firewalls along with other Zyxel devices in a single window, including on/off monitoring, firmware management, configuration backup/restore, and accessing the remote GUI.

To register your USG FLEX H firewall with Nebula, please select an Organization and a Site under your authority, or create new ones.

You organize Zyxel devices in Nebula into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory".

First step is to create your Organization and Site

Organization ●
Organization name

Site
Site name x *

Next

After clicking **Next**, your firewall will be registered to Nebula server.

02

Please review your device & license information.

Here's your device information

Device name	D8:EC:E5:5C:0E:14
Mac address	D8:EC:E5:5C:0E:14
Serial number	S212L16295034
Model name	USG FLEX 200HP
License	Gold Security Pack 390 Days

The license includes:
Web Filtering, Anti-Malware, Application Patrol, IPS, Reputation Filter, SecuReporter, Device Insight, Sandboxing, Security Profile Sync and Nebula Professional Pack.

Back

Next

Let's take a look for what you had done

Organization summary

- Organization:Stanley_Gamma_TEST
- Site:200HP_Handbook

Devices

MAC address: D8:EC:E5:5C:0E:14

Serial number: S212L16295034

Model name: USG FLEX 200HP

Everything seems fine, ready to go?

Register

Once registration is complete, your browser will return to the Initial Setup Wizard, and showing the device registration status.

✓ Connect To Internet

✓ System Time

3 Device Registration

4 License Summary

5 Subnet Planning

6 Finish

Device Registration

Congratulations!

You have successfully completed the registration process. Click "Next" to finalize the installation wizard.

Back

Next

✓ Connect To Internet

✓ System Time

✓ Device Registration

4 License Summary

5 Subnet Planning

6 Finish

License Summary

Refresh

Service	Status	Expiration
Nebula Professional Pack Trial	Activated	2025/12/31
IPS Trial	Activated	2025/12/31
Anti-Malware Trial	Activated	2025/12/31
Application Patrol Trial	Activated	2025/12/31
Security Profile Sync Trial	Activated	2025/12/31
Web Filtering Trial	Activated	2025/12/31
SecuReporter Trial	Activated	2025/12/31
Reputation Filter Trial	Activated	2025/12/31
Device Insight Trial	Activated	2025/12/31
Sandboxing Trial	Activated	2025/12/31
Secure WIFI Trial	Activated	2025/12/31

Back

Next

In step 5, you can choose whether to use the default interface IP address or apply the interface IP address already configured in Nebula server. If need using Nebula SD VPN suggestion to select "Yes" to apply Nebula site assign IP subnet to avoid subnet conflict.

✓ Connect To Internet

✓ System Time

✓ Device Registration

✓ License Summary

5 Subnet Planning

6 Finish

Subnet Planning

Nebula VPN automatically create and provision VPN tunnels to all Nebula firewalls within the same organization.

To avoid IP subnet conflicts among Nebula firewalls participating VPNs, the Auto Subnet Planning feature replaces default subnets of ge3/ge4 with non-overlapping subnets.

Enable Auto Subnet Planning?

☐ Yes, let Nebula adjust subnets of ge3/ge4.

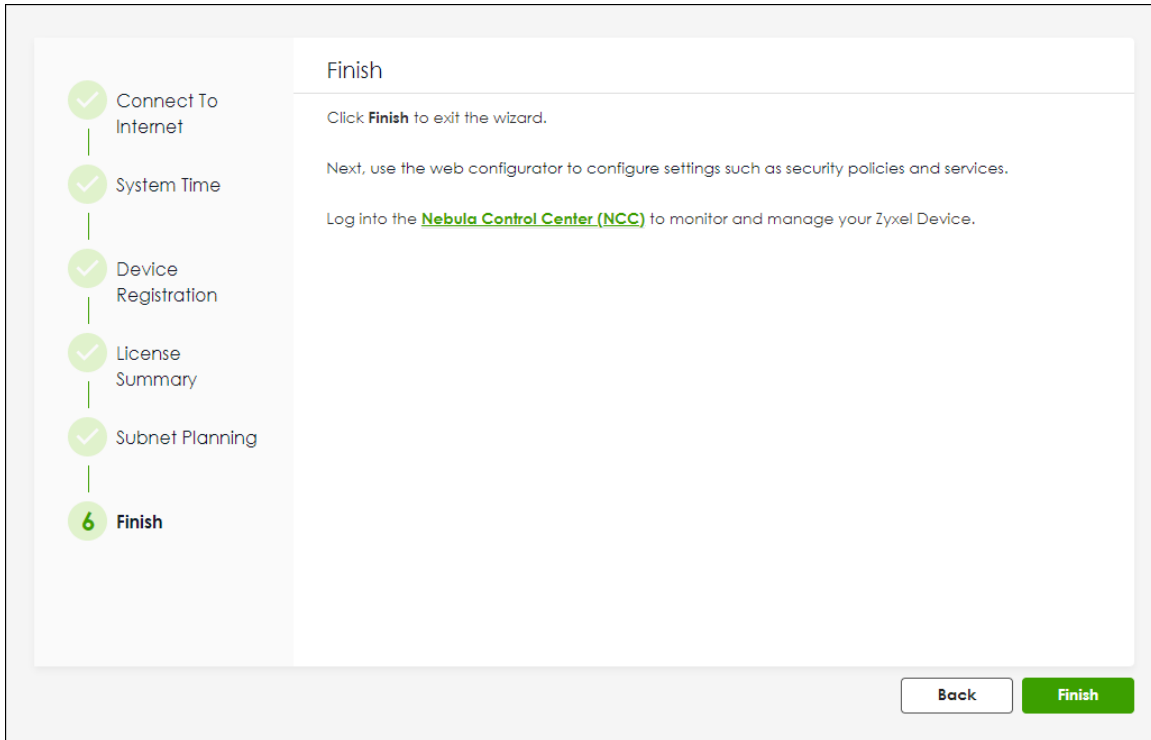
☒ No, I prefer to keep using default subnets of ge3/ge4.

Important notice: In VPN scenario, connection may fail when the internal subnet of a firewall conflicts with the others. The problem happens when the firewall uses default subnets participating VPNs and you have to manually adjust internal subnets to fix the problem.

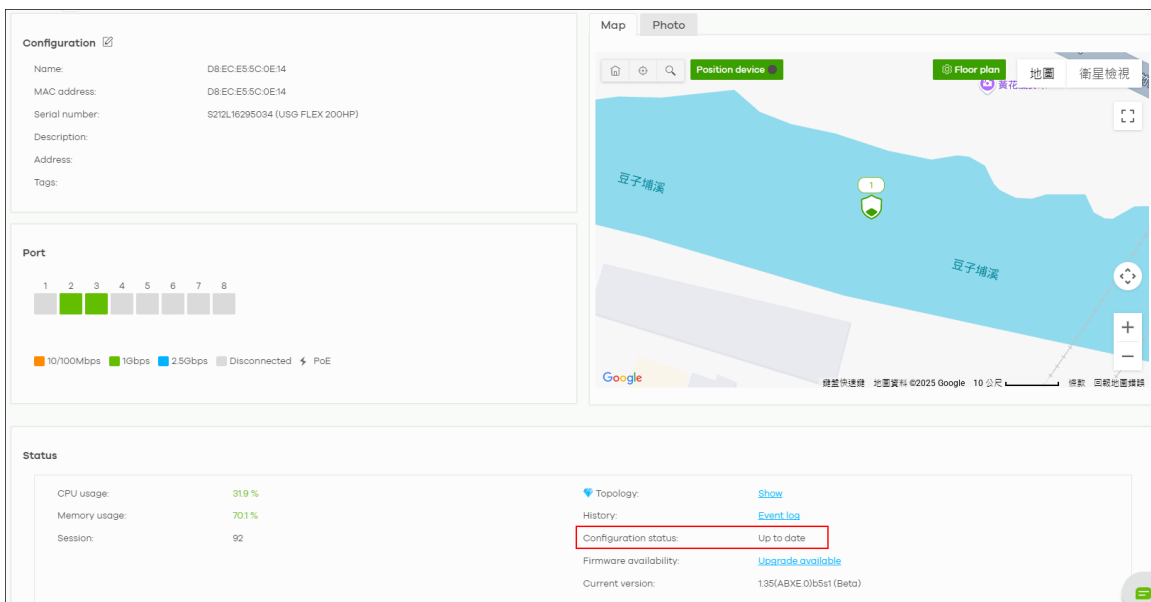
Back

Next

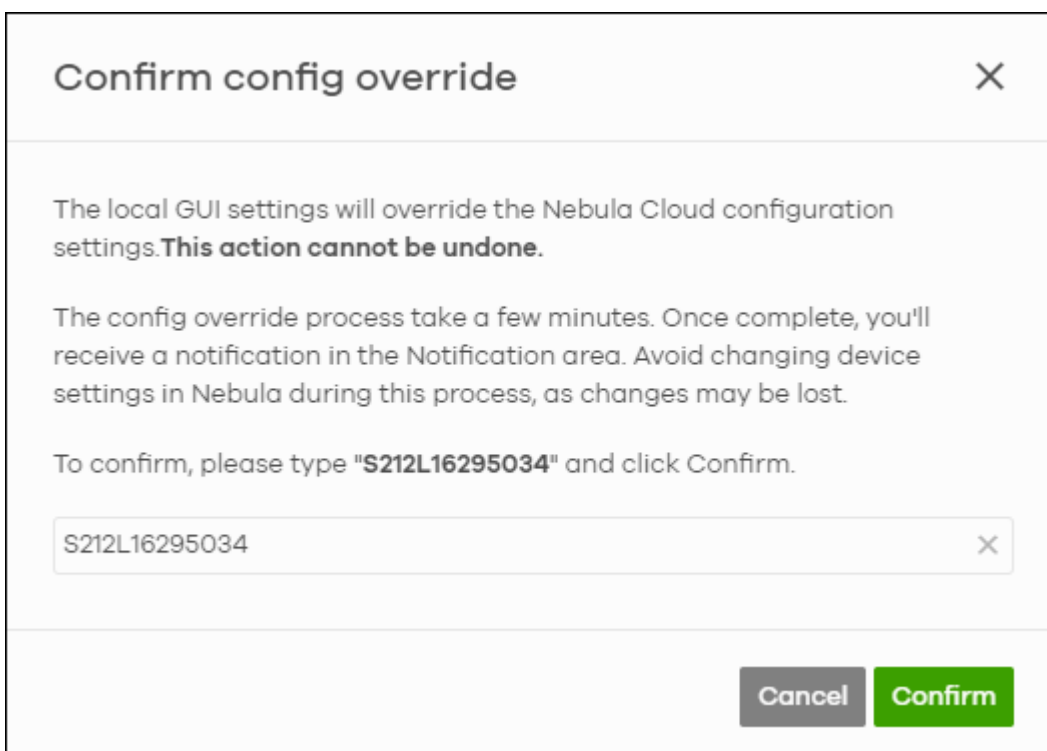
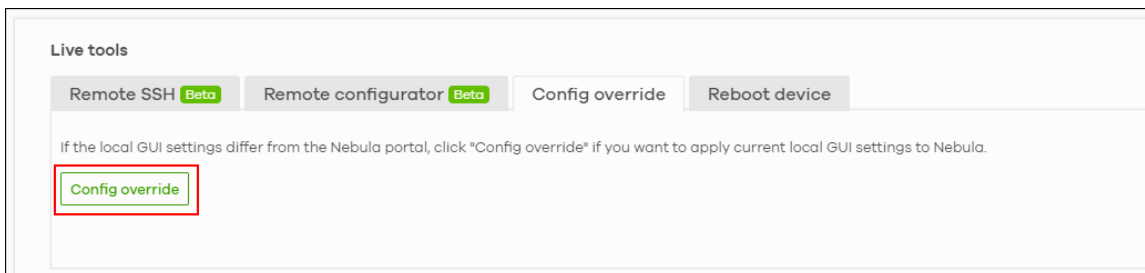
In Step 6, Click **Finish** to close the wizard from Web GUI.



After completing the wizard, you can log in to Nebula Control Center (NCC) to check your firewall status. Ensure the **Configuration Status** shows **Up to date**, indicating the firewall has fully synchronized with the cloud.



If needed, you can click **Config Override** to force a configuration sync from the firewall to the Nebula server immediately.



Onboarding via Nebula (Cloud Configuration First)

You can also onboard your firewall by registering it to Nebula in advance or by pre-configuring it in your site settings. Once your firewall connects to the Internet and NCC, configuration will be automatically provisioned from Nebula to the device.

Go to <https://nebula.zyxel.com/>, log in with your Zyxel account, and create a new Organization and Site.

[hs2]

01 _____

With Nebula Control Center, you can efficiently manage multiple USG FLEX H firewalls along with other Zyxel devices in a single window, including on/off monitoring, firmware management, configuration backup/restore, and accessing the remote GUI.

To register your USG FLEX H firewall with Nebula, please provide your Organization and Site names.

You organize Zyxel devices in Nebula into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory".

First step is to create your Organization and Site

Organization

Organization name

Site

Site name

Country

Taiwan

Time zone

Asia - Taipei (UTC +8.0)

Next

Click **Add** to register your firewall to the created site.

Add devices

[Add devices](#)

Firmware upgrade

Devices

Enter one or more MAC address and serial number.

Or you can download the [template](#) here and [import](#) multiple records for faster registration.

[What Zyxel devices support Nebula?](#)

[Where can I find these numbers?](#)













MAC address	Serial number	Name	Model	License info	Expiration date
D8:EC:E5:5C:0E:14 <input type="text"/>	S212L16295034 <input type="text"/>	D8:EC:E5:5C:0E:14 <input type="text"/>	USG FLEX 200HP	Gold Security Pack	2026-08-15

[+ Add another device](#)

Next


Cancel

You can pre-configure interface settings in Nebula to match your network environment.

Interface									
External									
Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description	Reference	
ge1					p1	WAN		View	 
ge2		192.168.1.55	255.255.255.0		p2	WAN		View	 
+Add									
Internal									
Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description	Reference	
ge3		192.168.68.1	255.255.255.0		p3 p4 p5 p6	LAN		View	 
ge4		192.168.69.1	255.255.255.0		p7 p8	LAN		View	 
+Add									


The default WAN setting on the firewall is DHCP. If your Internet connection also uses DHCP, you can simply connect the WAN cable to the firewall without needing to manually configure the device through the wizard.

Do you want to use Nebula or the Web Configurator for initial configuration?



Nebula

First, register your Device in the next screen, then Nebula will send the initial configuration to your Device. (If you have already set up Nebula.)



Web Configurator

Continue with the local wizard.

☐ Restore from a file
Import configuration (.conf) or Recovery Manager backup file (.rbf).

[Next](#)

In Step 1, Configure the WAN IP address to ensure the firewall can connect to the Internet.

1 Connect To Internet

2 System Time

3 Device Registration

4 License Summary

5 Finish

Connect To Internet

Interface Type: Static

Port: p2

Address Assignment

WAN IP: 192.168.1.101

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

First DNS Server: 8.8.8.8

Second DNS Server: 1.1.1.1

VLAN Tag: ☐

Connection Test ✔ Pass

Next

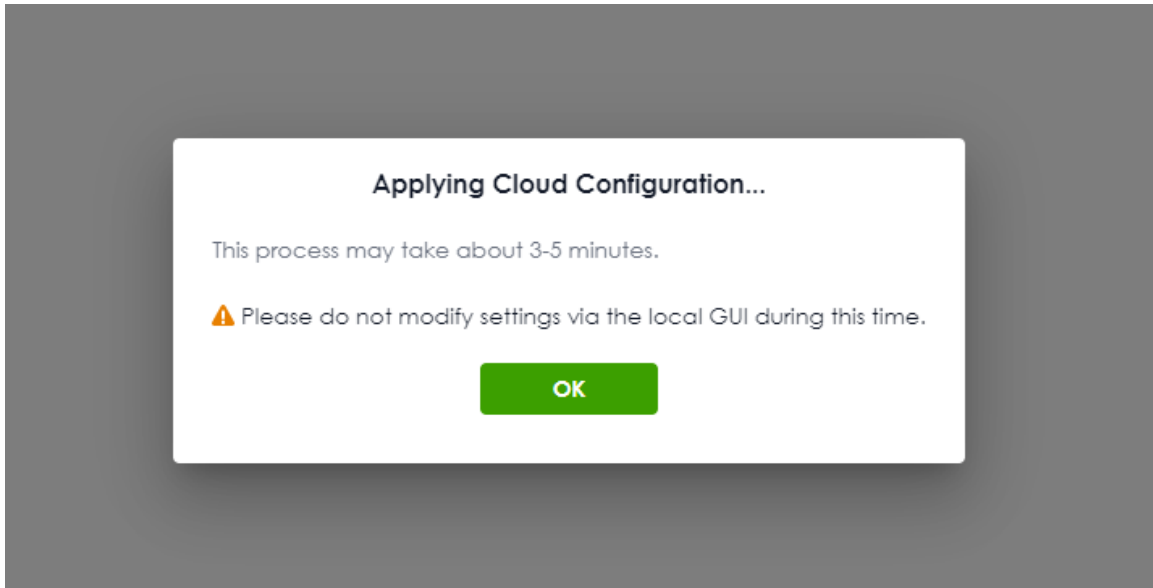
Once connected to the Internet and Nebula CC, the wizard will automatically verify the device's registration status.

The screenshot shows the 'Device Registration' step of a ZyXel installation wizard. On the left, a vertical progress bar lists five steps: 'Connect To Internet' (checked), 'System Time' (checked), '3 Device Registration' (highlighted with a green circle), '4 License Summary' (grey), and '5 Finish' (grey). The main content area is titled 'Device Registration' and contains the text: 'Congratulations! You have successfully completed the registration process. Click "Next" to finalize the installation wizard.' At the bottom right, there are two buttons: 'Back' and 'Next'.

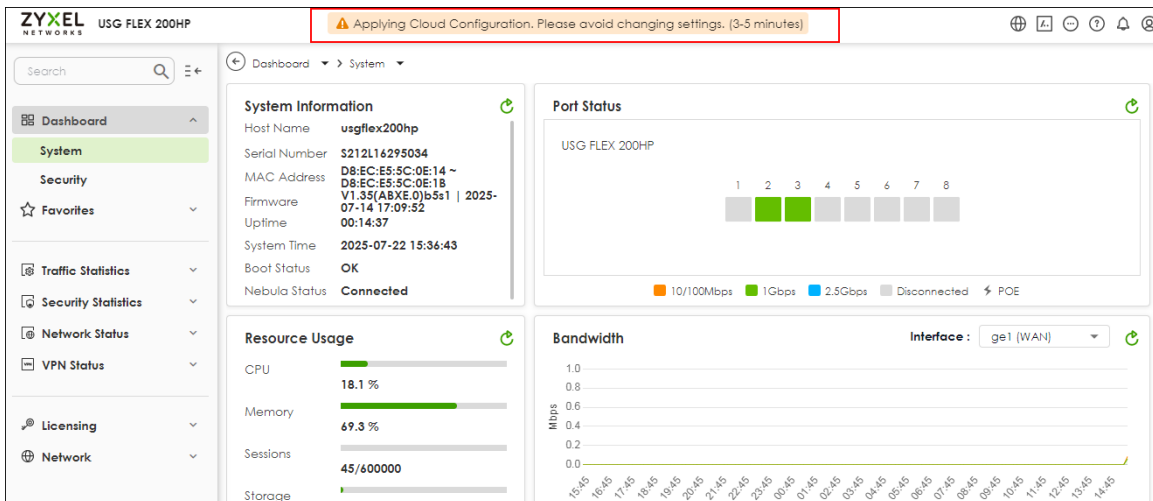
In step 5, Click **OK** to finish the wizard. Please wait 3–5 minutes for Nebula CC to provision the configuration to the firewall.

The screenshot shows the 'Finish' step of the ZyXel installation wizard. The left progress bar now shows 'Device Registration' as checked, and '5 Finish' is highlighted with a green circle. The main content area is titled 'Finish' and displays: 'Applying Cloud Configuration... This process may take about 3-5 minutes.' Below this is an orange warning box with a triangle icon and the text: 'Please do not modify settings via the local GUI during this time.' Further down, it says: 'You can monitor the status and manage your Zyxel device in the [Nebula Control Center \(NCC\)](#).' At the bottom right, there is a single green button labeled 'OK'.

Before the configuration is fully applied, a notification message will appear. You will also see a banner at the top of the page.



You will also see a banner at the top of the page. Please wait 3–5 minutes until all settings from Nebula are applied. Once the synchronization is complete, the warning message will disappear.



You can also monitor the firewall's status on the Nebula site and ensure the **Configuration Status** becomes **Up to date**.

The screenshot displays the Zyxel Nebula management interface for a specific firewall device. The interface is divided into several sections:

- Configuration:**
 - Name: D8:EC:E5:5C:0E:14
 - MAC address: D8:EC:E5:5C:0E:14
 - Serial number: S212L16295034 (USG FLEX 200HP)
 - Description:
 - Address:
 - Tags:
- Port:**
 - A row of 8 port status indicators. Ports 1 and 2 are green, indicating they are active. Ports 3 through 8 are grey, indicating they are disconnected.
 - Legend: 10/100Mbps (orange), 1Gbps (green), 2.5Gbps (blue), Disconnected (grey), PoE (lightning bolt icon).
- Map:**
 - Shows a map of the device's location with a green pin and a shield icon.
 - Buttons: "Position device", "Floor plan", "地圖", "衛星檢視".
- Status:**
 - CPU usage: 31.9 %
 - Memory usage: 70.1 %
 - Session: 92
 - Topology: [Show](#)
 - History: [Event log](#)
 - Configuration status: Up to date** (highlighted with a red box)
 - Firmware availability: [Upgrade available](#)
 - Current version: 1.35(ABXE.0)b5s1 (Beta)