

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 1.39

Jul. 2026

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	18
How to Configure IPSec Site to Site VPN while one Site is behind a NAT router	24
How to Configure Remote Access VPN with Zyxel VPN Client	36
How to Configure Site-to-site IPSec VPN between ZLD and uOS device	56
How to Configure Route-Based VPN	67
How to Use Tailscale.....	79
How to use Ext-group user to connect Remote Access VPN.....	91
How to Configure SSL VPN Access Profile	94
Chapter 2- Security Service	100
How to Block HTTPS Websites Using Content Filtering and SSL Inspection	100
How to Configure Content Filter with HTTPs Domain Filter	109
How to Block Facebook Using a Content Filter Block List	114
How to block YouTube access by Schedule	118
How to Control Access to Google Drive	127
How to Block the Spotify Music Streaming Service	135
How does Anti-Malware Work	138
How to Detect and Prevent TCP Port Scanning with DoS Prevention	141
How to block the client from accessing to certain country using Geo IP?	145
How to Use Sandbox to Detect Unknown Malware?	150
How to Configure Reputation Filter- IP Reputation.....	154
How to Configure Reputation Filter- URL Threat Filter.....	159

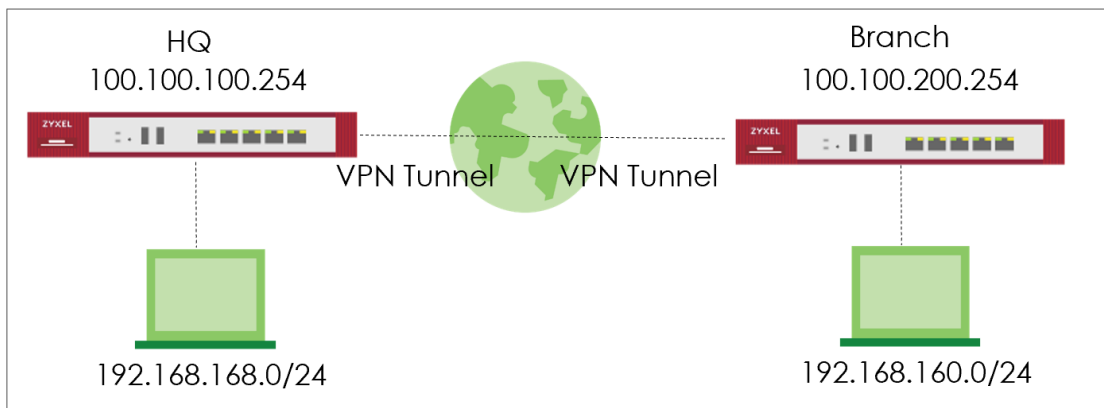
How to Configure Reputation Filter- DNS Threat Filter	163
How to Configure DNS Content Filter	168
External Block List for Reputation Filter	173
How to set up DNS SafeSearch?	178
Chapter 3- Authentication	186
How to Use Two Factor with Google Authenticator for Admin Access	186
How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN	194
How to set up AD authentication with Microsoft AD	204
How to Set Up Captive Portal?	209
Captive Portal authentication with Google	219
Captive Portal authentication with Microsoft Entra ID	239
SSLVPN authentication with Google	259
SSLVPN authentication with Microsoft Entra ID	272
Captive Portal authentication with Microsoft Entra ID Group	282
Chapter 4- Maintenance	289
How to Manage Configuration Files	289
How to Manage Firmware	293
How to set up configuration file backup rotation	295
Chapter 5- Others	299
How to Setup and Configure Daily Report	299
How to Setup and Send Logs to a Syslog Server	304
How to Setup and Send logs to the USB storage	307
How to Perform and Use the Packet Capture Feature	309
How to Allow Public Access to a Server Behind USG FLEX H	313
How to Configure DHCP Option 60 – Vendor Class Identifier	317
How to Configure Session Control	319

How to Configure Bandwidth Management for FTP Traffic	322
How to Configure WAN trunk for Spillover and Least Load First	327
How Does SIP Pinhole Function Work on USG FLEX H?	333
How to Deploy Device HA	338
How to check Packet Flow Explorer	352
How to set up a Link Aggregation Group (LAG) interface	358
How to Set Up AP Control Service for Zyxel APs	364
How to set up SMTP with Microsoft OAuth2.0?	369
How to Configure IGMP Proxy	382
How to Configure Application-Based Policy Route	388
How to Configure ACME client for Let's Encrypt	391
Chapter 6- Nebula	401
How to Set Up Nebula site-to-site VPN on the USG FLEX H?	401
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)?	405
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)?	409
How to Onboard Firewall to Nebula within Initial Setup Wizard	413
How to Configure Remote Access VPN with Nebula Cloud Authentication?	426
How to Configure CDR on Nebula	448
Nebula identity federation service (NID FS) support Captive Portal	460
Nebula identity federation service (NID FS) support SSL VPN	475

Chapter 1- VPN

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

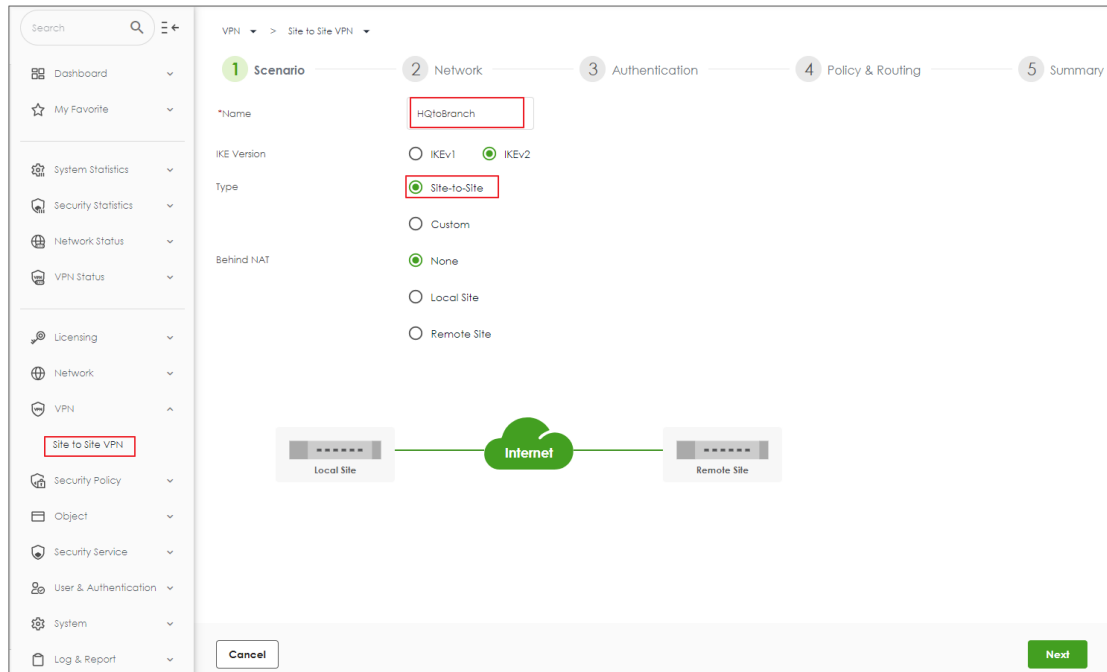
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



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, with 'Next' being a green button.

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	*****
----------------	----------------	-------

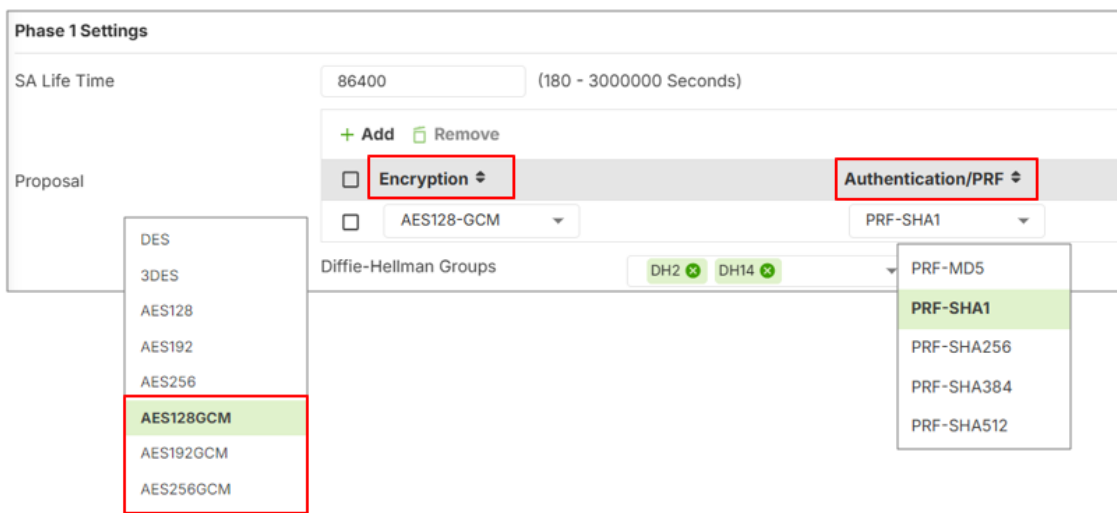
Policy & Routing

Local Subnet	192.168.168.0/24
Remote Subnet	192.168.160.0/24

Close

 Note: Beginning with uOS 1.37, IKEv2 supports AES-GCM encryption.

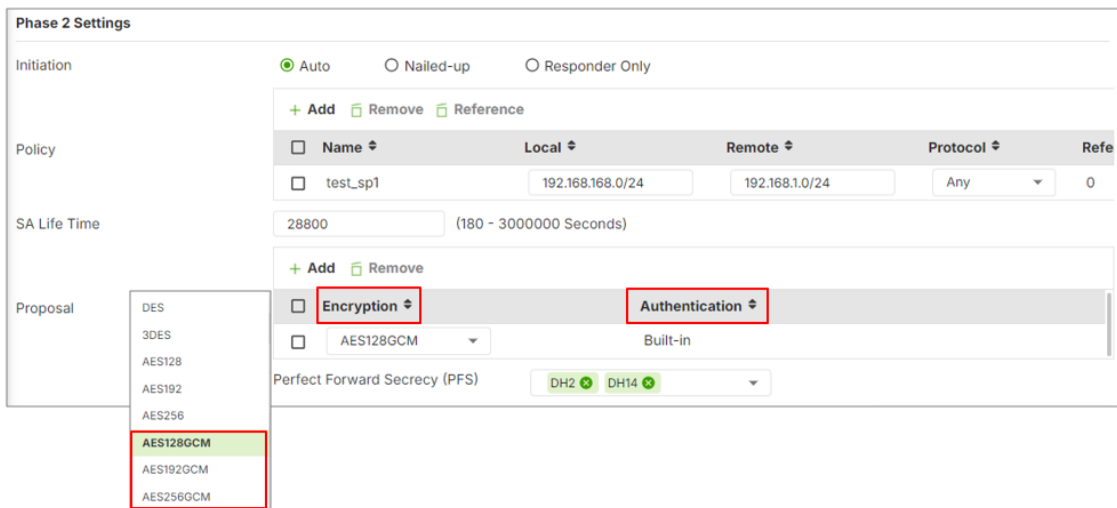
Phase 1 Settings - When AES-GCM is selected, PRF algorithm is used for key derivation. Authentication is not used.



The Phase 1 Settings interface shows the following configuration:

- SA Life Time:** 86400 (180 - 3000000 Seconds)
- Proposal:**
 - Encryption:** AES128-GCM (selected from a dropdown menu that also includes DES, 3DES, AES128, AES192, AES256, AES192GCM, and AES256GCM).
 - Authentication/PRF:** PRF-SHA1 (selected from a dropdown menu that also includes PRF-MD5, PRF-SHA256, PRF-SHA384, and PRF-SHA512).
 - Diffie-Hellman Groups:** DH2 and DH14 (both selected).

Phase 2 Settings - AES-GCM handles both encryption and authentication internally, so there is no additional integrity algorithm.



The Phase 2 Settings interface shows the following configuration:

- Initiation:** Auto (selected), Nailed-up, Responder Only
- Policy:**
 - Name:** test_sp1
 - Local:** 192.168.168.0/24
 - Remote:** 192.168.1.0/24
 - Protocol:** Any
 - Refe:** 0
- SA Life Time:** 28800 (180 - 3000000 Seconds)
- Proposal:**
 - Encryption:** AES128GCM (selected from a dropdown menu that also includes DES, 3DES, AES128, AES192, AES256, AES192GCM, and AES256GCM).
 - Authentication:** Built-in (selected from a dropdown menu).
 - Perfect Forward Secrecy (PFS):** DH2 and DH14 (both selected).

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 is titled 'VPN > Site to Site VPN' and shows a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. Below the progress bar, the configuration fields are:

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

 At the bottom, there 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

1 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

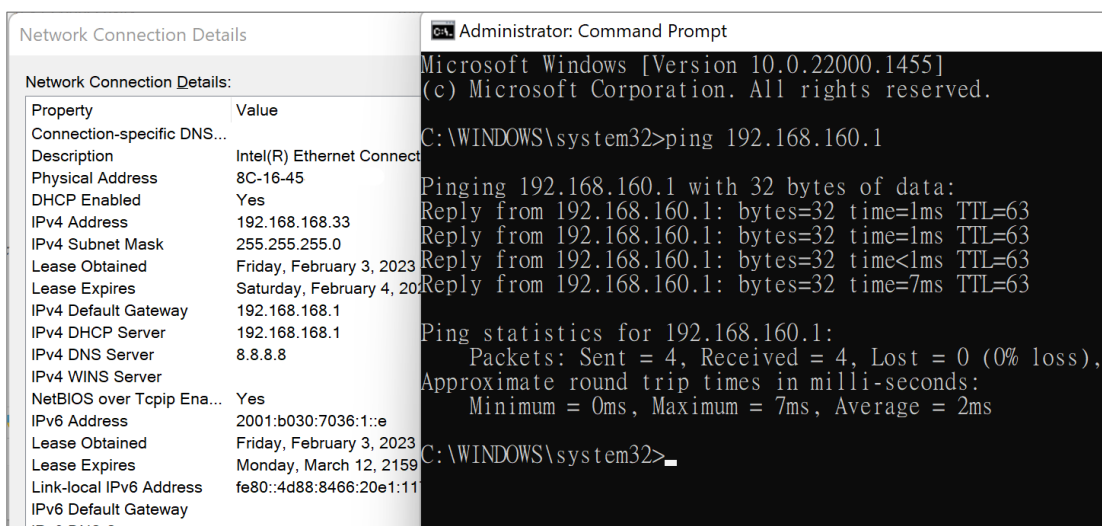
192.168.168.0/24

Close

Test IPsec VPN Tunnel

Ping the PC in Branch Office

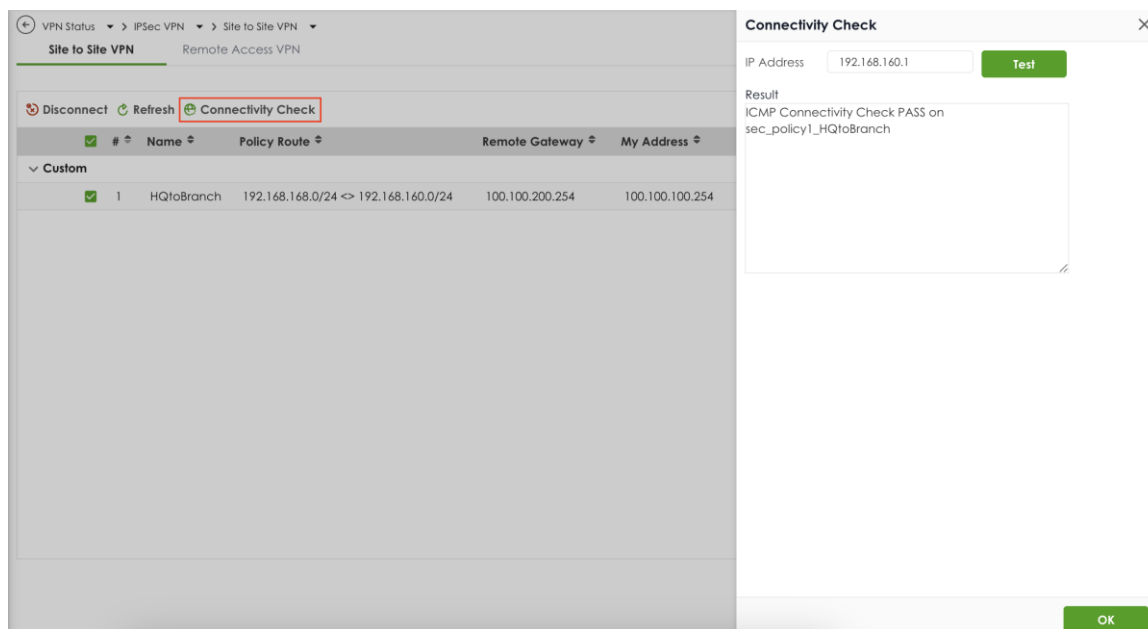
Win 11 > cmd > ping 192.168.160.1



The screenshot displays two windows side-by-side. On the left is the 'Network Connection Details' window for the 'Intel(R) Ethernet Connection 10-16-45'. It lists various network properties such as Physical Address (8C-16-45), IPv4 Address (192.168.168.33), and IPv4 Subnet Mask (255.255.255.0). On the right is an 'Administrator: Command Prompt' window. It shows the execution of the command 'ping 192.168.160.1', which successfully pings the remote IP address with 32 bytes of data, showing a 0% loss and an average round trip time of 2ms.

VPN Status > IPsec VPN

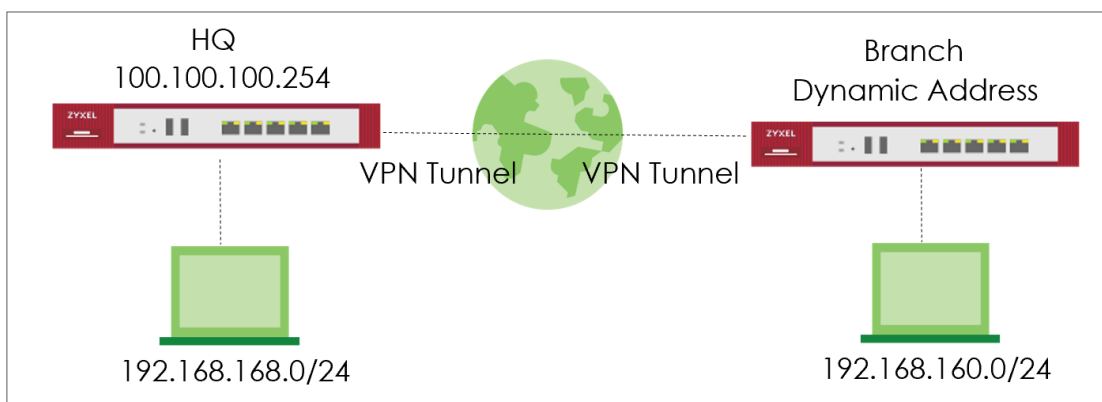
Verify the IPsec VPN status and do the Connectivity Check



The screenshot shows the 'VPN Status' interface in the Zyxel management console. The 'IPsec VPN' section is active, showing a 'Site to Site VPN' configuration. A 'Connectivity Check' button is highlighted. To the right, a 'Connectivity Check' dialog box is open, displaying the IP address '192.168.160.1' and a 'Test' button. The result of the check is shown as 'ICMP Connectivity Check PASS on sec_policy1_HQtoBranch'. The main interface also shows a table of VPN connections, including a 'Custom' connection named 'HQtoBranch' with a status of 'Connected'.

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:

Local	Remote	Protocol	Active Protocol	Encapsulation		
192.168.160.0/24	192.168.168.0/24	Any	ESP	Tunnel	☒	☐

Rows per page: 50 1 of 1 < 1 >

SA Life Time: 28800 (180 - 3000000 Seconds)

Proposal:

Encryption	Authentication
☐ aes128-cbc	hmac-sha1

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups: DH2

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

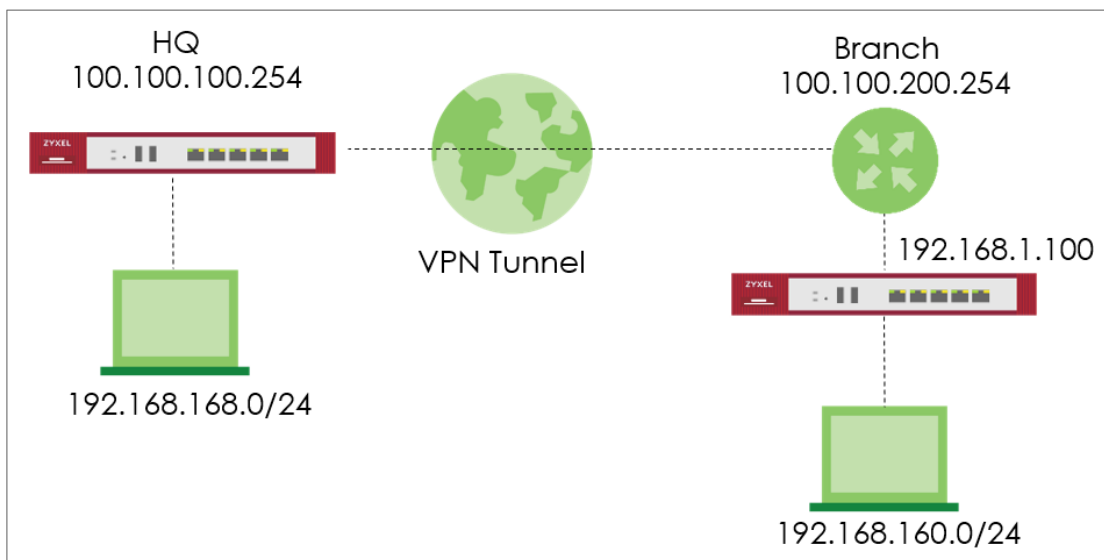
IP Address: 192.168.160.1 Test

Result
ICMP Connectivity Check PASS on sec_policy1_HQtoBranch

OK

How to Configure 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.

The screenshot shows the ZyXel VPN configuration interface for Site to Site VPN. The breadcrumb trail is: VPN > Site to Site VPN. The configuration steps are: Scenario (checked), Network (checked), Authentication (checked), **4 Policy & Routing** (active), and 5 Summary.

Type: ☐ Route-Based ☒ Policy-Based

Local Subnet: 192.168.168.0/24

Remote Subnet: 192.168.160.0/24

The diagram below illustrates the network topology:

```

graph LR
    L[Local Site: 100.100.100.254] --- I((Internet))
    I --- R[Remote Site: Dynamic Address]
    L --- L_N[192.168.168.0/24]
    R --- R_N[192.168.160.0/24]
    style I fill:#008000,color:#fff
  
```

At the bottom, there are buttons for **Cancel**, **Back**, and **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: ☒ 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.

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

192.168.1.100

Router

Internet

Remote Site

100.100.100.254

192.168.168.0/24

Cancel

Back

Finish

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

▼

Network

Local Site

192.168.1.100

Remote Site

100.100.100.254

Authentication

pre-shared-key

🔍

Policy & Routing

Local Subnet

192.168.160.0/24

Edit

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
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
Custom	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

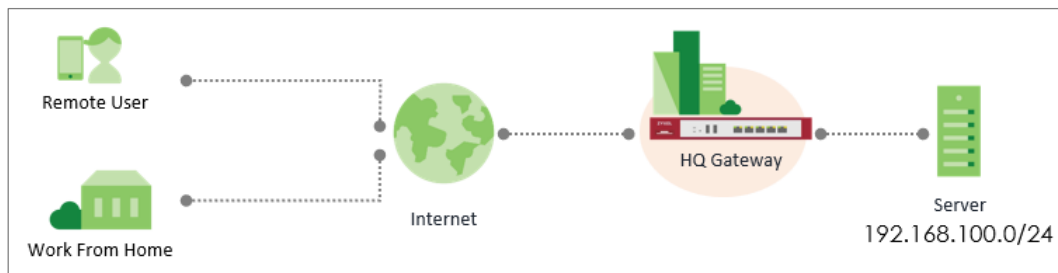
Result

ICMP Connectivity Check PASS on sec_policy1_HQtoBranch

OK

How to Configure Remote Access VPN with Zyxel VPN Client

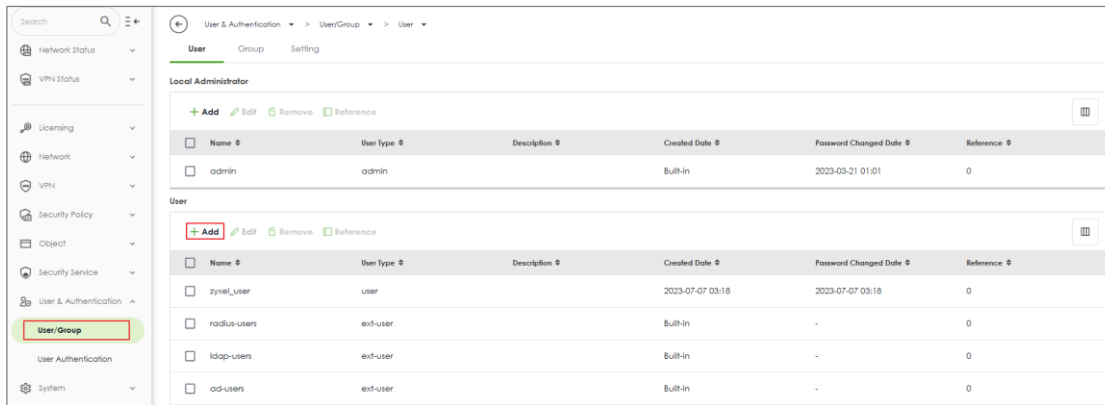
This example shows how to setup Remote Access VPN on USG FLEX H and Zyxel VPN Client. The example instructs how to implement Remote Access VPN by SSL VPN and IPSec VPN.



Before Begin

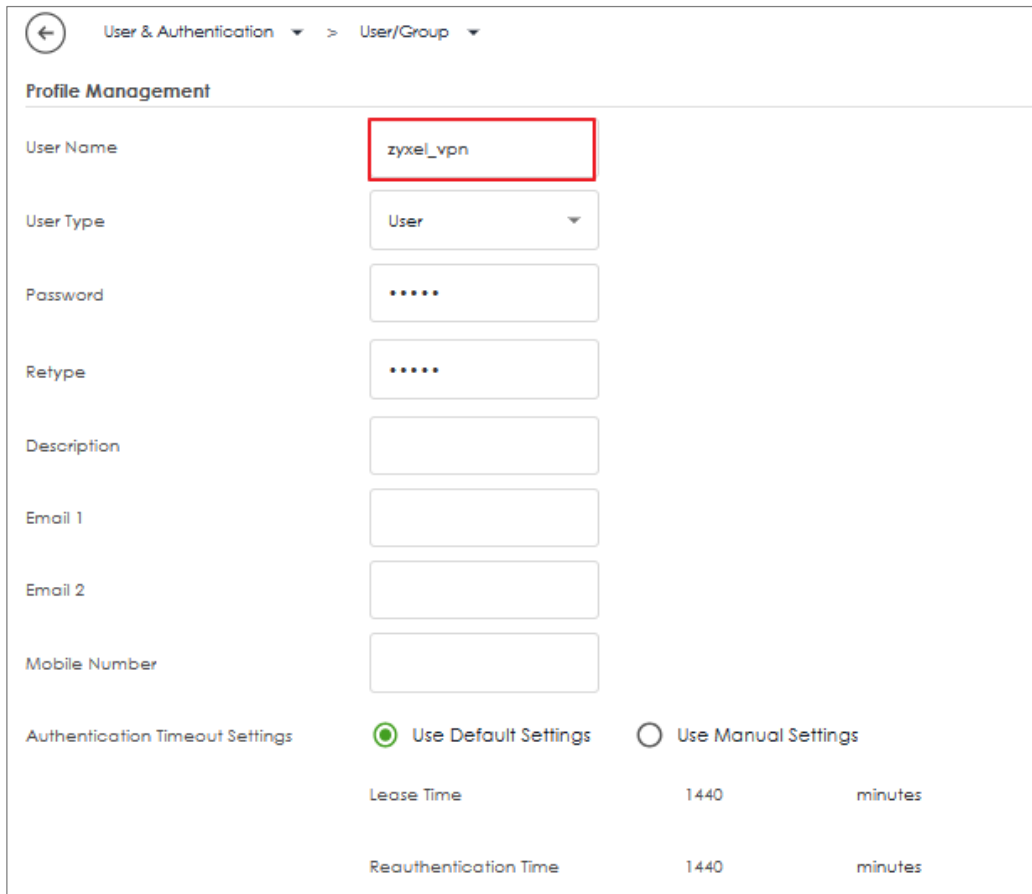
User & Authentication > User/Group > User

Create local user for remote access authentication.



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:

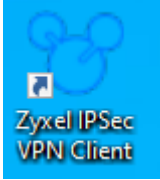
Mobile Number:

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

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Download and install the new TGB Client

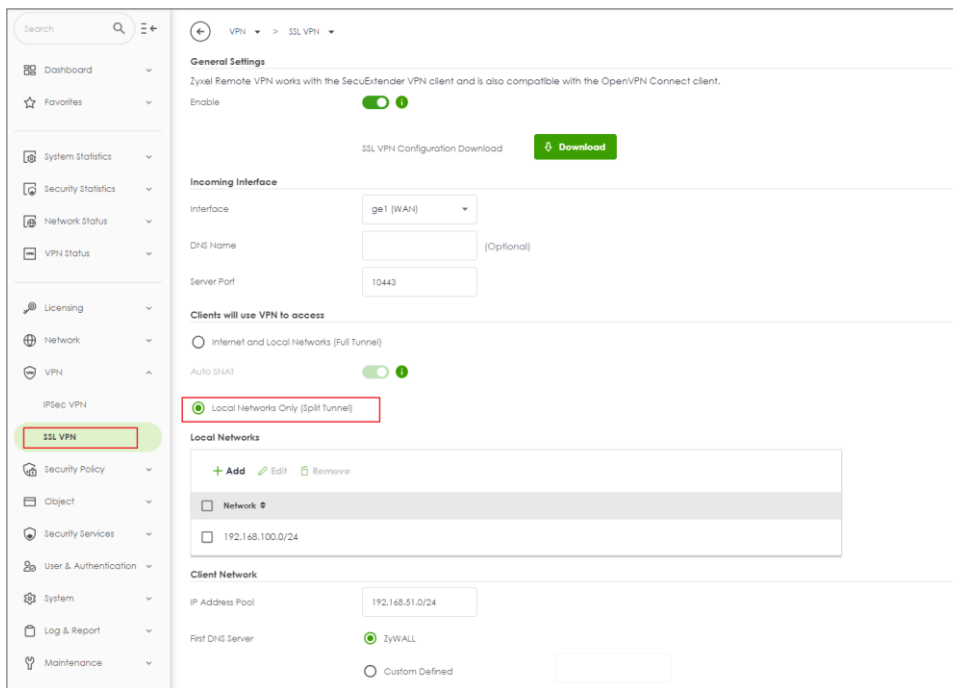


Set up SSL VPN

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)' and a 'Server Port' field set to '10443'. 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. Below this is a 'Local Networks' section with a table listing 'Network 0' and '192.168.100.0/24'. The 'Client Network' section has an 'IP Address Pool' field set to '192.168.51.0/24' and a 'First DNS Server' dropdown 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	☒ ZyWALL ☐ 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

Search
Dashboard
Favourites
System Statistics
Security Statistics
Network Status
VPN Status
Licensing
Network
VPN
IPSec VPN
SSL VPN
Security Policy
Object
Security Services
User & Authentication

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
Get SecuExtender VPN Client Software
Windows macOS
VPN configuration script download
Windows IOS/macOS Android (strongSwan)

Incoming Interface

Interface get
Domain Name / IP

Certificate for VPN Validation

Auto
Manual default

Clients will use VPN to access

Internet and Local Networks (Full Tunnel)
Auto NAT
Local Networks Only (Split Tunnel)
Local Network 192.168.100.0/24

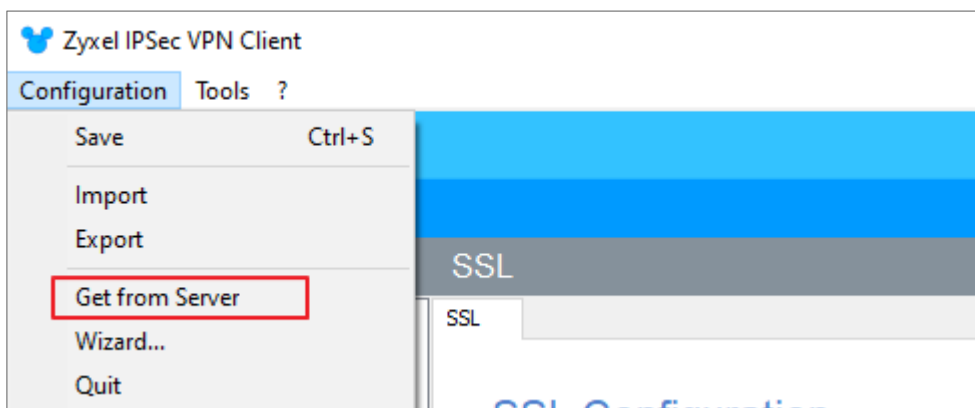
The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.

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 area 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.

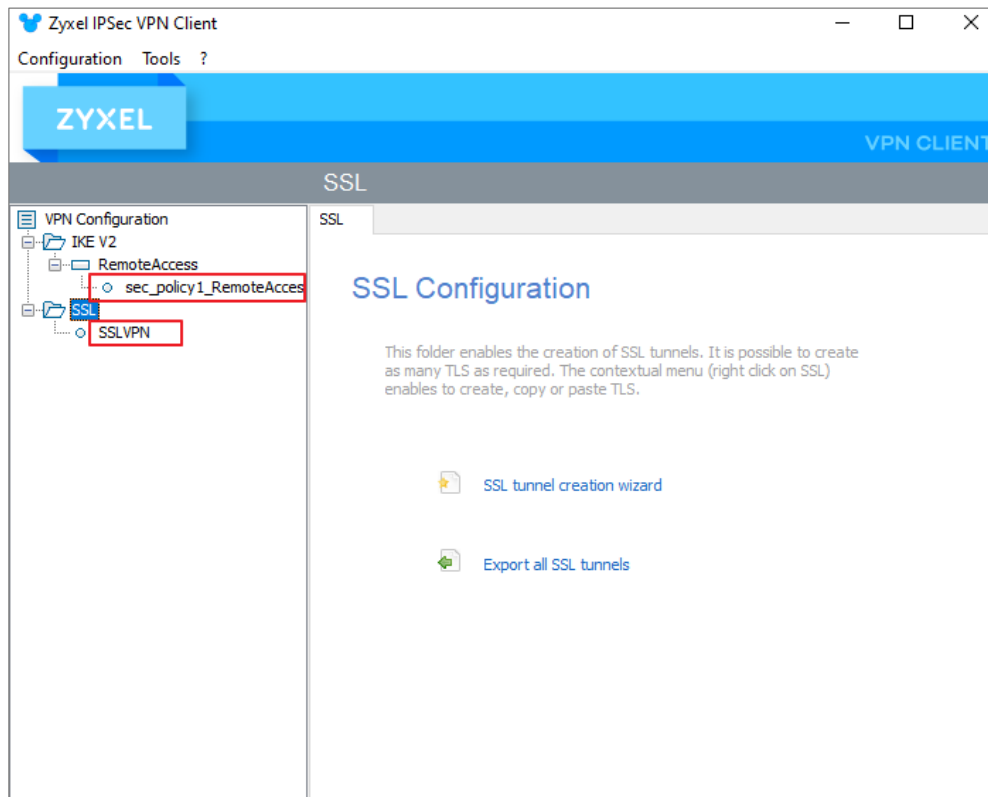
Gateway Address: Port:

Authentication:

Login:

Password:

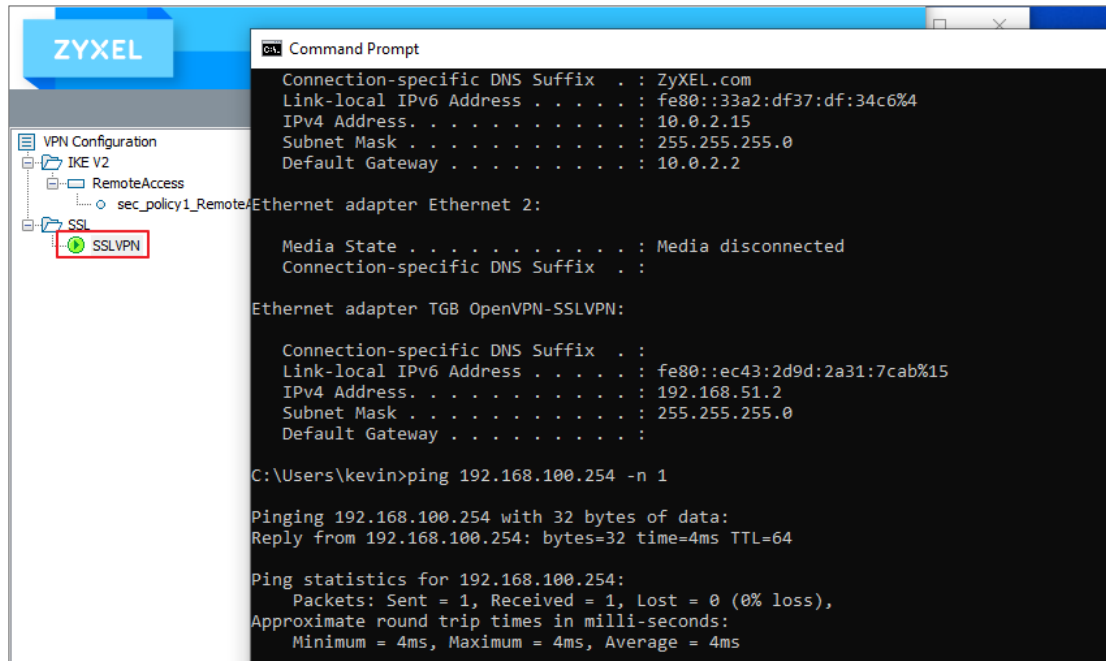
You will obtain IKEv2 as well as SSLVPN settings.



Test SSLVPN Tunnel on TGB Client

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

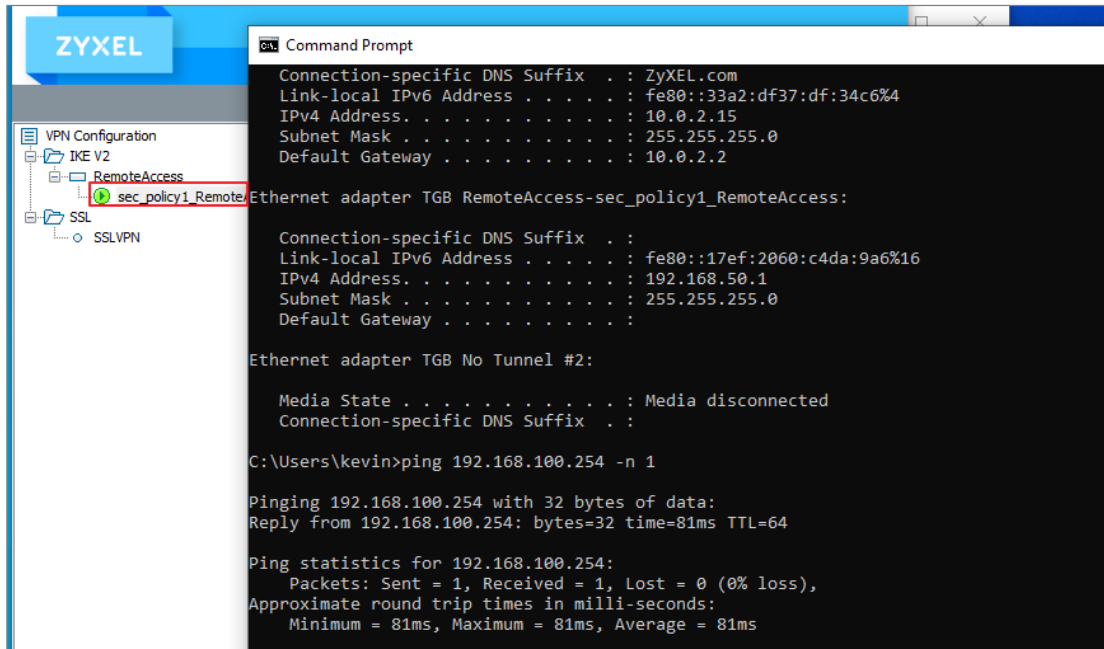
You will see the profile being green and can access internal resource now.



Test IKEv2 Tunnel on TGB Client

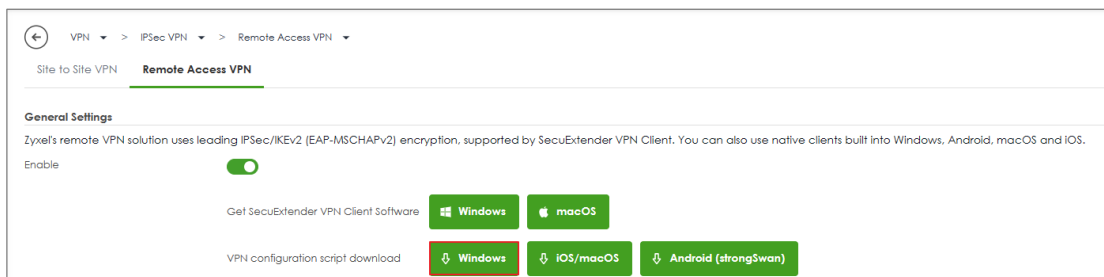
Right click the profile and "Open Tunnel" and log in.

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

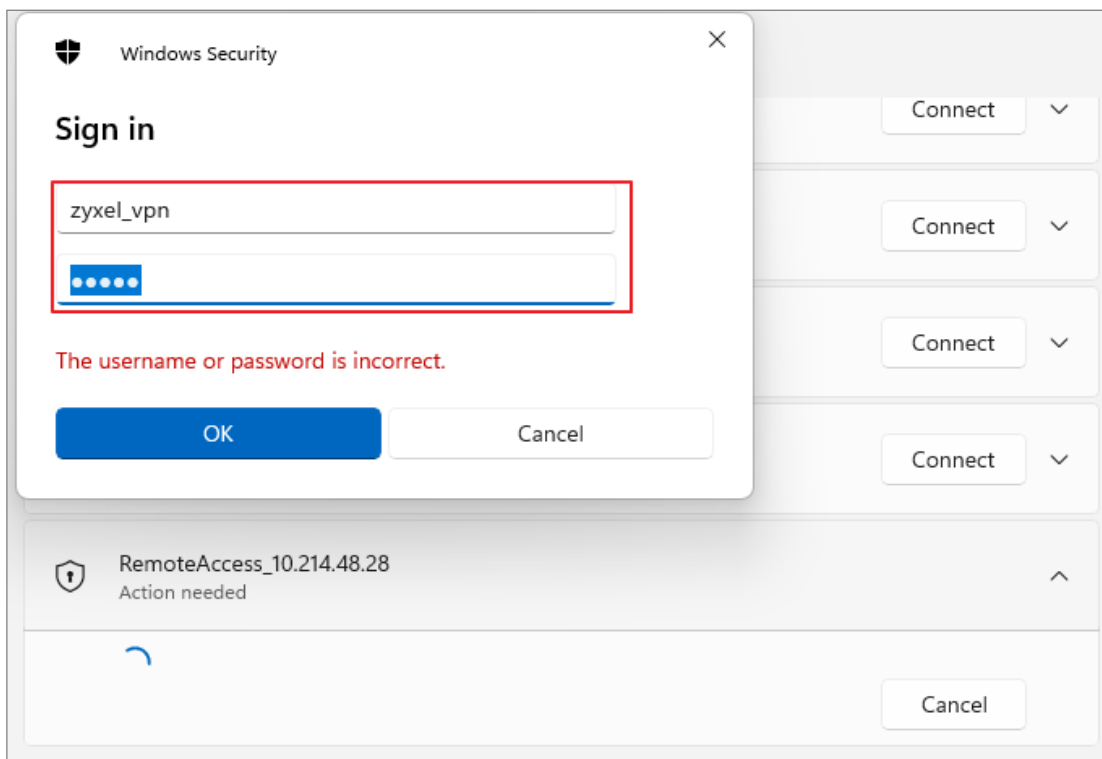


Test IKEv2 Tunnel on Windows Client

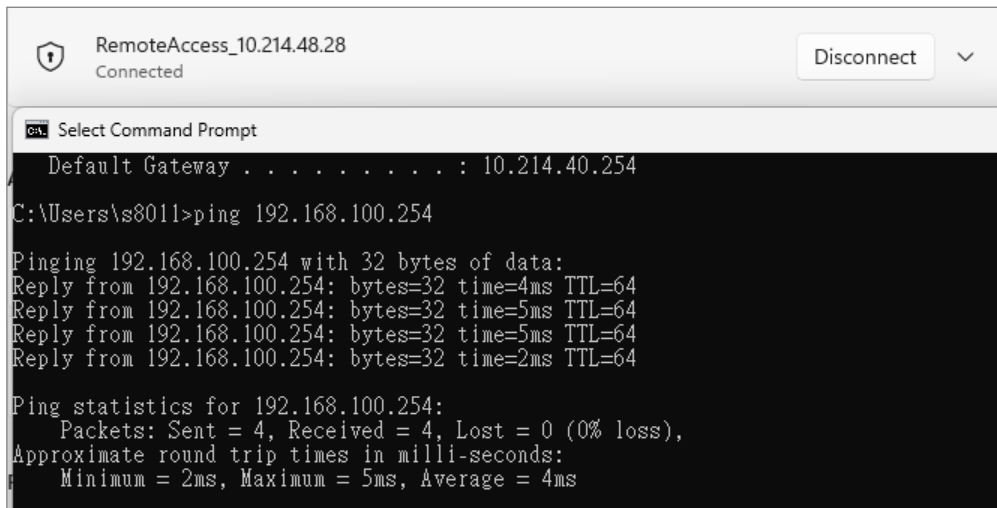
Download Windows VPN configuration script



Perform the windows bat file and input credentials.

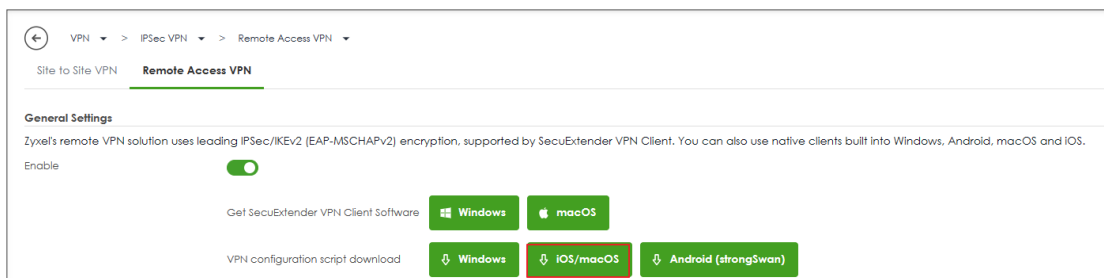


VPN is connected and can access internal resource.

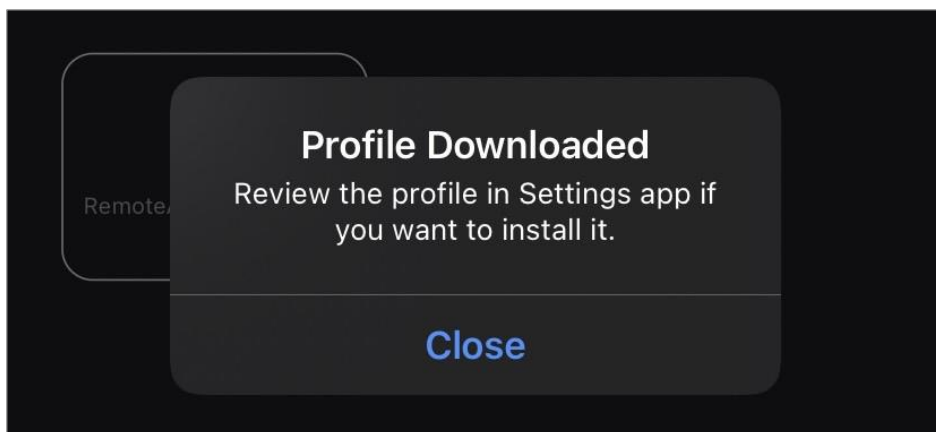


Test IKEv2 Tunnel on iOS Client

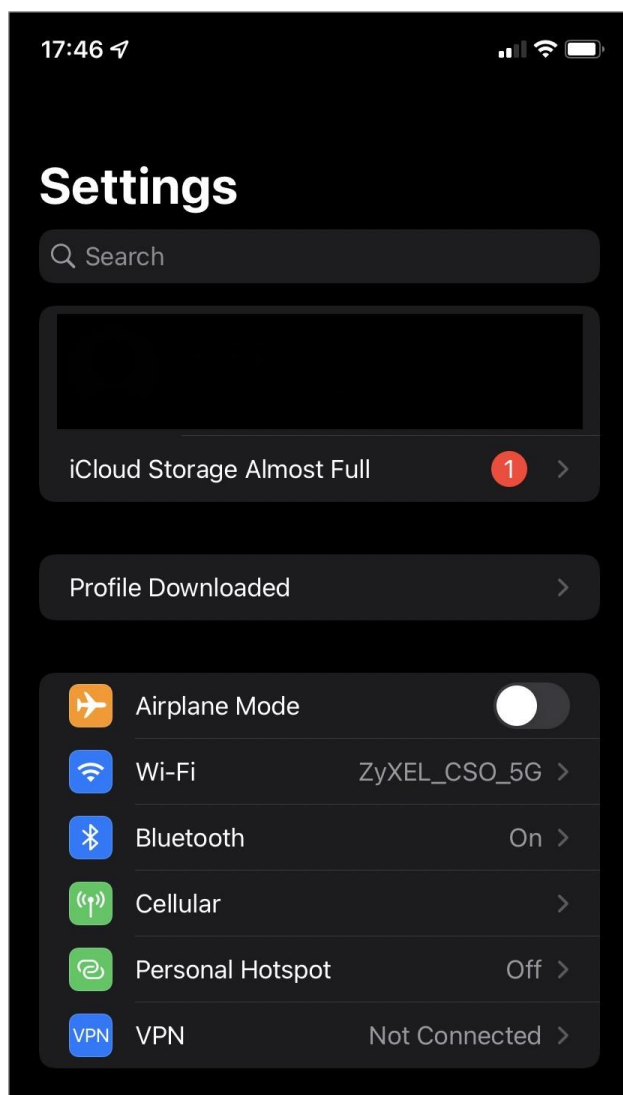
Download iOS/macOS VPN configuration script.



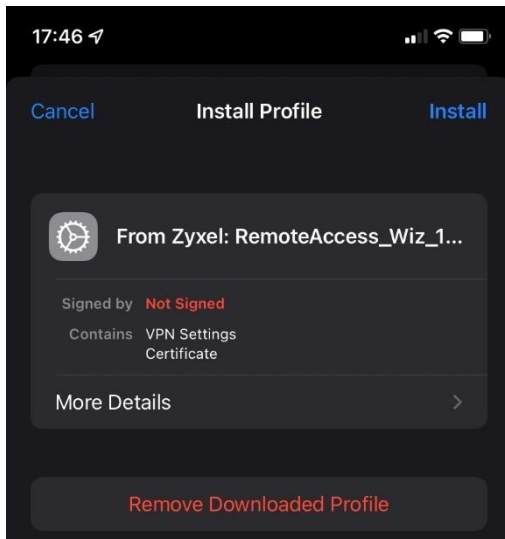
Send the script to Device.



Settings > Profile Downloaded



Press Install.



Enter Username and Password.

Cancel

Enter Username

Next

ENTER YOUR USERNAME FOR THE VPN PROFILE
"VPN"

zyxel_vpn

×

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

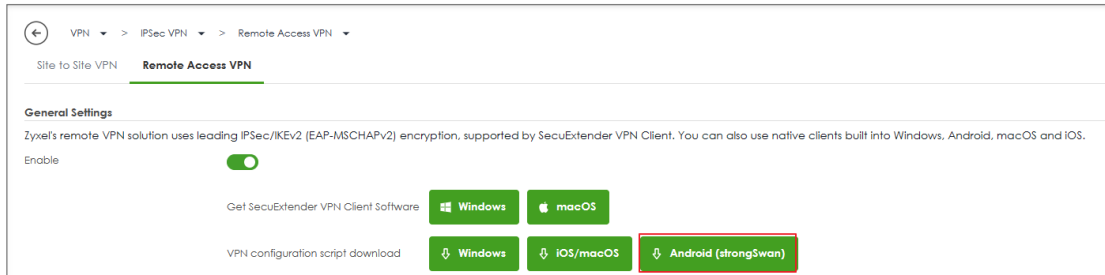
Now, it can connect.

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

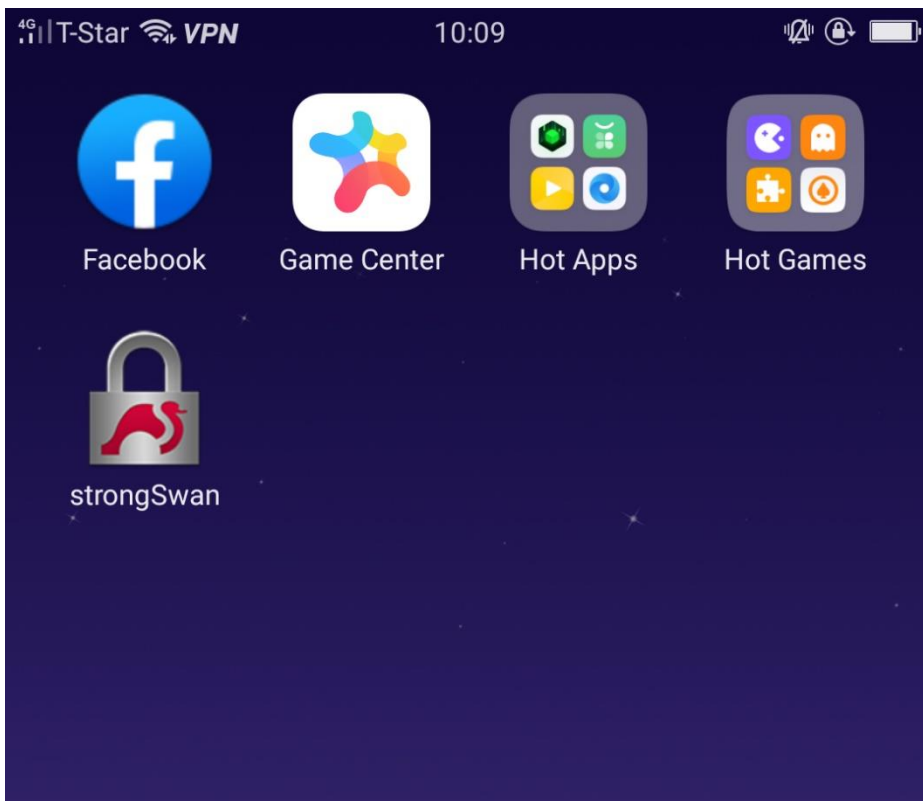
Type	IKEv2
Server	10.214.48.28
Account	zyxel_vpn
Address	192.168.50.1
Connect Time	0:09

Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



Download strongSwan from Google Play Store.

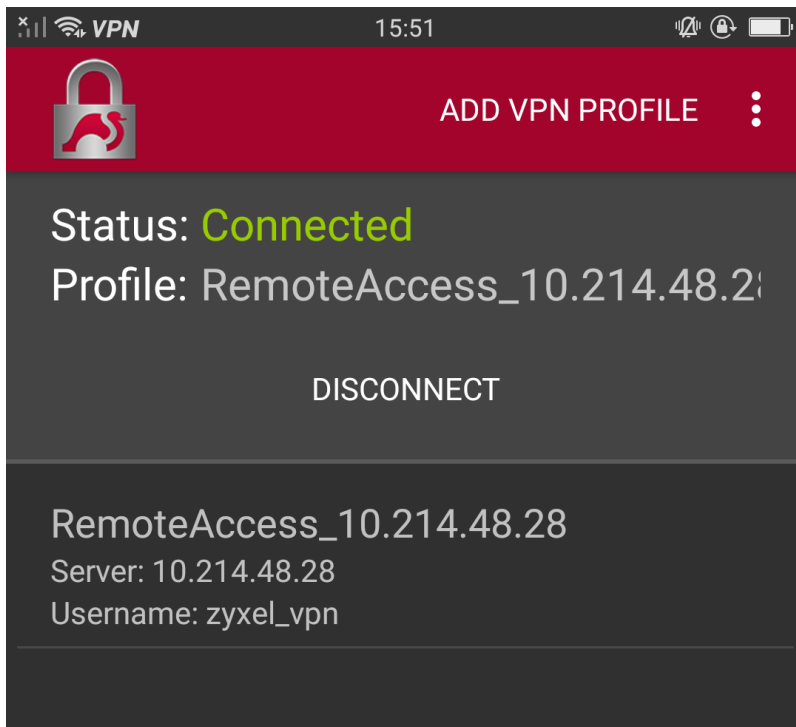


Send the script to device then Install and Import strongSwan profile.

The screenshot shows an Android interface for importing a VPN profile. The status bar at the top indicates the time is 15:51. The dialog has a red header bar with a close button (X), the title 'Import VPN profile', and an 'IMPORT' button. The form fields are as follows:

- Profile name: RemoteAccess_10.214.48.28
- Server: 10.214.48.28
- VPN Type: IKEv2 EAP (Username/Password)
- Username: zyxel_vpn (highlighted with a red box)
- Password (optional): (masked)
- CA certificate: 10.214.48.28

VPN is connected.



Test OpenVPN

VPN > SSL VPN

We now support OpenVPN config file, Click Download to obtain the ovpn file.

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

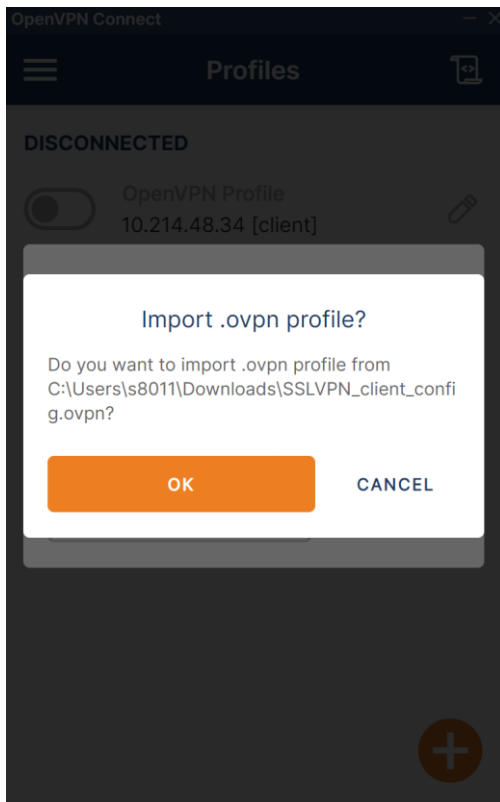
Clients will use VPN to access

Internet and Local Networks (Full Tunnel)

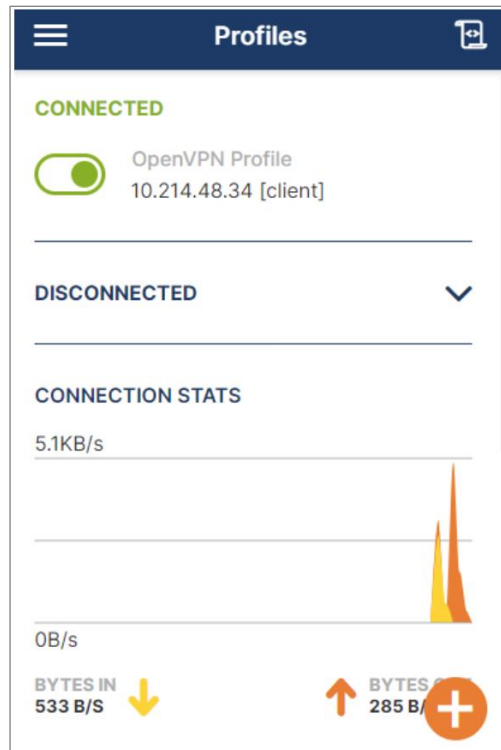
Auto SNAT

Local Networks Only (Split Tunnel)

Import the config file.

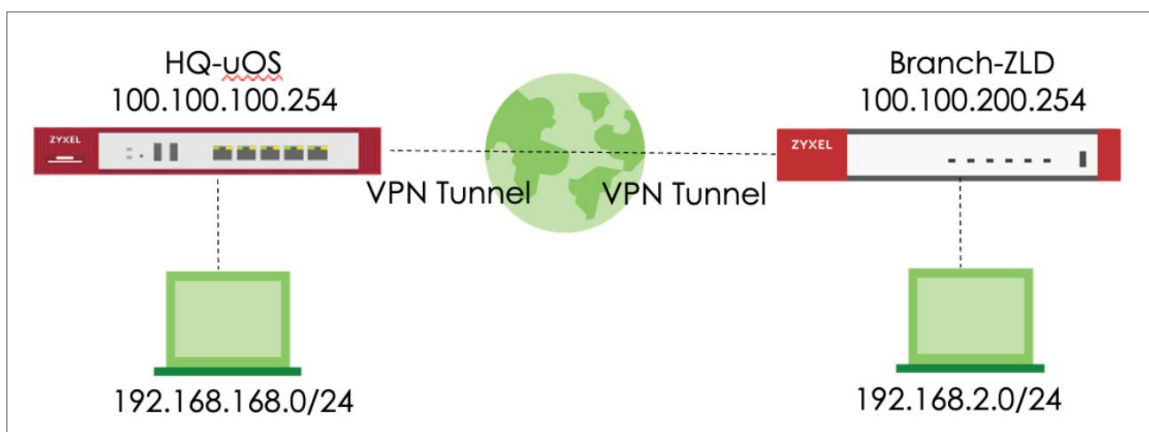


VPN is connected.



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: HQtoFLEX

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

Remote Subnet

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

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

HQtoFLEX

IKE Version

2

Type

Policy-based

Proposal

▼

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

Close

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 x

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)

Advance

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. . . . . : 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 Ethernet 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
  
```

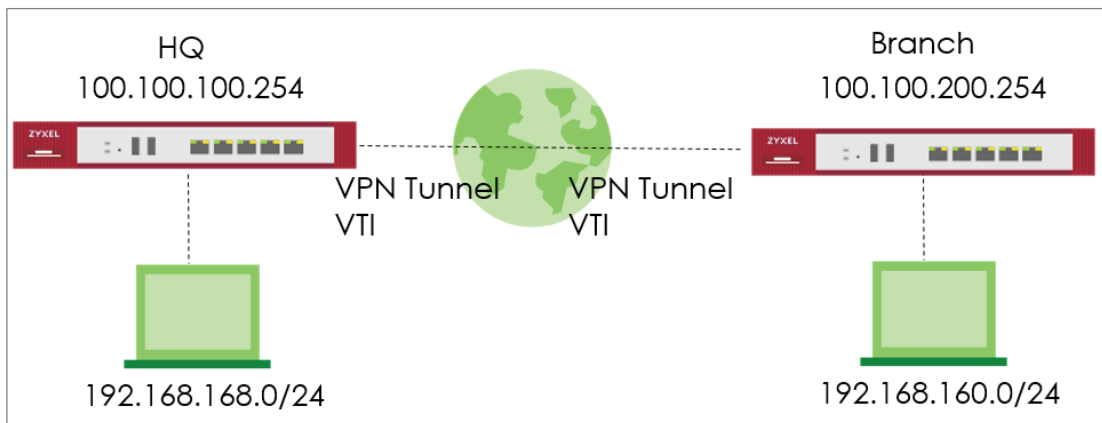
VPN Status > IPsec VPN

Verify the IPsec VPN status and do the Connectivity Check

The screenshot shows the ZyXEL VPN Status interface. The 'IPsec VPN' tab is selected, and the 'Connectivity Check' button is highlighted with a red box. A dialog box titled 'Connectivity Check' is open, showing the IP Address '192.168.160.1' and a 'Test' button. The result of the check is displayed as 'ICMP Connectivity Check PASS on sec_policy1_HQtoFLEX'. The background interface shows a table with VPN status information, including a 'Custom' entry with a status of '1' and a name 'HQtoFLEX'.

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 displays the ZyXel VPN configuration web 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 with a red box), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main content area shows the 'VPN > Site to Site VPN' configuration path. A progress bar at the top indicates five steps: 1. Scenario (active), 2. Network, 3. Authentication, 4. Policy & Routing, and 5. Summary. In the 'Scenario' step, the following settings are visible:

- *Name: HQtoBranch (text box with a red border)
- 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' and a 'Remote Site' connected via an 'Internet' cloud. At the bottom of the configuration area are 'Cancel' and 'Next' buttons. The 'Next' button is green and active.

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	*****
----------------	----------------	-------

Policy & Routing

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

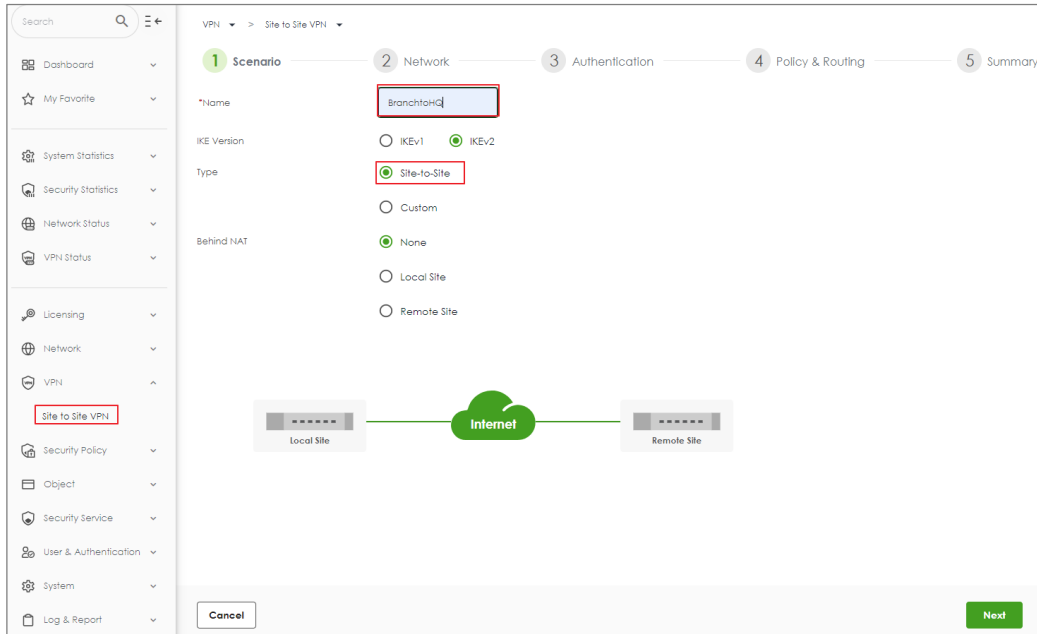
Close

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 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 'Name' field contains 'BranchtoHQ' (highlighted with a red box). The 'IKE Version' is set to 'IKEv2'. The 'Type' is set to 'Site-to-Site' (highlighted with a red box). The 'Behind NAT' option is set to 'None'. Below the configuration fields is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is then connected to a 'Remote Site'. At the bottom, there 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 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	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.

The screenshot shows the 'VPN Status' page with 'IPsec VPN' selected. Under 'Site to Site VPN', the 'HQtoBranch' tunnel is active. The table below provides details for this tunnel.

	Name	Policy Route	Remote Gateway	My Address	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
Custom	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

The screenshot shows two windows side-by-side. The left window displays 'Network Connection Details' for the Intel(R) Ethernet Connection. The right window is an 'Administrator: Command Prompt' showing the execution of a ping command.

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 displays the Zyxel Tailscale management interface. At the top, the header shows 'zyxel.com.tw' with a 'Trial 14 days left' badge, and navigation links for 'Download', 'Support', 'Docs', and a user profile 'K'. Below the header is a main navigation bar with icons and labels for 'Machines', 'Apps', 'Services', 'Users', 'Access controls', 'Logs', 'DNS', 'Settings' (highlighted), and a 'Get started' button. On the left side, a sidebar lists 'Tailnet Settings' with sub-items: 'General', 'User management', 'Device management', 'OAuth clients', 'Webhooks', 'Contact preferences', and 'Billing'. Below these is 'Personal Settings' (highlighted with a red box) which contains a 'Keys' link (also highlighted with a red box). The main content area is titled 'Keys' and includes the text: 'View and manage your Auth keys and API access tokens. Your private device keys are not included here: they are always private, stay on your device, and are never shared with Tailscale. [Learn more](#)'. Below this is the 'Auth keys' section with the text: 'Authenticate devices without an interactive login. [Learn more](#)'. A red box highlights the 'Generate auth key...' button in the top right of this section. The main content area also displays a message: '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.

Zyxel

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.

90 — + days

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](#)

Cancel

Generate key

Copy the key.

Generated new key



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

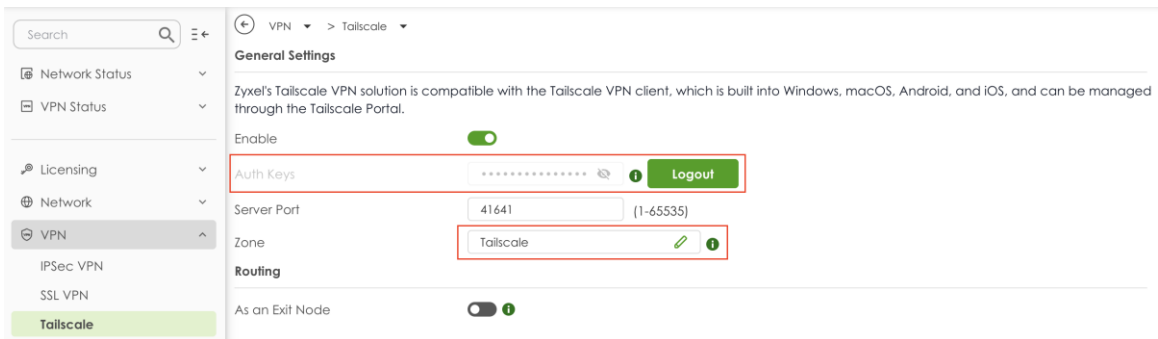
tskey-auth-kc5HbhKcQQ11CNTRL-



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".



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

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

2 machines

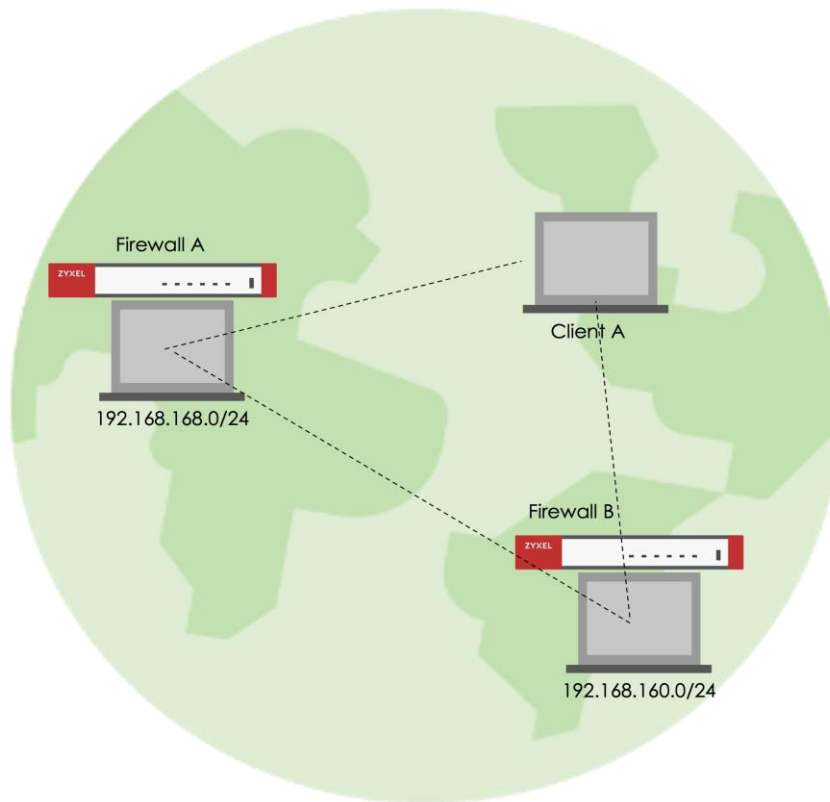
MACHINE	ADDRESSES	VERSION	LAST SEEN
twbnbt123234-01 Kevin.Wu4@zyxel.com.tw	100.95.1	1.80.2 Windows 11 22H2	Connected
usgflex500h Kevin.Wu4@zyxel.com.tw	100.115.1	1.75.16 Linux 4.14.207-10.3.7.0-2	Connected

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... Edit machine name... Edit machine IPv4... Share... Disable key expiry
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
☐ 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

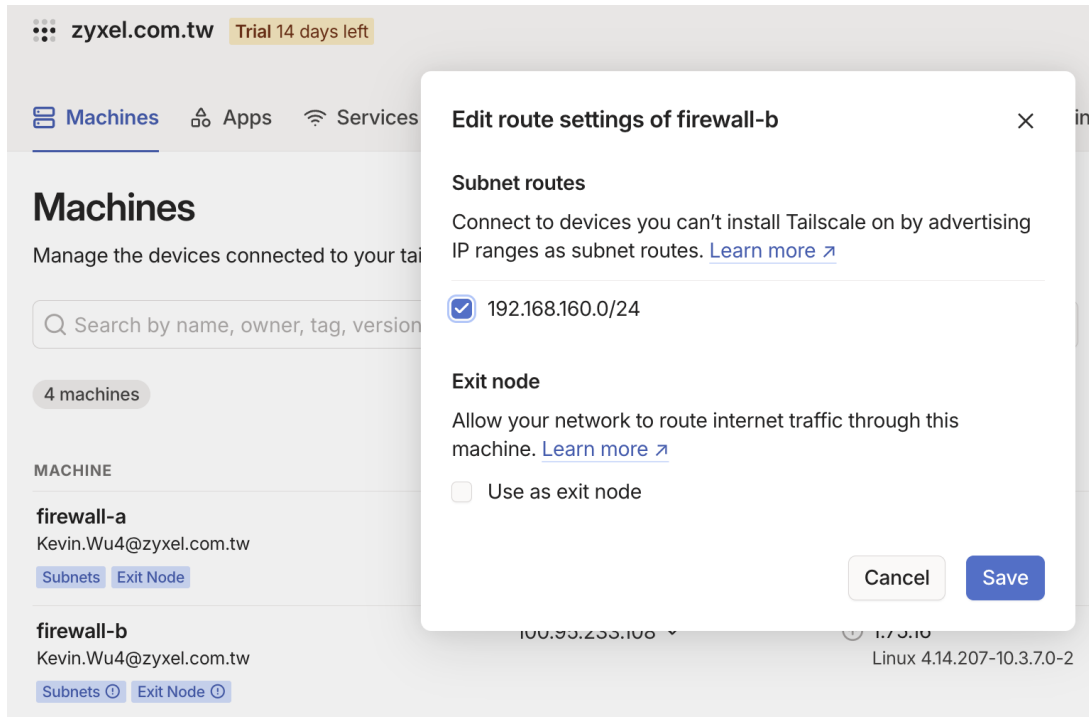
As an Exit Node ☐

Advertised Networks

+ Add Remove

Network
☐ 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

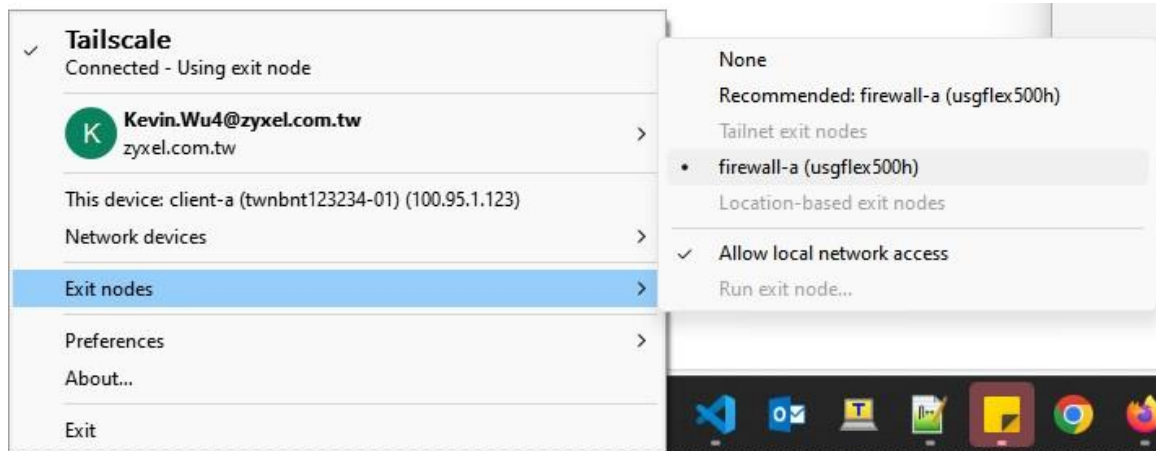
Allow your network to route internet traffic through this machine. [Learn more ↗](#)

☒ 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
```

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

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.

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.

Copyright © 2026 Zyxel and/or its affiliates. All rights reserved. 91

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 ☒ ?

SSL VPN Configuration Download [Download](#)

Incoming Interface

Interface

DNS Name (Optional)

Server Port

Zone ?

Clients will use VPN to access

☒ Internet and Local Networks (Full Tunnel)

Auto SNAT ☒ ?

☐ Local Networks Only (Split Tunnel)

Client Network

IP Address Pool

First DNS Server ☒ ZyWALL

☐ Custom Defined

Second DNS Server

Authentication ?

Primary Server

Secondary Server

User ?

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

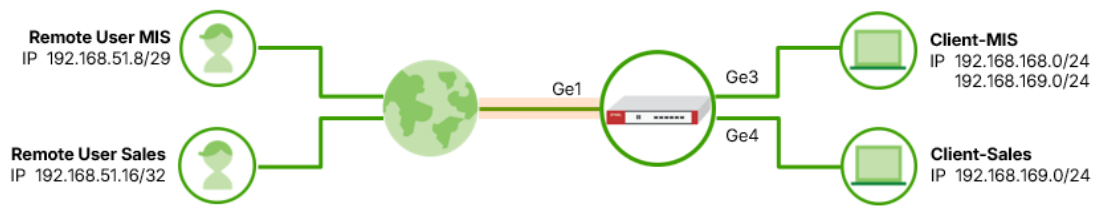
Disconnect Refresh

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

How to Configure SSL VPN Access Profile

With multiple SSL VPN client profiles, you can create one or more profiles to apply its own settings such as IP pool, DNS and tunnel type to specific users. This example illustrates how to create multiple SSL VPN client profiles for different groups.



 Note: This feature is supported from firmware version uOS 1.38.

Add Client Profiles

1. Go to VPN > SSL VPN > Advanced Settings > Client Profile and click +Add to add a client profile for MIS. In this example, users in group_MIS can access the network 192.168.168.0/24 and 168.168.169.0/24 after establishing SSL VPN.

Add/Edit Client Profile

Clients will use VPN to access

☐ Internet and Local Networks (Full Tunnel)

☒ Local Networks Only (Split Tunnel)

Auto SNAT ☐ *i*

Local Networks

i If no local network is specified, the profile inherits Local Network settings from Global SSL VPN.

+ Add ☐ Remove

☐ Network ↕
☐ 192.168.169.0/24
☐ 192.168.168.0/24

Client Network

IP Address Pool *i*

DNS Server

DNS Domain Suffix

Members

User *i*

2. Add another Client Profile for Sales. In this example, users in group_Sales can access the network 168.168.169.0/24 only after establishing SSL VPN.

Add/Edit Client Profile

Clients will use VPN to access

☐ Internet and Local Networks (Full Tunnel)

☒ Local Networks Only (Split Tunnel)

Auto SNAT ☐

Local Networks

If no local network is specified, the profile inherits Local Network settings from Global SSL VPN.

+ Add - Remove

☐ Network
☐ 192.168.169.0/24

Client Network

IP Address Pool: 192.168.51.16/32

DNS Server: ZyWALL

DNS Domain Suffix:

Members

User: group_Sales

3. Check the client profiles.

- The IP Address Pool of a client profile must be within the global SSL VPN IP Address Pool range. In this example, the global IP address Pool is 192.168.51.0/24, and the IP address Pool of client profiles are 192.168.51.16/29 and 192.168.51.8/29.
- The IP Address Pool of a client profile should be an IPv4 CIDR notation. For example,
192.168.51.8/29 for IP range 192.168.51.8 ~ 192.168.51.15
192.168.51.16/32 for single IP 192.168.51.16

VPN
SSL VPN

Client Network

IP Address Pool: 192.168.51.0/24
DNS Server: ZyWALL
DNS Domain Suffix:

Advanced Settings

Client Profile

+ Add Edit Remove Move to

Search insights

#	IP Address Pool	DNS Server	Tunnel Type	User
1	192.168.51.16/32	ZyWALL	Split Tunnel 192.168.169.0/24	group_Sales
2	192.168.51.8/29	ZyWALL	Split Tunnel 192.168.168.0/24, 192.168.169.0/24	group_MIS

Verification

1. Go to VPN > SSL VPN. Download SSL VPN configuration file and import the file to OpenVPN client.
2. Enter the username "MIS1" and the password to connect SSL VPN. The user "MIS1" receives the IP address 192.168.51.10 and can access both 192.168.168.0/24 and 192.168.169.0/24.

The screenshot displays the OpenVPN Connect application window on the left and a Windows Command Prompt on the right. The OpenVPN Connect window shows the 'Profiles' tab with a graph of network activity. Below the graph, it indicates 'BYTES IN 332 B/S' and 'BYTES OUT 840 B/S'. The connection duration is '00:00:40' and 'PACKET RECEIVED 2 sec ago'. Under the 'YOU' section, the username 'MIS1' is highlighted with a red box. Below it, 'YOUR PRIVATE IP' is listed as '192.168.51.10', also highlighted with a red box. The 'SERVER' section shows the IP '10.214.48.38' and 'SERVER PUBLIC IP 10.214.48.38'. The 'PORT' is '10443' and the 'VPN PROTOCOL' is 'TCP'.

The Command Prompt window shows the execution of two ping commands. The first command is 'ping 192.168.169.1', which returns four successful replies with 32 bytes of data, 1ms response time, and a TTL of 64. The second command is 'ping 192.168.168.1', which also returns four successful replies with 32 bytes of data, 1ms response time, and a TTL of 64. Both commands show a 0% loss of packets.

Verify the SSL VPN status in Log & Report > System.

2	2026-04-28 19:18:55	User	User MIS1 from sslvpn has logged out Device	10.214.48.36	127.0.0.1	0	Account: MIS1
3	2026-04-28 19:17:39	SSL VPN	SSL VPN client IP assigned 192.168.51.10 [profile2]	10.214.48.36	0.0.0.0	0	account MIS1
4	2026-04-28 19:17:39	SSL VPN	SSL VPN Tunnel established	10.214.48.36	0.0.0.0	0	account MIS1
5	2026-04-28 19:17:38	User	User MIS1(MAC=04:...) from sslvpn has logged in Device	10.214.48.36	127.0.0.1	0	Account: MIS1

- Enter the username "sales1" and the password to connect SSL VPN. The user "sales1" receives the IP address 192.168.51.16 and can access 192.168.169.0/24 only.

The screenshot displays the OpenVPN Connect application window on the left and a Windows Command Prompt on the right. The OpenVPN Connect window shows the 'Profiles' tab with a profile named 'sales1' and a private IP of 192.168.51.16. The Command Prompt window shows the following output:

```
C:\Users>
C:\Users>ping 192.168.169.1

Pinging 192.168.169.1 with 32 bytes of data:
Reply from 192.168.169.1: bytes=32 time=1ms TTL=64
Reply from 192.168.169.1: bytes=32 time=2ms TTL=64
Reply from 192.168.169.1: bytes=32 time=2ms TTL=64
Reply from 192.168.169.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.169.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users>ping 192.168.168.1

Pinging 192.168.168.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.168.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

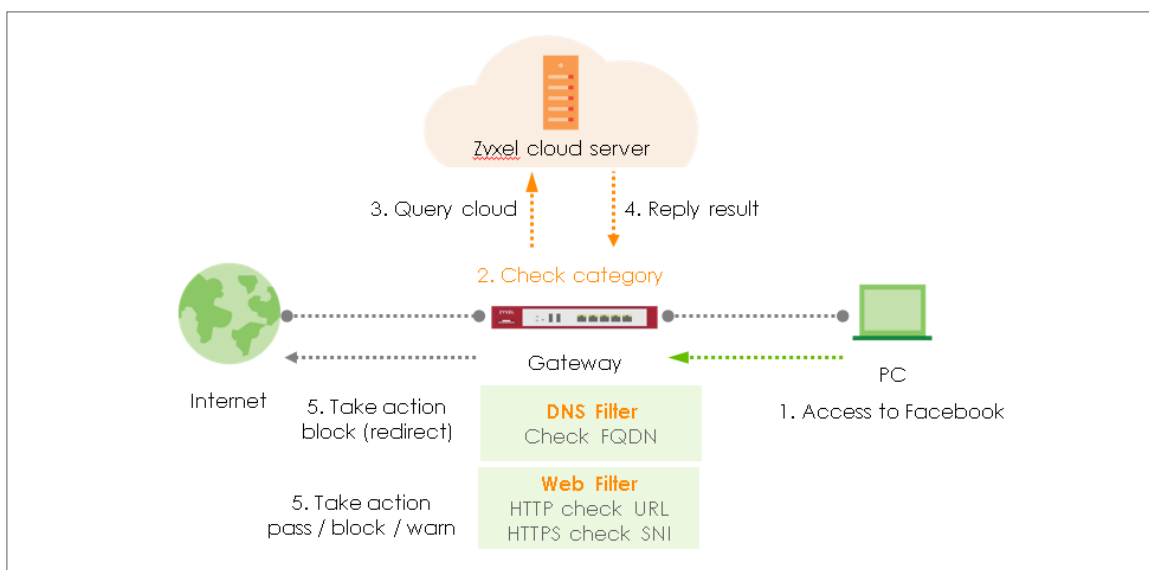
Verify the SSL VPN status in Log & Report > System.

3	2026-04-28 19:11:04	User	User sales1 from sslvpn has logged out Device	10.214.48.36	127.0.0.1	0	Account: sales1
4	2026-04-28 19:08:21	SSL VPN	SSL VPN client IP assigned 192.168.51.16 [profile1]	10.214.48.36	0.0.0.0	0	account sales1
5	2026-04-28 19:08:21	SSL VPN	SSL VPN Tunnel established	10.214.48.36	0.0.0.0	0	account sales1
6	2026-04-28 19:08:20	User	User sales1(MAC=04:0e:3c: from sslvpn has logged in Device	10.214.48.36	127.0.0.1	0	Account: sales1

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  

☐	Name	Description	Reference
☐	BPP		0
☐	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.

☐ Shareware Freeware	☐ Social Networking	☐ Software Hardware
☐ Sports	☐ Stock Trading	☒ Streaming Media
☐ Technical Business Forums	☐ Technical Information	☐ Text Spoken Only
☐ Text Translators	☐ Tobacco	☐ Travel
☐ Usenet News	☐ Violence	☐ Visual Search Engine

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



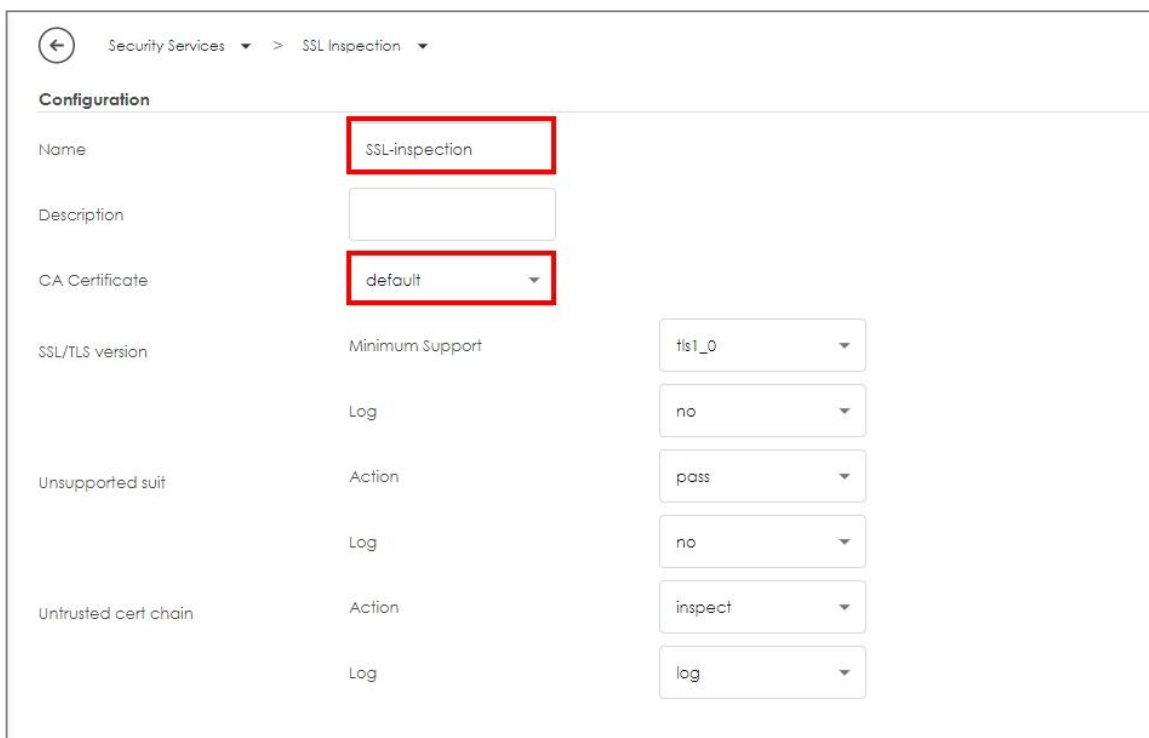
Profile Management

+ 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

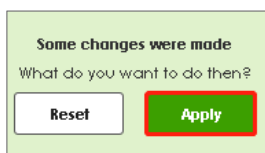
Unsupported suit: Action: pass

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	Valid From	Valid To	Refer...
default	SELF	CN=USG_FLEX_200HP_DB...	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.

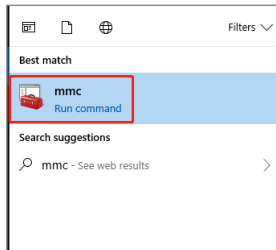
Export Certificate

Password

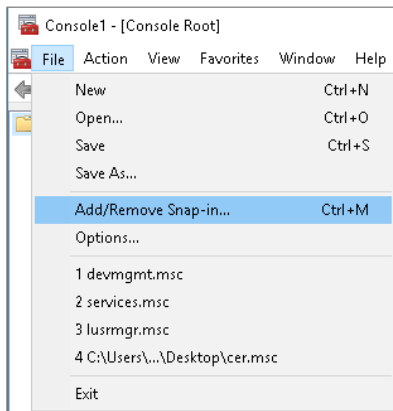
Leave the password field blank to export certificate only or fill in password to export certificate with private key.

Export Certificate

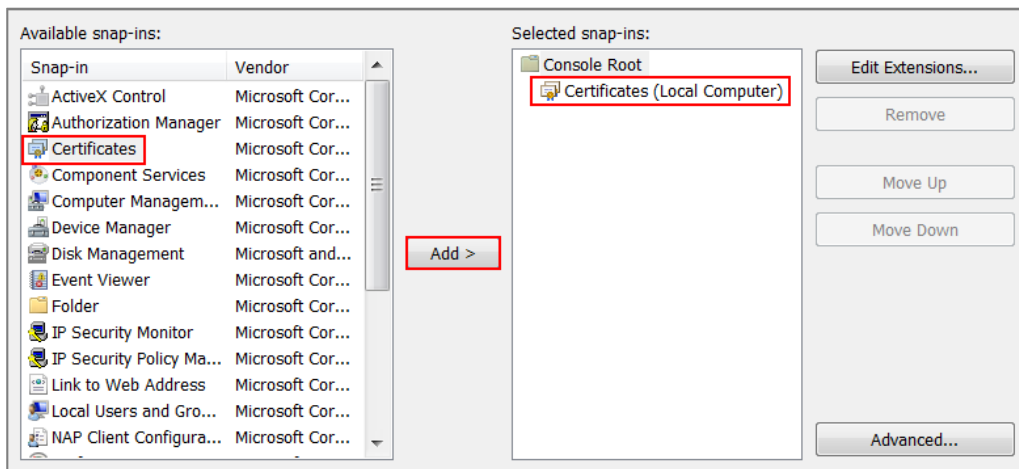
In Windows Start Menu > Search Box, type MMC and press Enter.



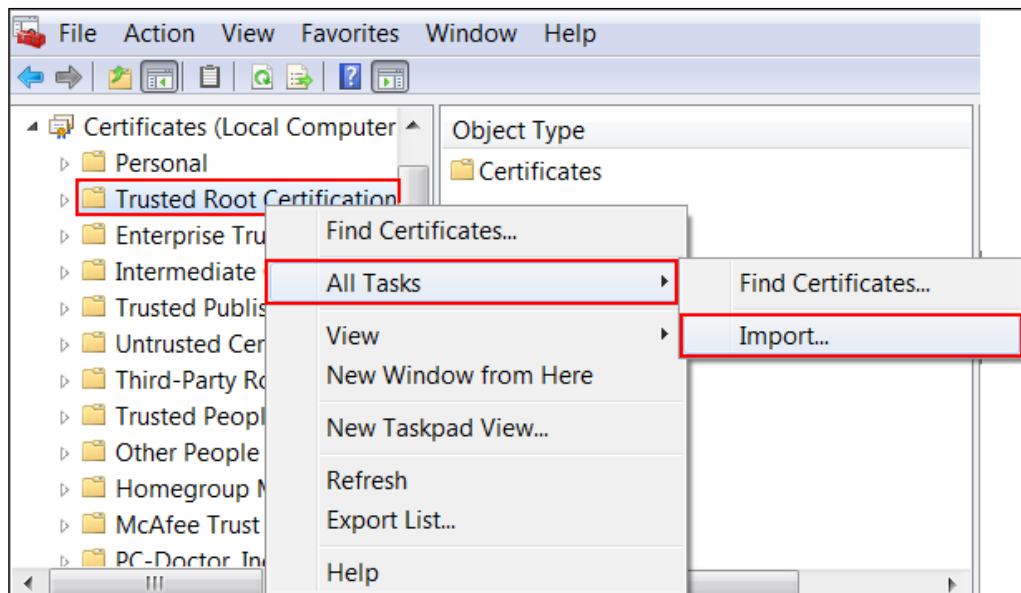
In the mmc console window, click File > Add/Remove Snap-in...



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.

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.



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 has the heading 'Certificate Store' followed by 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 displayed. There are two radio button options: 'Automatically select the certificate store based on the type of certificate' and 'Place all certificates in the following store:'. The second option is selected and highlighted with a red rectangular box. Below the selected option, there is a text field labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities'. To the right of the text field 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

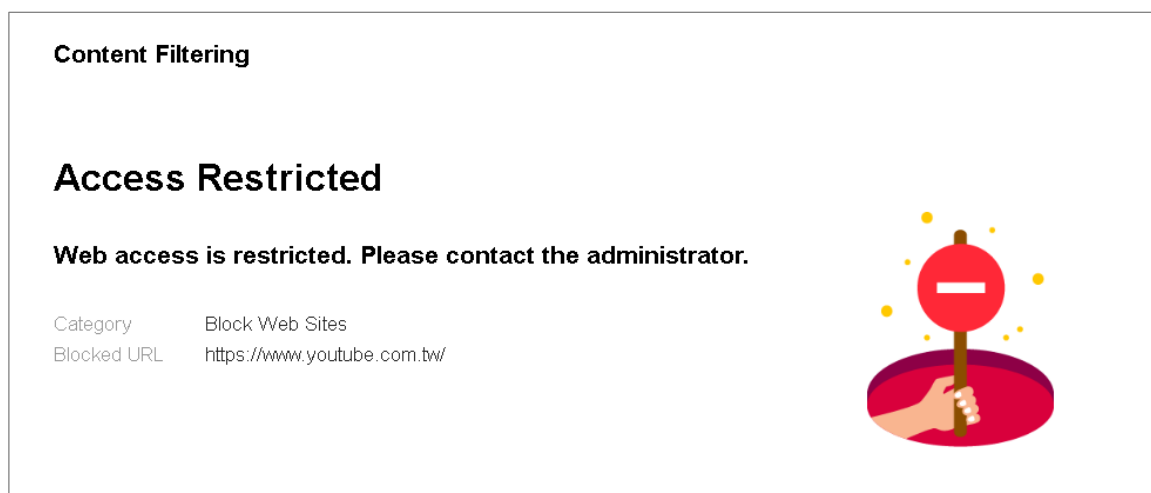
☒ Place all certificates in the following store:

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

1

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
Item Count

Streaming Media 18 (100%)

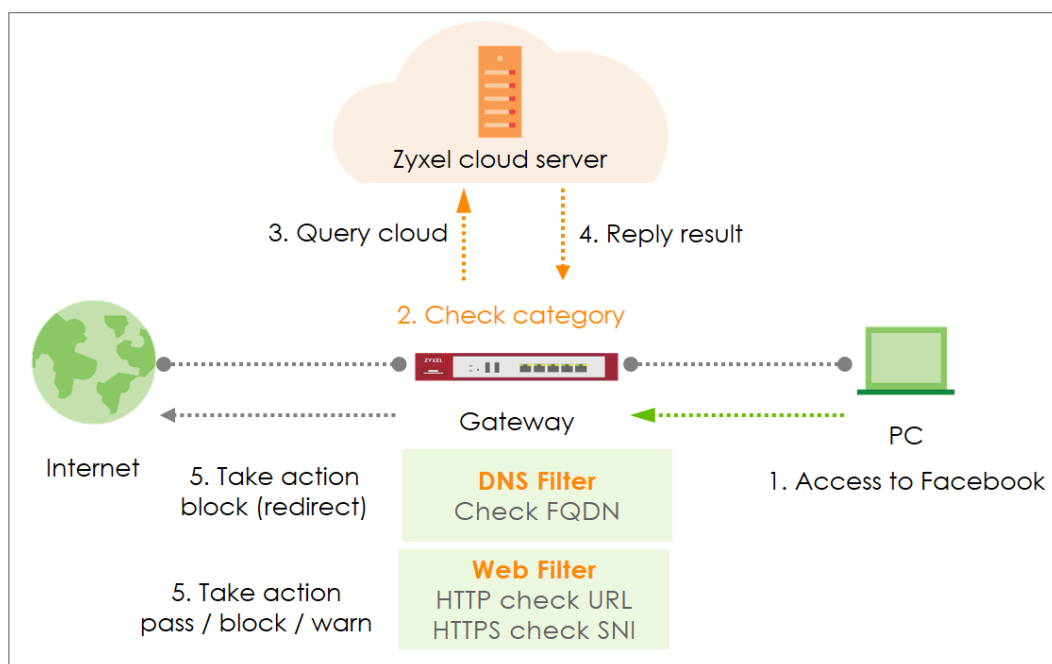
Content Filter Events

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.

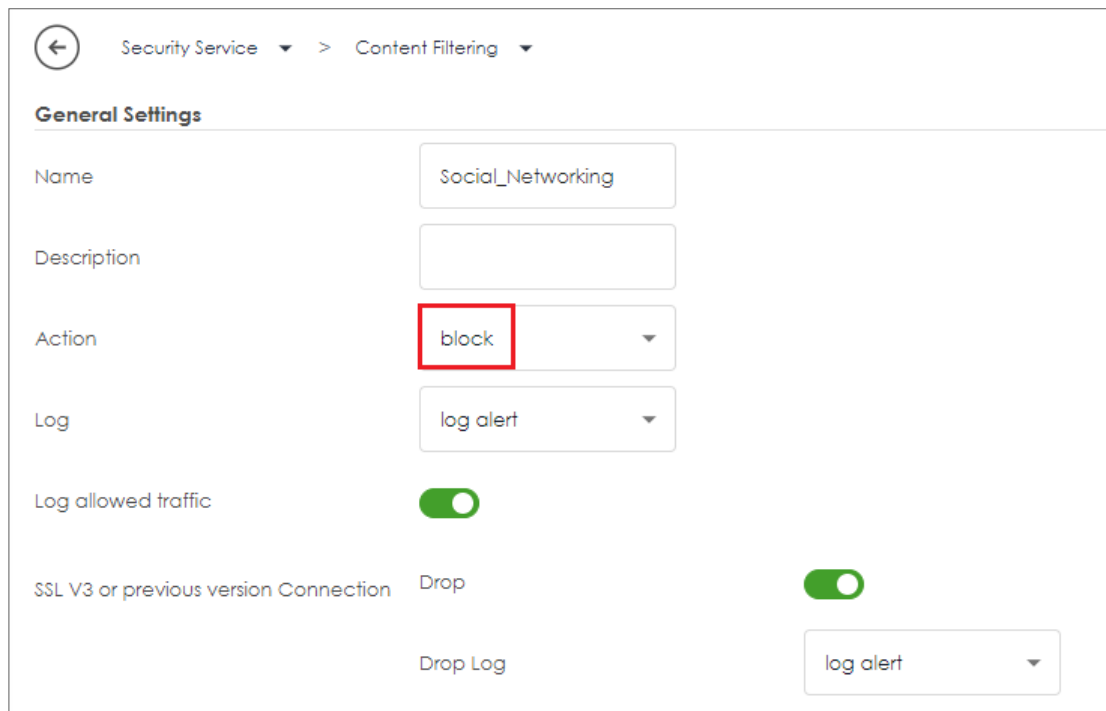
When the user makes an HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then the cloud database, then take action when it matches the block category in the Content Filter profile.



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

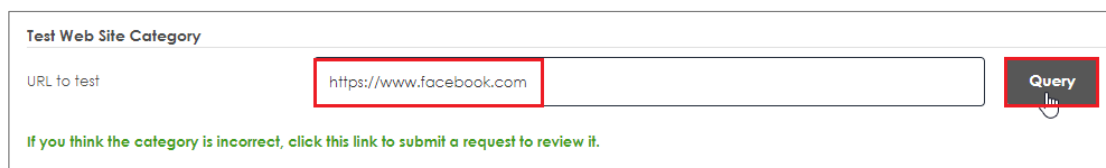
Log: log alert

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**.



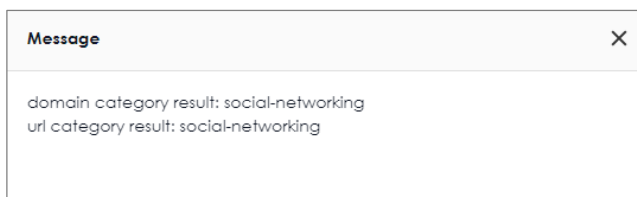
Test Web Site Category

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

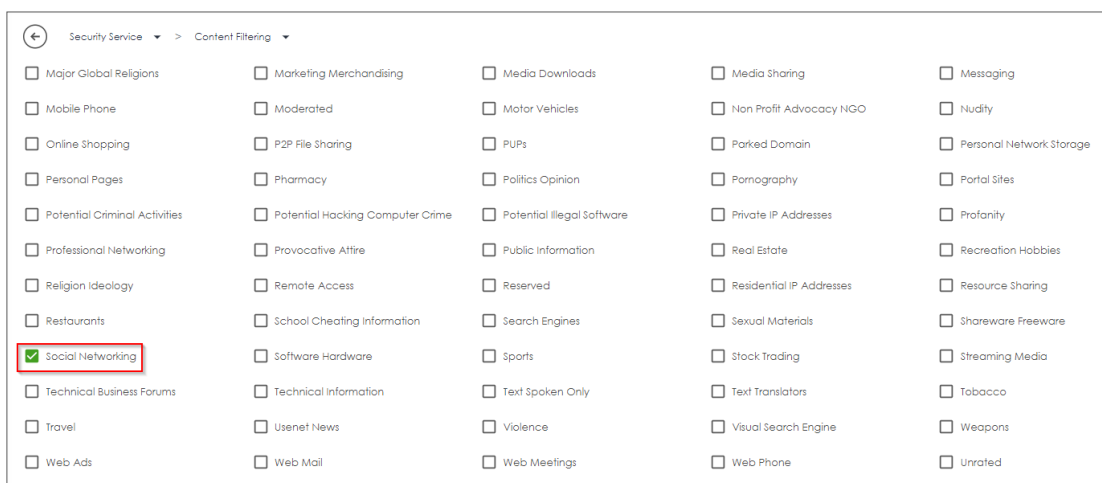
Query

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.



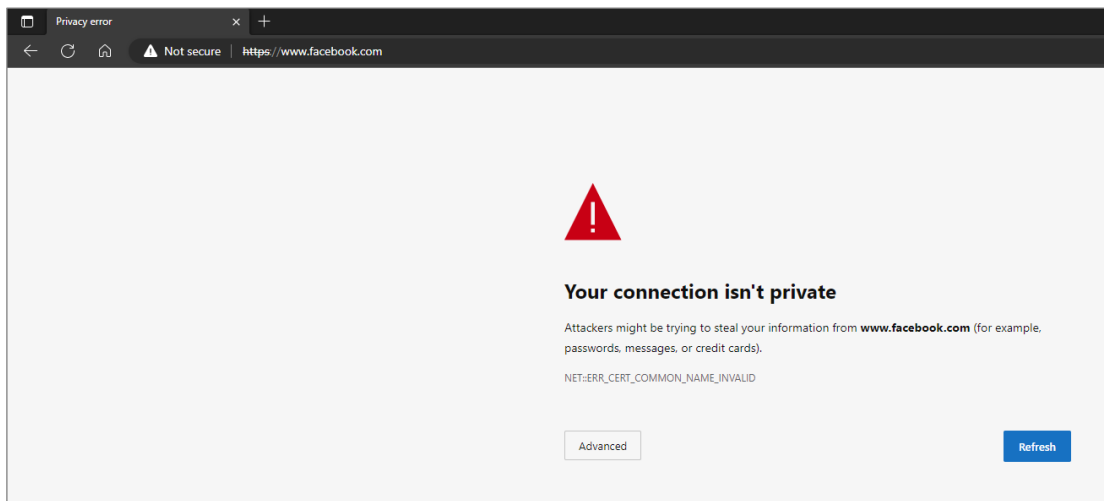
Set Up the Security Policy

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 at the top shows 'Security Policy' and '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 fields for 'From' (set to 'LAN'), 'To' (set to 'WAN'), 'Source' (set to 'any'), 'Destination' (set to 'any'), 'Service' (set to 'any'), 'User' (set to 'any'), and 'Schedule' (set to 'none'). The 'Action' is set to 'allow' and 'Log' is set to 'no'. The 'Profile' section at the bottom includes 'Application Patrol' (set to 'none'), 'Content Filter' (set to 'Social_Networking'), and 'SSL Inspection' (set to 'none'). Each of these three fields has a 'Log' checkbox and a 'by profile' dropdown menu.

Test Result

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

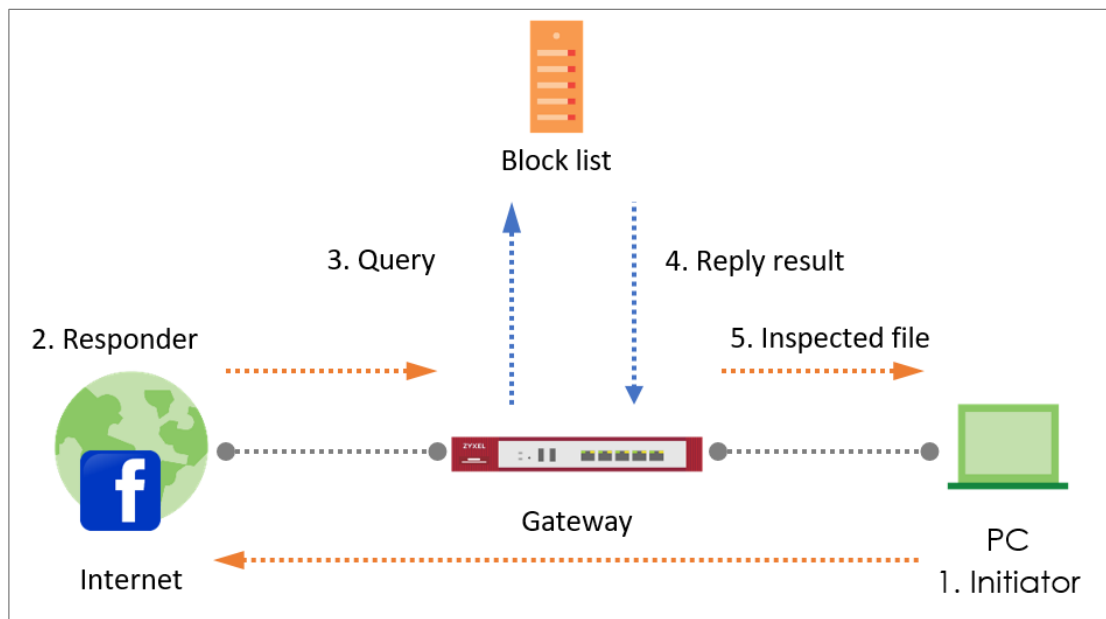


Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

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

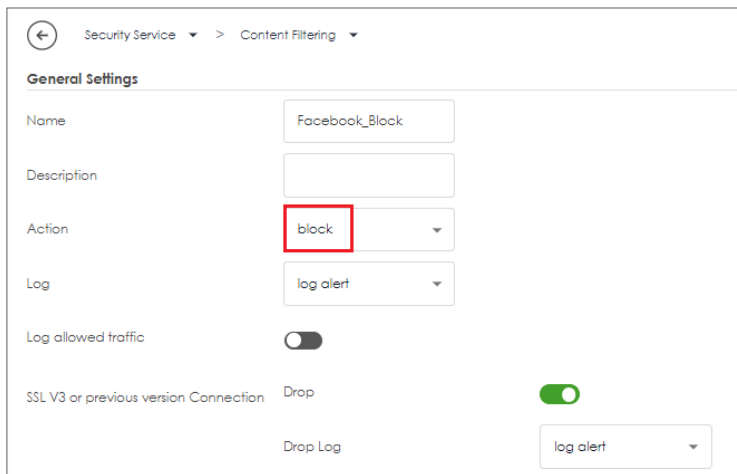
This is an example of using USG Flex H UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.



 **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**

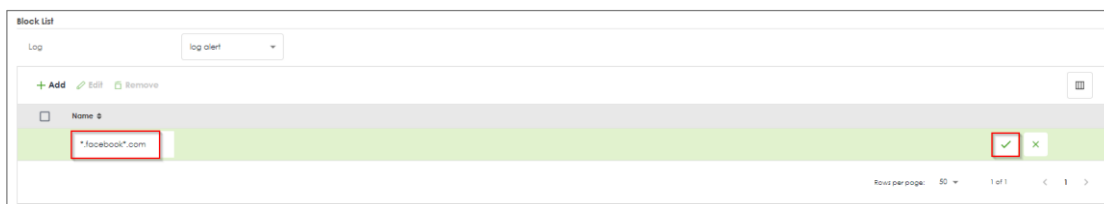
Log: log alert

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: *.facebook*.com

Rows per page: 50 1 of 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

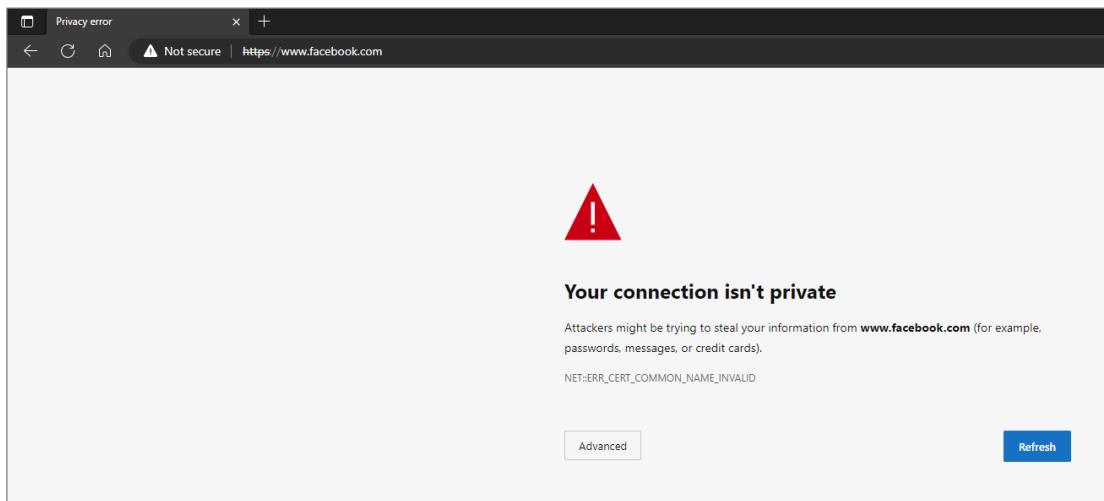
Content Filter: Facebook_Block

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.

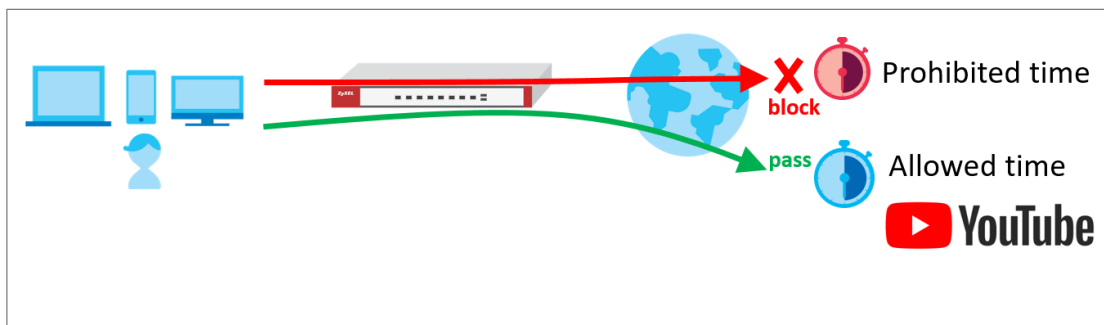


Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

#	Time	Category	Message	Source	Destination	Note
1	2023-05-22 15:36:59	content-filter	www.facebook.com\Block List, Rule_name:Facebook_Block, SSIN (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 [X]

Category and Application

1 youtube [X]

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	QUIC_UDP_443	
Description		
IP Protocol	UDP ▾	
Starting Port	443	(1..65535)
Ending Port	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	☒
Name	Block_QUIC_UDP443
Description	
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	☒		
Name	Block_Youtube		
Description			
From	LAN		
To	WAN		
Source	LAN1_SUBNET		
Destination	any		
Service	any		
User	any		
Schedule	Youtube_Block_Time		
Action	allow	▼	
Log	log alert	▼	

Profile

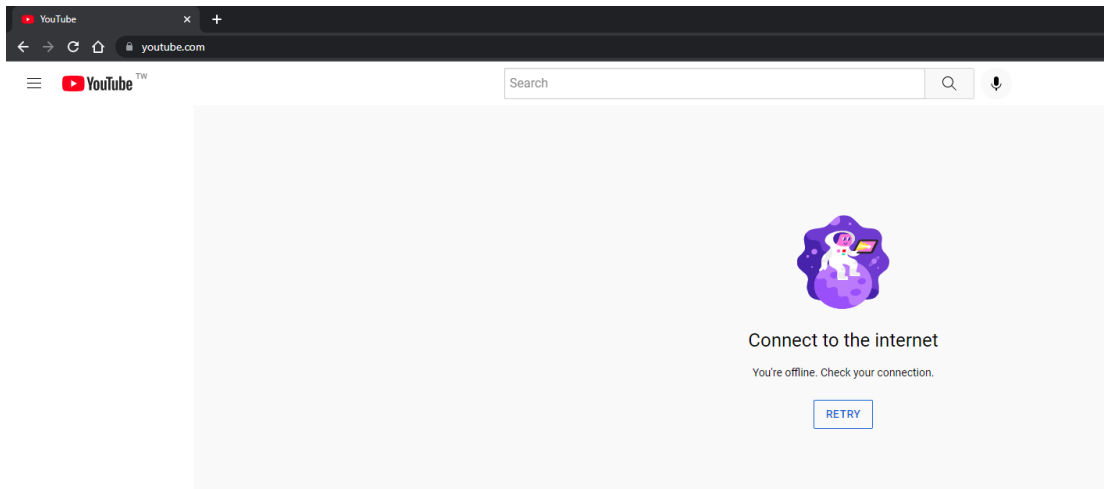
Application Patrol	Youtube	▼	Log	by profile	▼
Content Filter	none	▼	Log	by profile	▼
SSL Inspection	none	▼	Log	by profile	▼

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

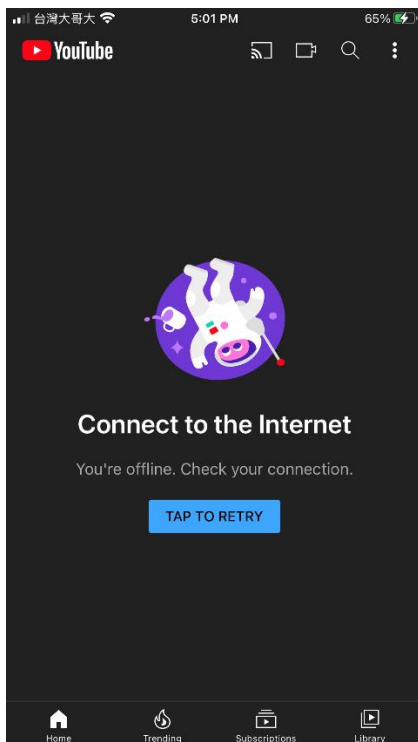
☐	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
☐		1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
☐		2	Block_YouTube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log-alert	

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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	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 SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT

How to Control Access to Google Drive

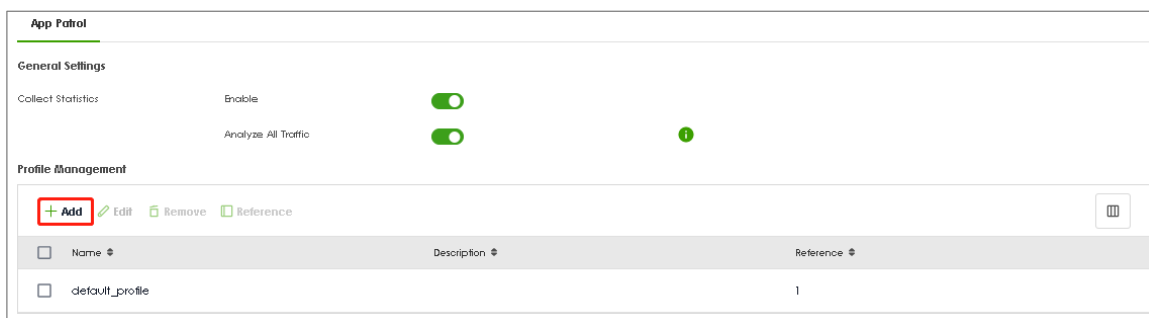
This is an example of using a FLEX UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.



 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 ☒

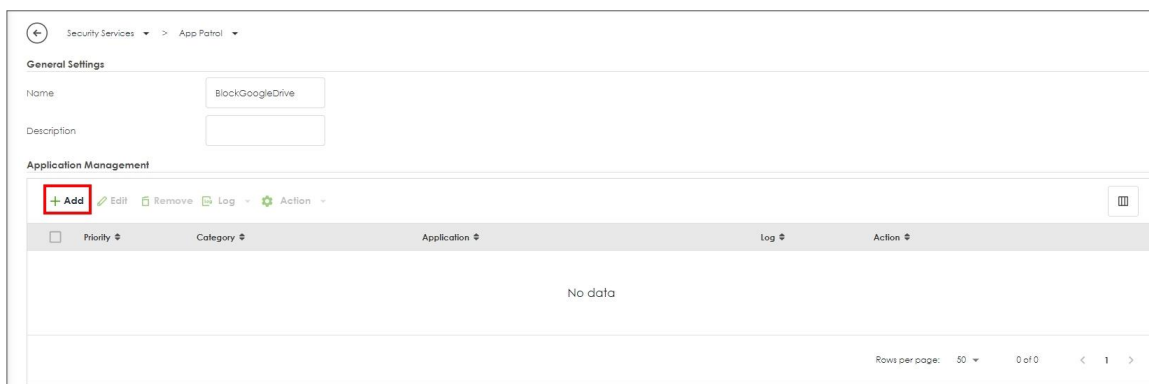
Analyze All Traffic: ☒ 1

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	tlsl_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.

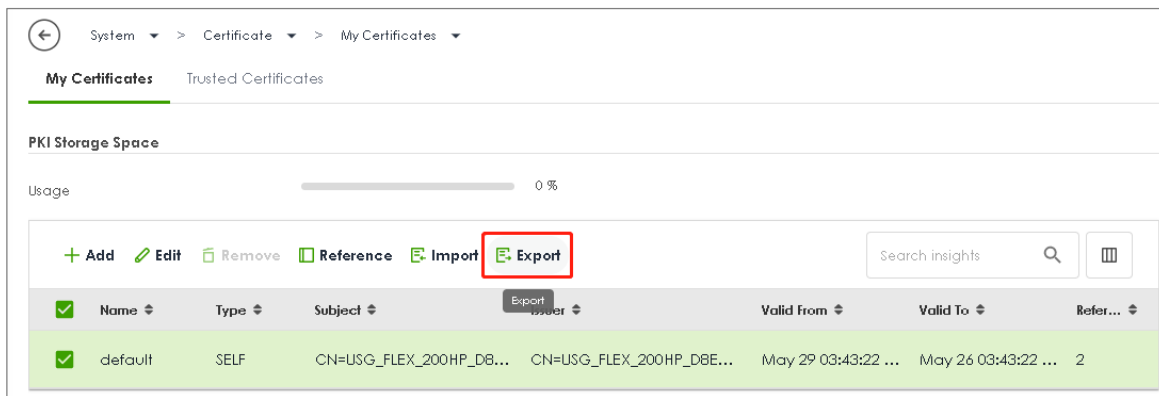
Profile

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

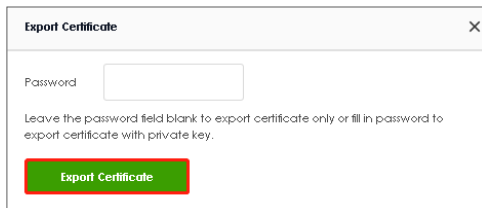
Export Certificate from FLEX and import to Lan hosts

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.

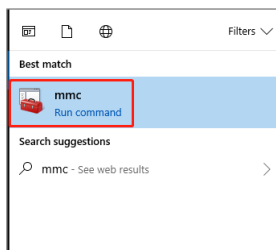
Go to System > Certificate > My Certificates to export default certificate from FLEX.



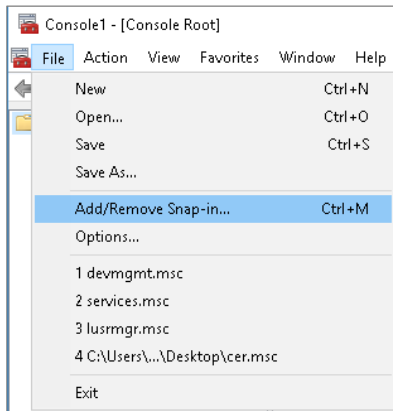
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



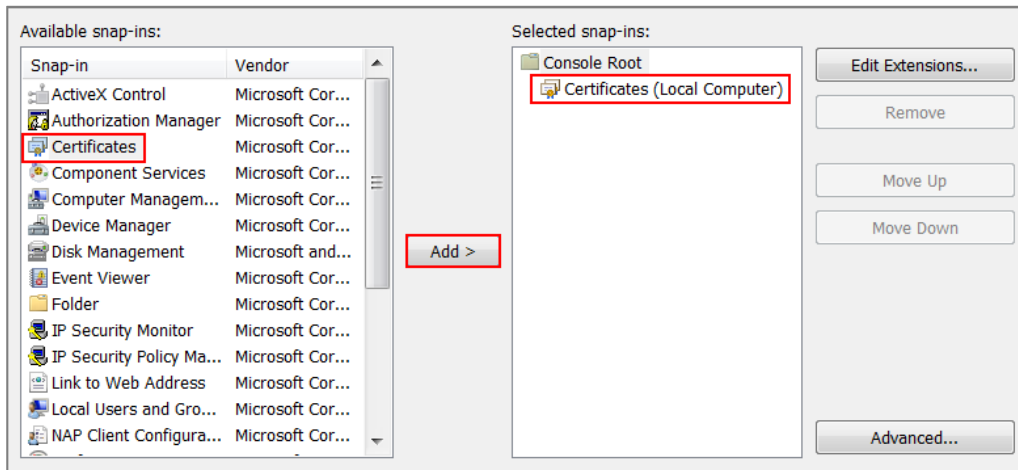
In Windows Start Menu > Search Box, type MMC and press Enter.



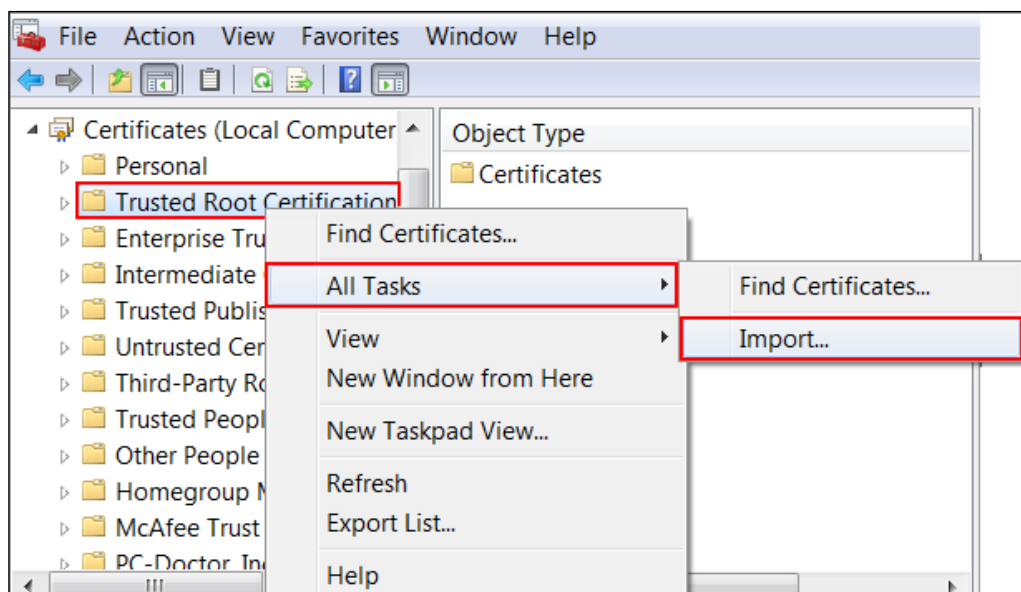
In the mmc console window, click File > Add/Remove Snap-in...



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.

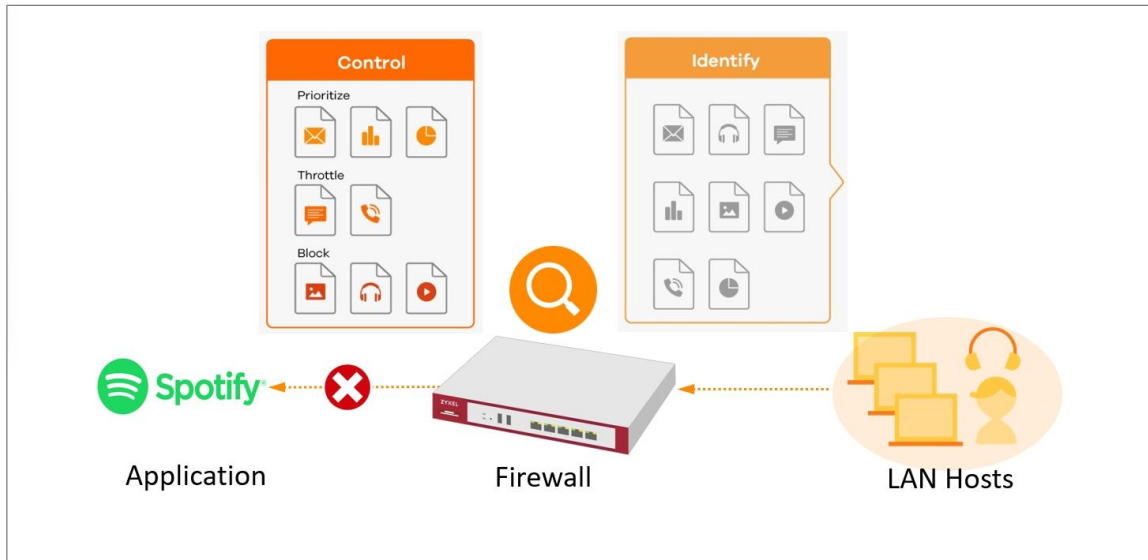
Go to Log & Report > Log/Events and select Application Patrol to check the logs.



#	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: Drop

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

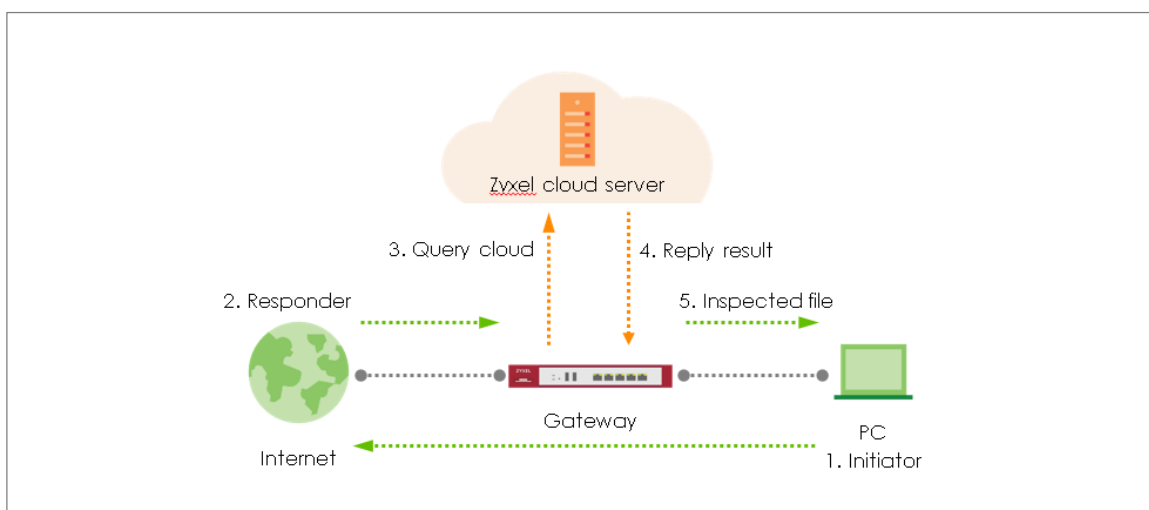
Clear Log

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

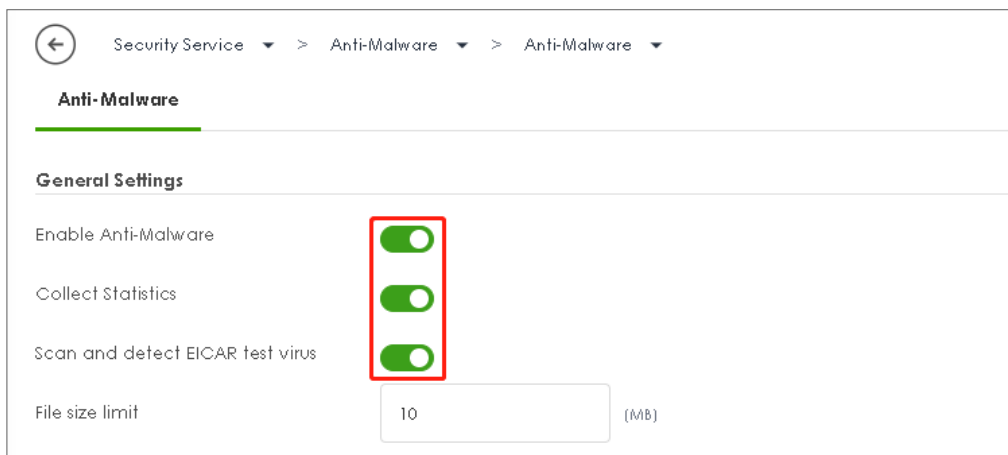
How does Anti-Malware Work

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

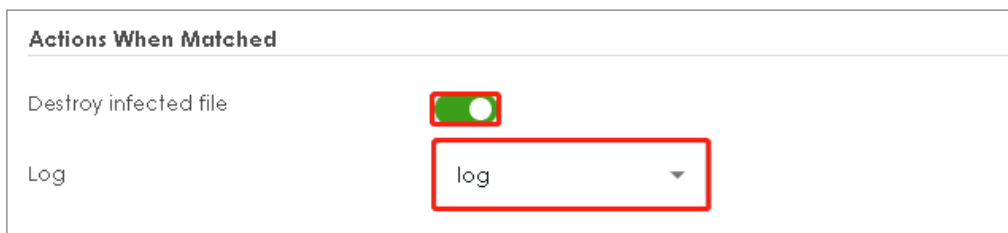
Enable Anti-Malware ☒

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

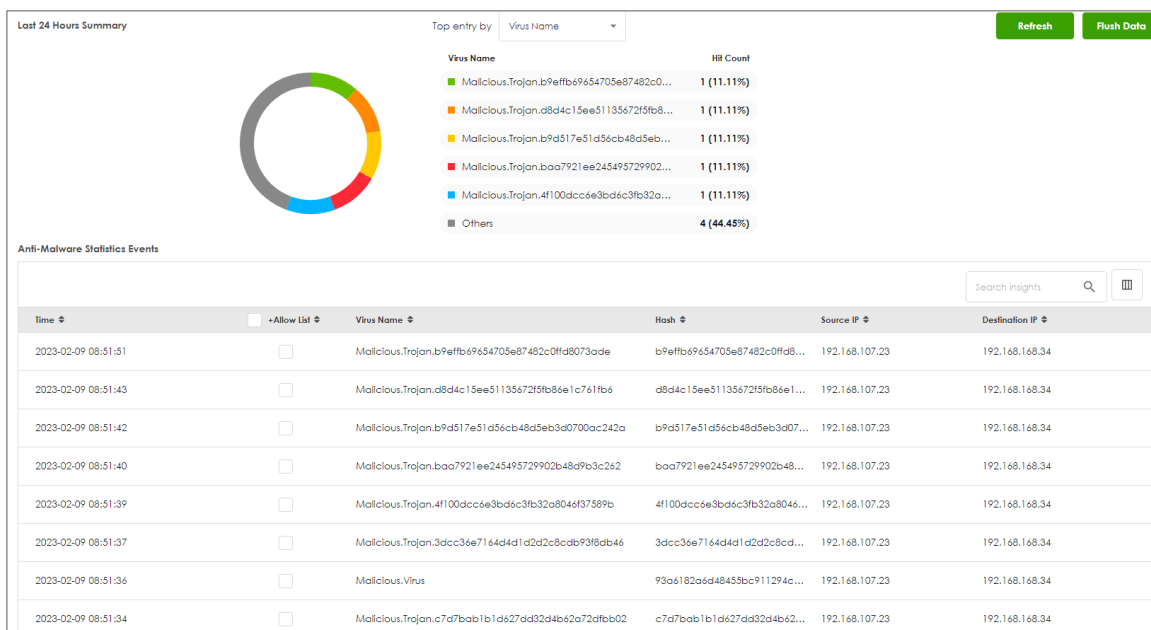
Test the Result

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.

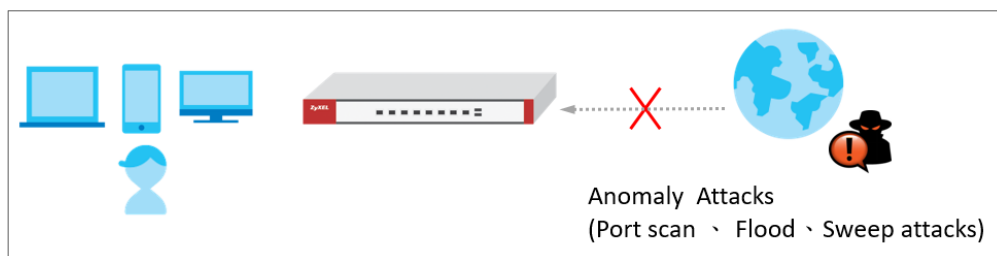
Category: Anti Malware						
Filter Refresh Clear Log						
#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus infected SSL:N Type:Cloud Query Virus:Malicious.Trojan.44d88612fea8a8f36de82e1278abb02f File:eicar.com.txt Protocol:HTTP md5:4d88612fea8a8f36de82e1278abb02f	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)

Status	Name	Log	Action
☐ Active	(portcan) IP Protocol Scan	log	block
☐ Active	(portcan) TCP Portscan	log	block
☐ Active	(portcan) UDP Portscan	log	block
☐ Active	(sweep) ICMP Sweep	log	block
☐ Active	(sweep) IP Protocol Sweep	log	block
☐ Active	(sweep) TCP Sweep	log	block
☐ Active	(sweep) UDP Sweep	log	block

Flood Detection

Block Period: 5 (1-3600 seconds)

Status	Name	Log	Action	Threshold
☐ Active	(flood) ICMP Flood	log	block	1000
☐ Active	(flood) IP Flood	log	block	1000
☐ Active	(flood) TCP Flood	log	block	1000
☐ Active	(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

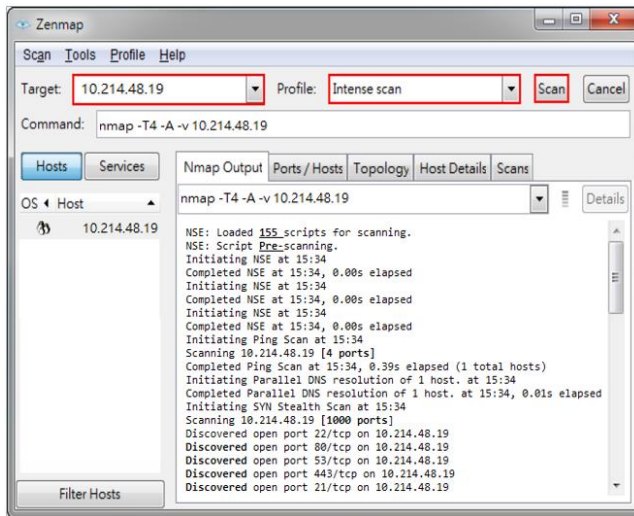
	Status	Priority	Name	From	Anomaly Profile
☐	Active	1	DoS_Prevention	WAN	DoS_Prevention

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.



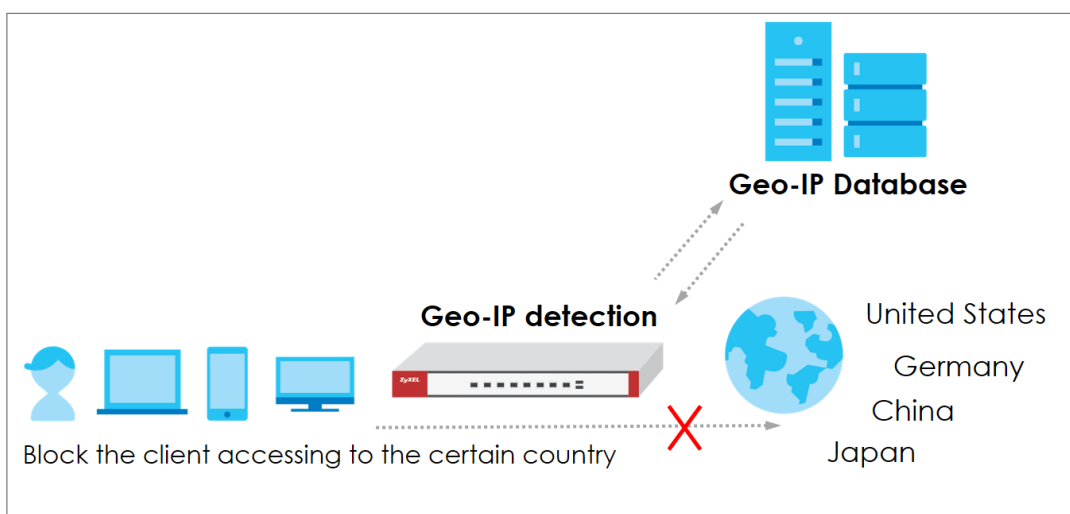
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.

Log & Report > Log / Events						
Category: All Log 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.

Object > Address > Address

Address Address Group Geo IP

IPv4 Address Configuration

+ Add Edit Remove Reference

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.

←

Object ▾ > Address ▾

Group Members

Name

geo_block

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).

Copyright © 2026 Zyxel and/or its affiliates. All rights reserved. 148

←

Security Policy ▾ > Policy Control ▾

Configuration

Enable

Name

geo_block_policy

Description

From

LAN

To

WAN

Source

any

Destination

geo_block

Service

any

User

any

Schedule

none

Action

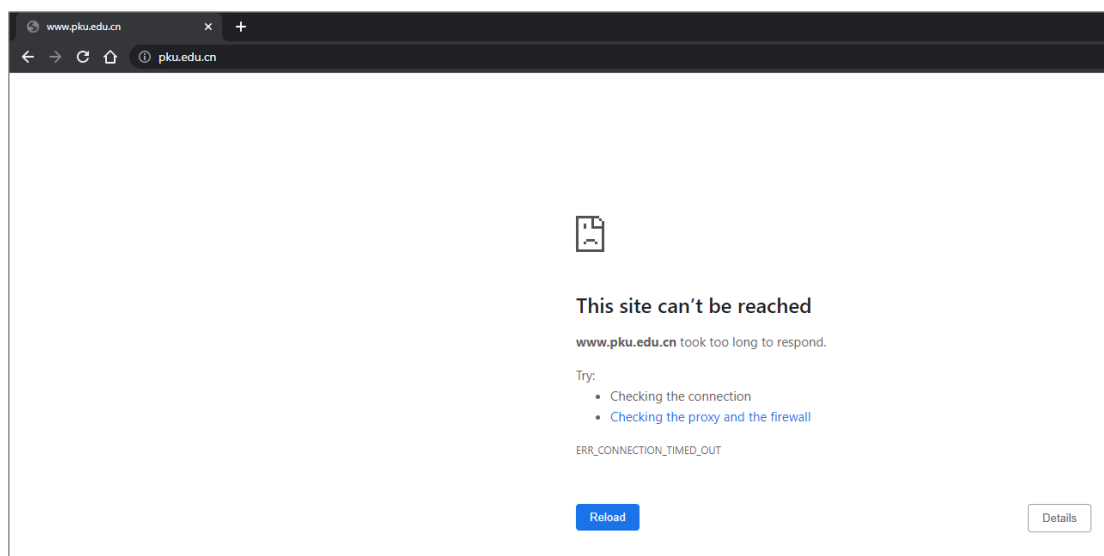
deny

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.

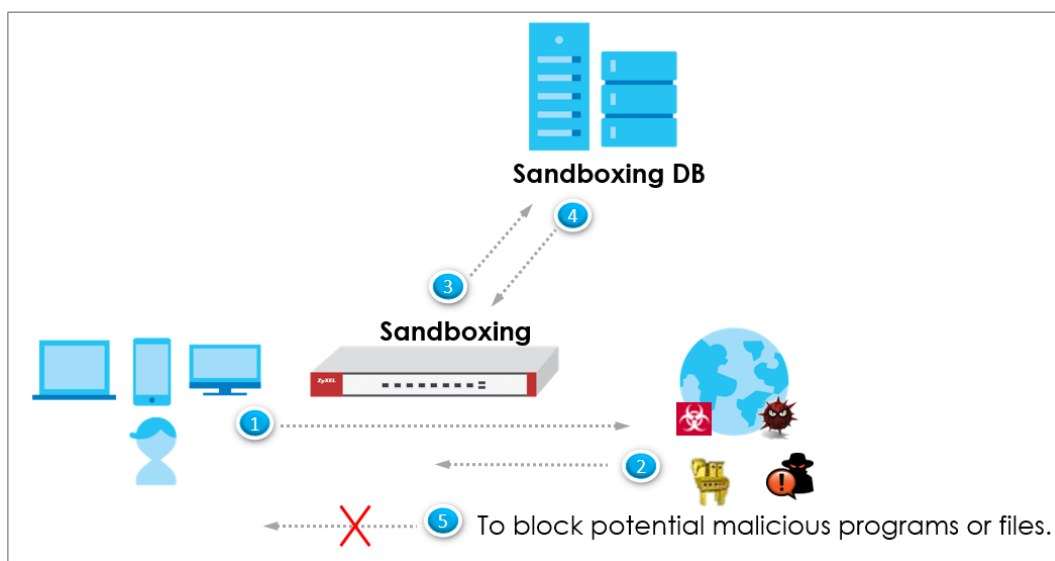


To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

#	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?

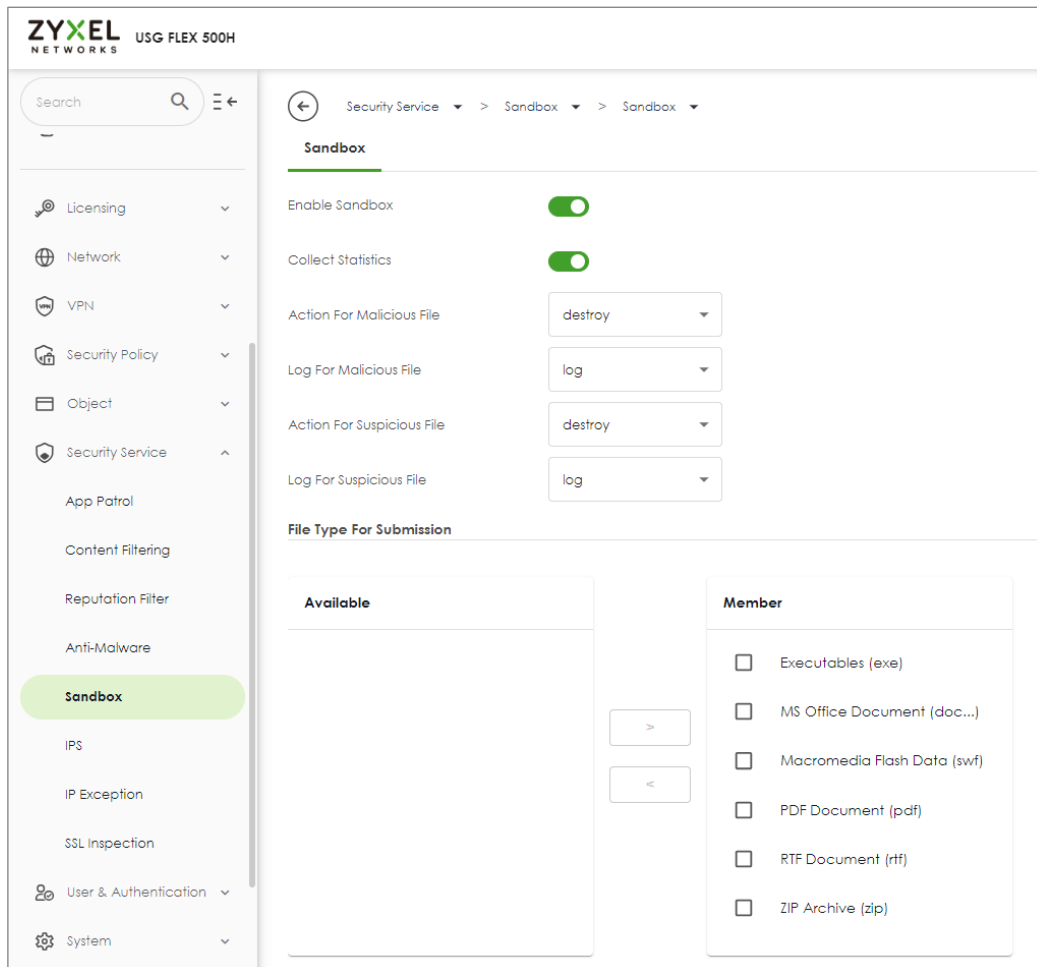
This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



 **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).



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.



The screenshot shows the 'Log & Report' interface with the 'Log / Events' tab selected. The 'Category' is set to 'Sandbox'. The log entry shows a query for a file named 'wildfire-test-pe-file.exe' with MD5 'a2b6588b52aebc5a7e164b70114b4a57' and file ID '58207' over HTTP from source IP '34.84.44.247' to destination IP '192.168.168.34'. The note indicates it was a 'SANDBOX QUERY'.

#	Time	Category	Message	Source	Destination	Note
2	2023-07-31 16:18:14	Sandbox	Query File name: wildfire-test-pe-file.exe, md5: a2b6588b52aebc5a7e164b70114b4a57, file id: 58207, protocol: HTTP, hidi: 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	☒	
Action	block ▼	
Threat Level Threshold	high ▼	
Log	log ▼	
Statistics	☒	

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		
☒ Anonymous Proxies	☒ Denial of Service	☒ Exploits
☒ Negative Reputation	☒ Scanners	☒ Spam Sources
☒ TOR Proxies	☒ Web Attacks	☒ Phishing
Types of Cyber Threats Coming From The Internet And Local Networks		
☒ 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

☐

Status

IPv4 Address

No data

Rows per page: 50

0 of 0

<

1

>

Block List

Enable

☒

Log

log

+ Add

Edit

Remove

Active

Inactive

☐

Status

IPv4 Address

☐

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

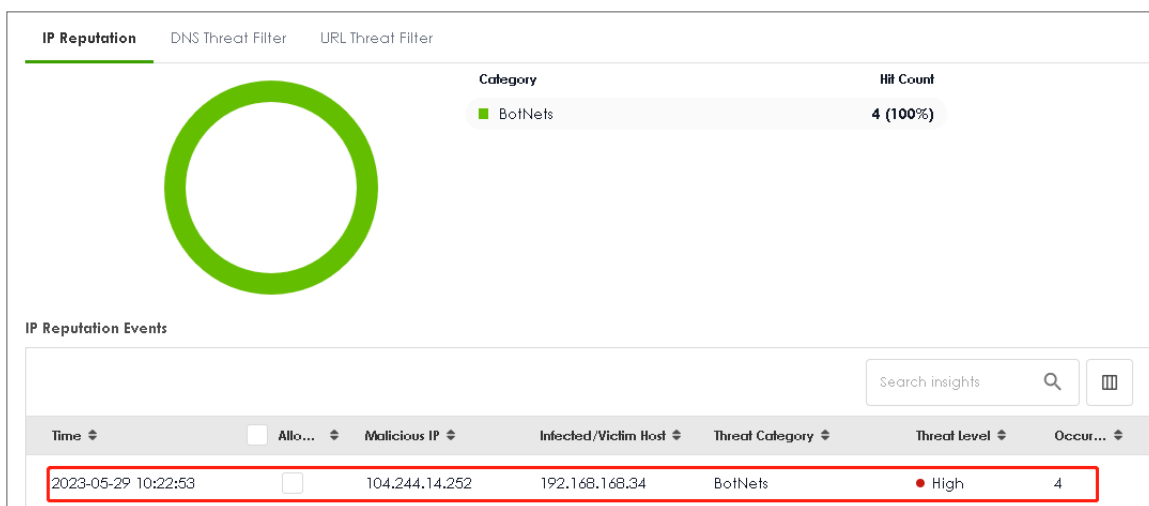
Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.

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	☒	
Action	block ▼	
Log	log alert ▼	
Statistics	☒	

Security Threat Categories

☒ Anonymizers

☒ Browser Exploits

☒ Malicious Downloads

☒ Malicious Sites

☒ Phishing

☒ Spam URLs

☒ 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

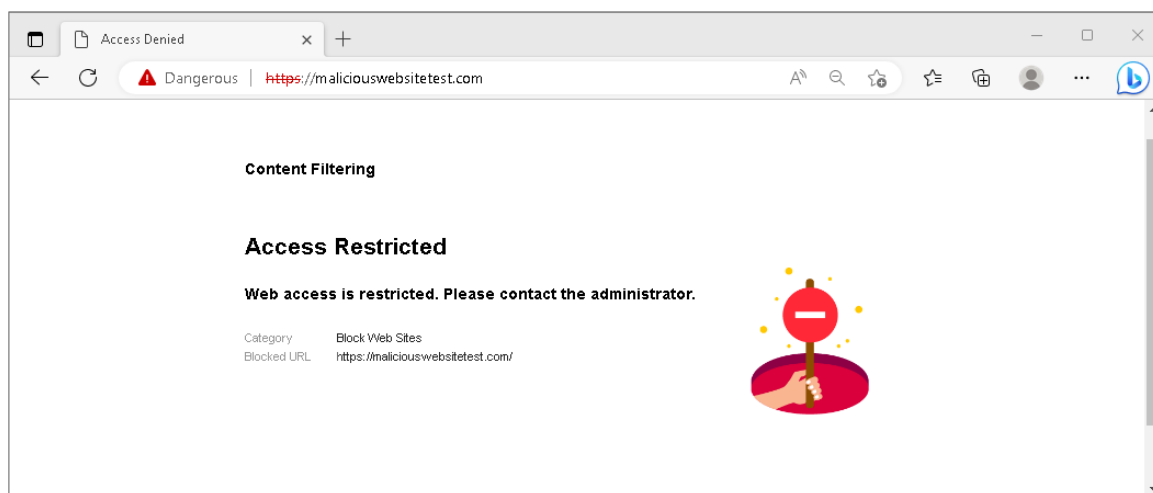
Query

Message

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

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

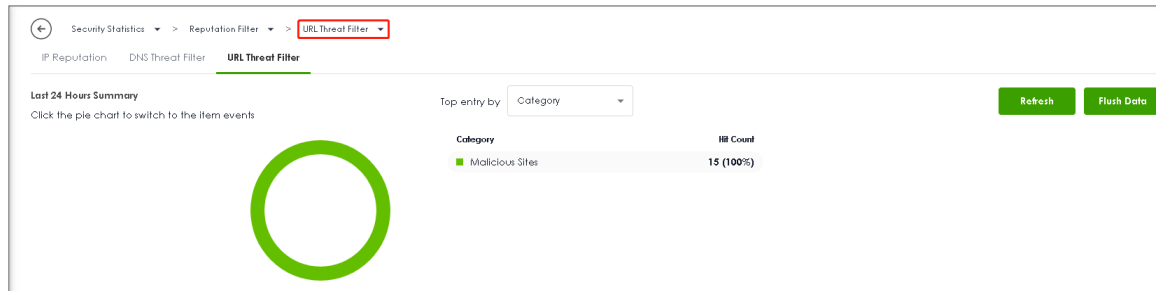
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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	maliciouswebsitetest.com:Malicious Sites, SSItN	192.168.168.34	50.63.7.226	ACCESS BLOCK
3	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSItN	192.168.168.34	50.63.7.226	ACCESS BLOCK
4	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSItN	192.168.168.34	50.63.7.226	ACCESS BLOCK
5	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSItN	192.168.168.34	50.63.7.226	ACCESS BLOCK
6	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSItN	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.



Time	Allow list	URL	Category	Source IP	Destination IP
2023-05-28 02:33:39	☐	maliciouswebsite-test.com/	Malicious Sites	192.168.1.68.33	54.163.229.19
2023-05-28 02:33:40	☐	maliciouswebsite-test.com/favicon.ico	Malicious Sites	192.168.1.68.33	54.163.229.19
2023-05-28 02:33:41	☐	maliciouswebsite-test.com/favicon.ico	Malicious Sites	192.168.1.68.33	54.163.229.19
2023-05-28 07:40:47	☐	maliciouswebsite-test.com	Malicious Sites	192.168.1.68.34	50.63.7.226
2023-05-28 07:40:51	☐	maliciouswebsite-test.com	Malicious Sites	192.168.1.68.34	50.63.7.226
2023-05-28 07:40:55	☐	maliciouswebsite-test.com	Malicious Sites	192.168.1.68.34	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
maliciouswebsitetest.c
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)

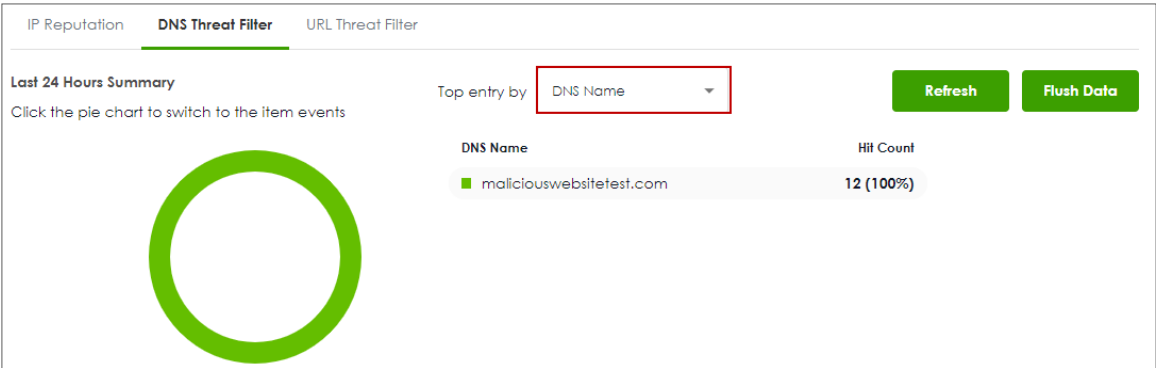
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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.

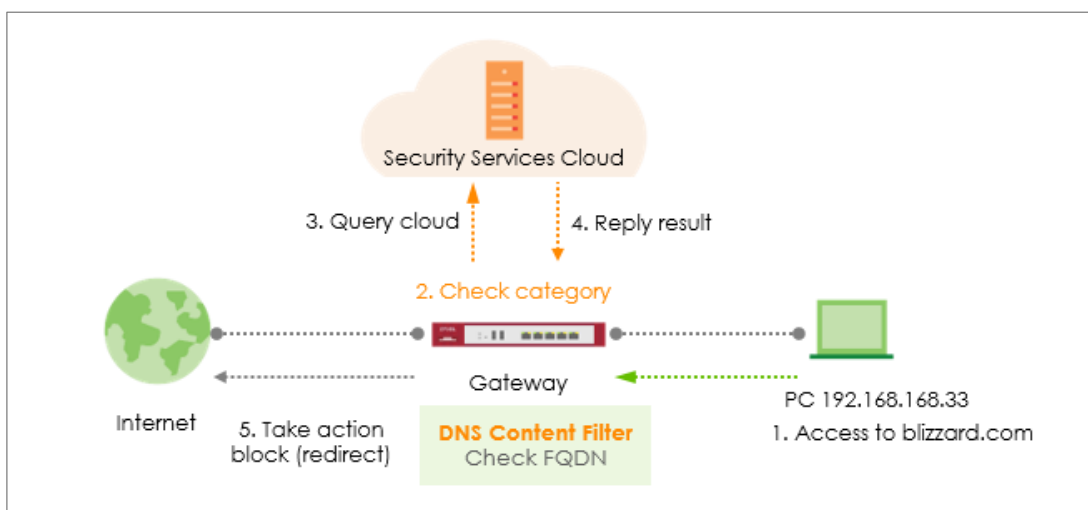


DNS Threat Filter Events				
Search insights				
Time	☐ +Allow ...	DNS Name	Category	Source IP
2023-05-21 16:29:36	☐	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:44:04	☐	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:47:02	☐	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:49:26	☐	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.

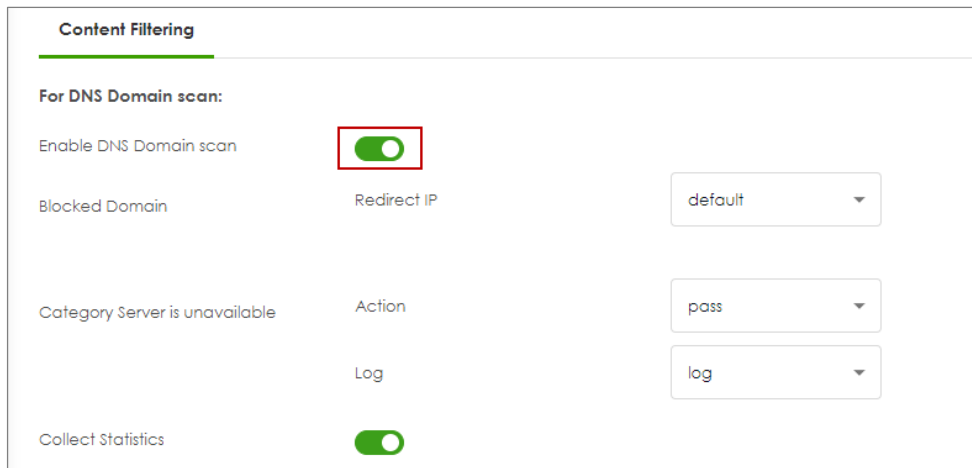
DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those 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/>.

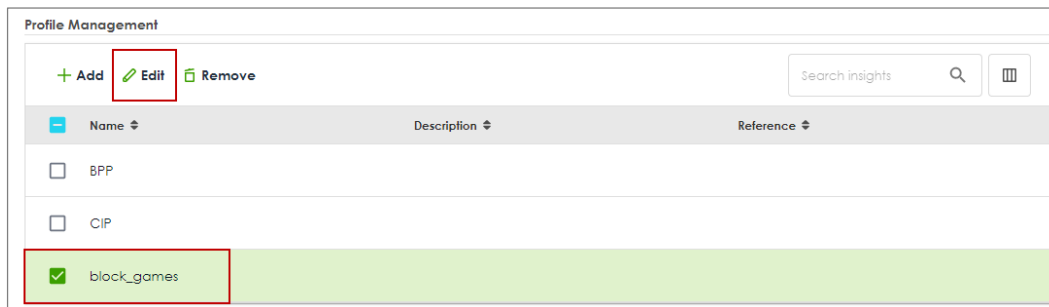


The screenshot shows the 'Content Filtering' configuration page. Under the 'For DNS Domain scan:' section, the 'Enable DNS Domain scan' toggle is turned on and highlighted with a red box. Below this, there are three rows of settings:

- 'Blocked Domain' is set to 'Redirect IP'.
- 'Category Server is unavailable' is set to 'pass'.
- 'Log' is set to 'log'.

At the bottom, the 'Collect Statistics' toggle is also turned on.

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



The screenshot shows the 'Profile Management' page. At the top, there are buttons for '+ Add', 'Edit' (highlighted with a red box), and 'Remove'. Below these is a search bar labeled 'Search insights'. The main area is a table with columns for 'Name', 'Description', and 'Reference'. The table contains three rows:

- 'BPP' with an unchecked checkbox.
- 'CIP' with an unchecked checkbox.
- 'block_games' with a checked checkbox, highlighted with a red box.

Action: block

Log: log or log alert

General Settings

Name

block_games

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
☐		1	LAN_Out...	LAN	any (Ex...	any	any	any	any	none	allow	no	☒
☐		2	DMZ_to_...	DMZ	WAN	any	any	any	any	none	allow	no	block_games

Test the Result

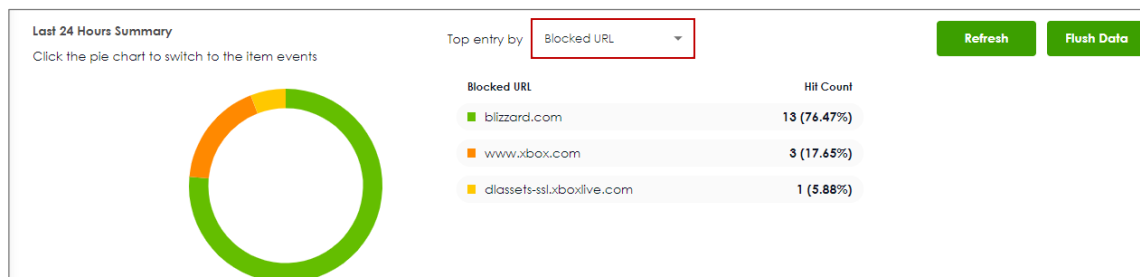
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



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

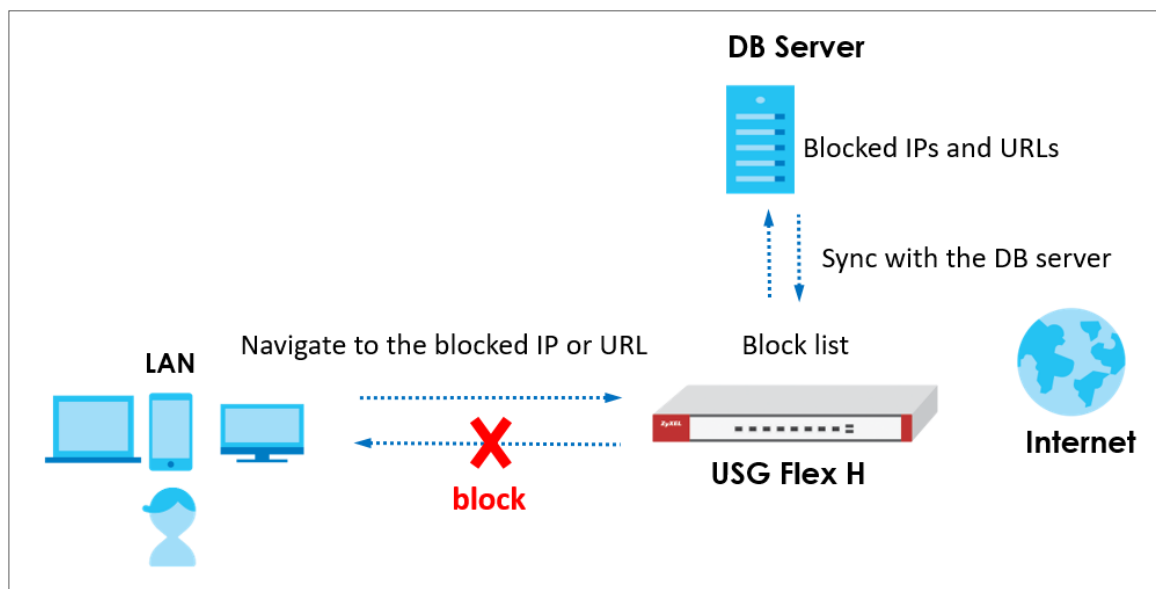
Go to Security Statistics > Content Filter to check summary of all events.



Content Filter Events						
Search insights						
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.

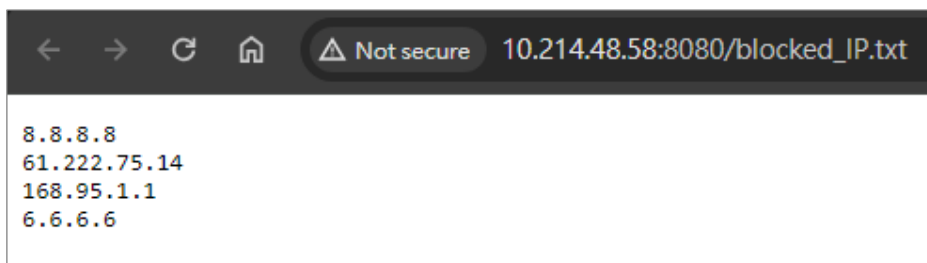


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

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
☐	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

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. Below this is the 'Profile Management' section, which includes '+ Add' and 'Remove' buttons. A table lists the 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. It contains the text 'Synchronize the signature to the latest version with online update server.' and a green 'Update Now' button. There is also an 'Auto Update' toggle switch that is turned off. Underneath, there are radio buttons for 'Every N Hours', 'Daily' (which is selected), and 'Weekly'. Each radio button 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 'Category' dropdown set to 'All Log', and buttons for 'Refresh', 'Clear Log', and 'Export'. A search bar is also present. Below this is a table with the following data:

#	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.

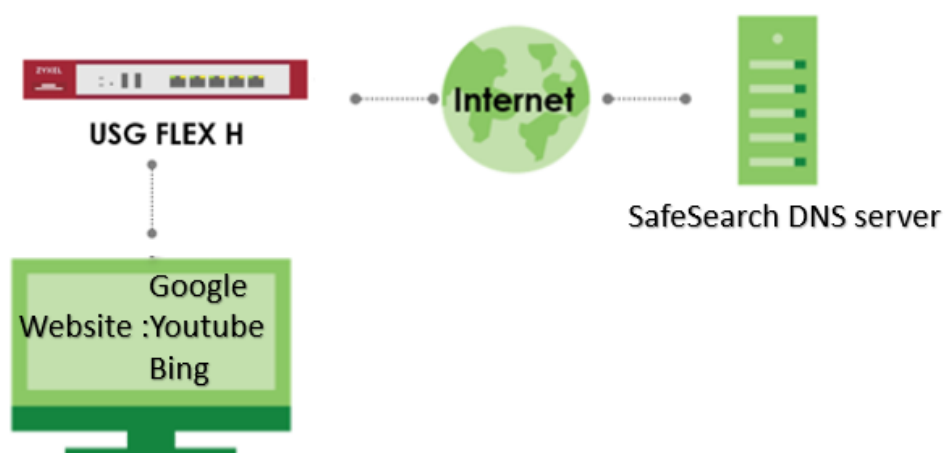
Go to Log & Report > Log / Events to observe block messages.

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.

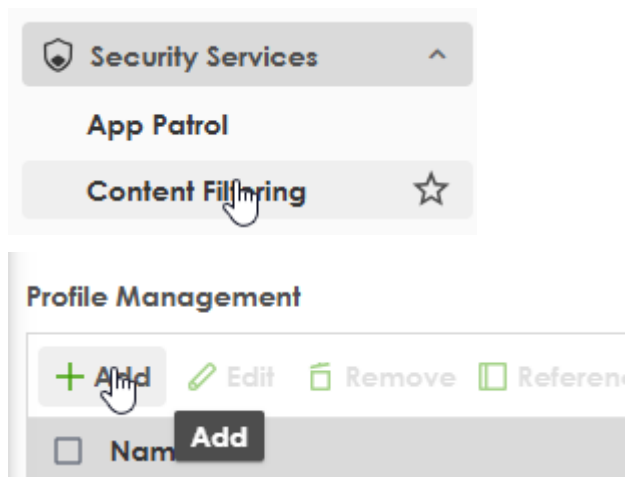
This guide explains how to configure your gateway to set up DNS Safe Search.



 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 in the ZyXel Local Web GUI. The page is titled 'General Settings' and contains 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

DNS SafeSearch 

SSL V3 or previous version Connection

- Enforce safe search on Google, YouTube and Bing.
- To enable DNS Safe Search, please make sure DNS Domain Scan is turned on.

Restrict YouTube Access Strict

Drop

Drop Log

Strict

Moderate

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

Info

Profile SafeSearch has been saved. A profile takes effect only when it is applied to a security policy. Apply this profile to a security policy now?

Cancel OK

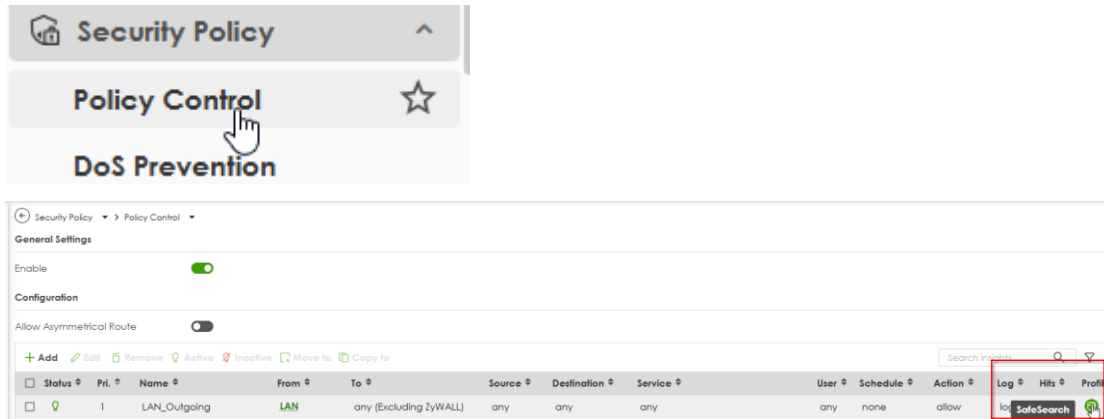
[hs1]

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
☒		1	LAN_Outgoing	LAN	any (Excluding ZyWALL)	any	any	any	any	none	allow	log
☐		2	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no
☐		3	IPSec_VPN_Outgoing	IPSec_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
☐		8	SSL_VPN_Outgoing	SSL_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
☐		10	NEBULAVPN_Outgoing	NEBULAVPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
☐		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.



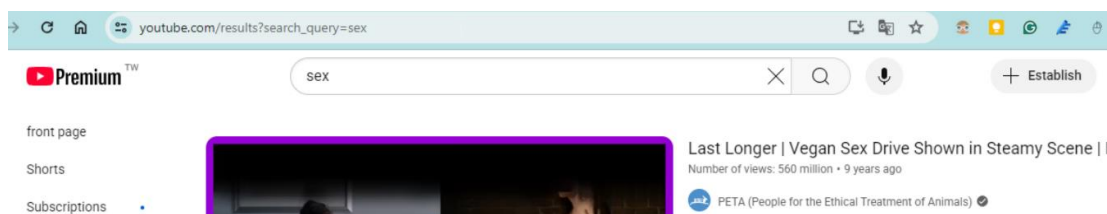
Step 3: Verified SafeSearch Function

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

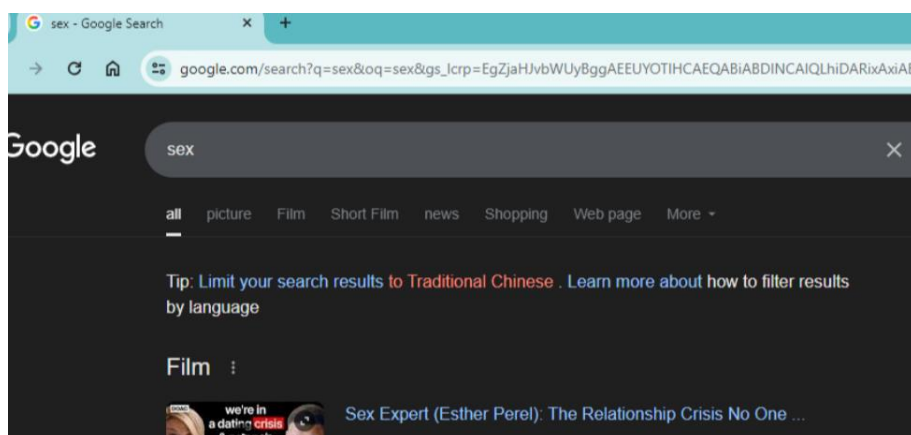
Non-authoritative answer:
Name:     youtube-ui.l.google.com
Addresses: 2404:6800:4012:9::200e
           2404:6800:4012:6::200e
           2404:6800:4012:5::200e
           2404:6800:4012:8::200e
           142.250.66.78
           142.250.204.46
           142.250.196.206
           142.250.198.78
Aliases: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



www.google.com

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

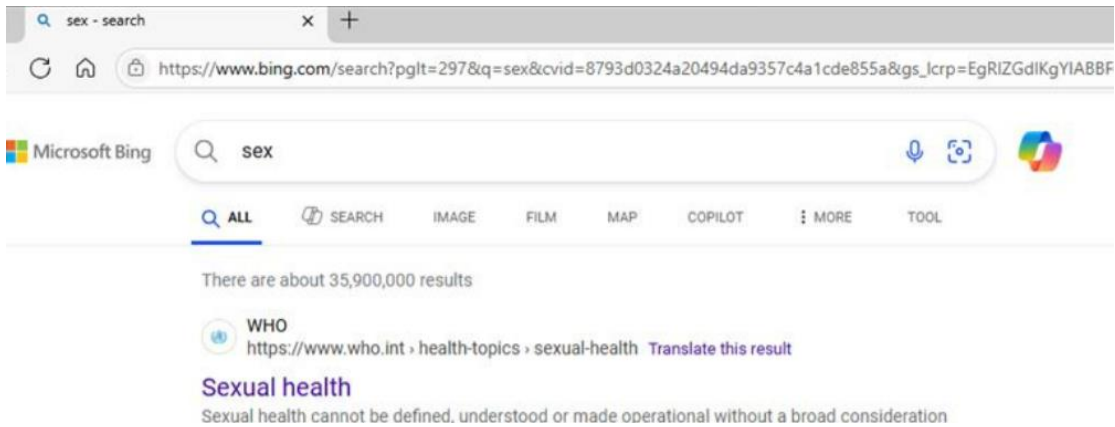
Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4012:9::2004
          142.250.196.196
```



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
```



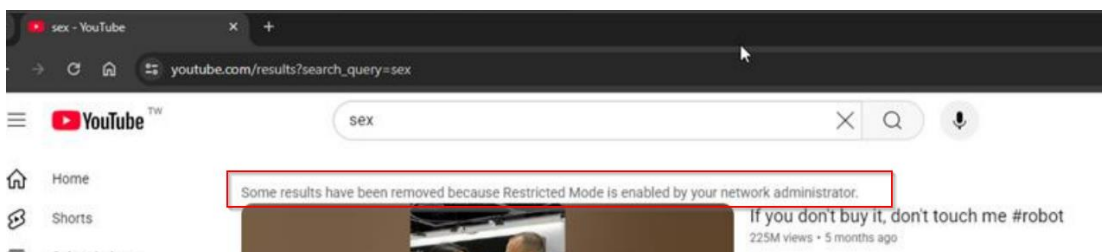
Ensure that the DNS server assignment is automatic get from the firewall.

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

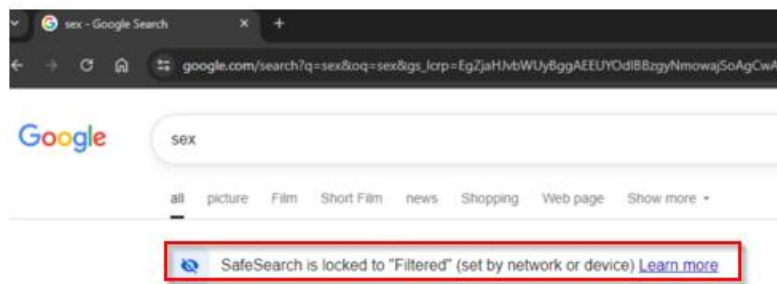
Name: www.youtube.com
Address: 216.239.38.120
Aliases: www.youtube.com
```



www.google.com

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

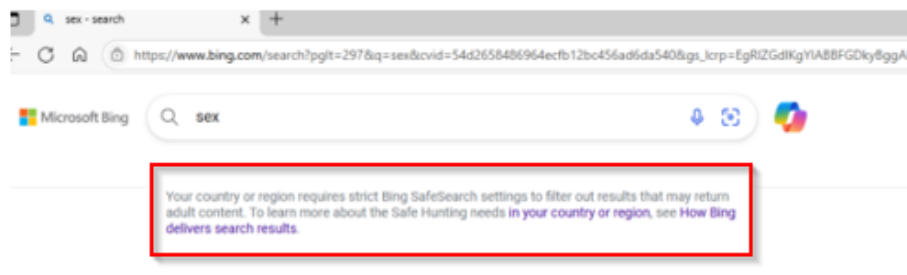
Name:    www.google.com
Address: 216.239.38.120
Aliases: www.google.com
```



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

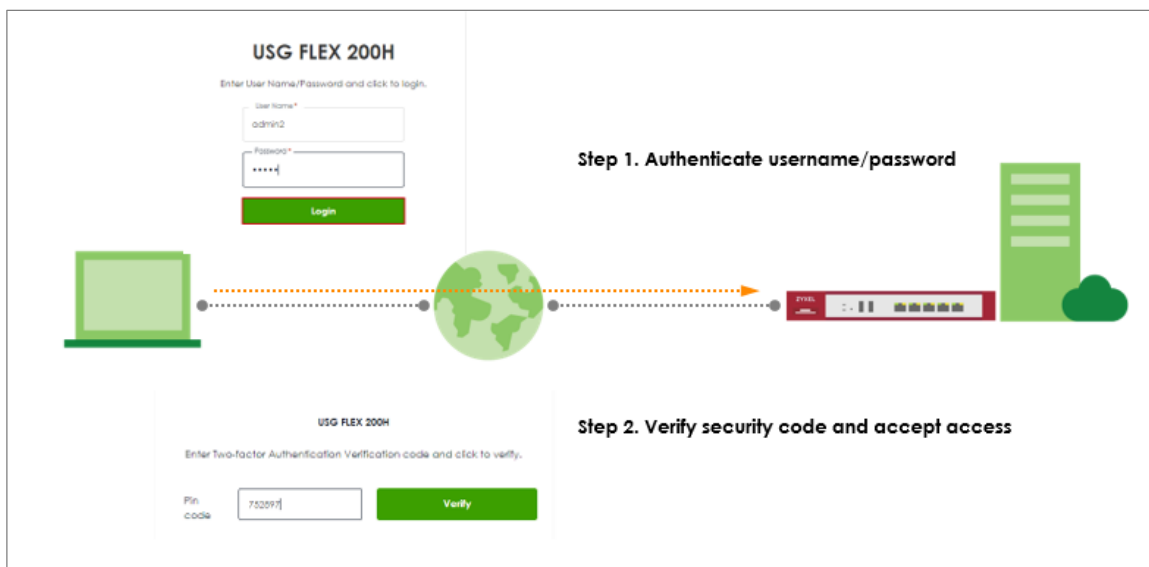
DNS Safe Search is not working

- 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.

Email 1

Email 2

Mobile Number

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

Lease Time: 1440 minutes

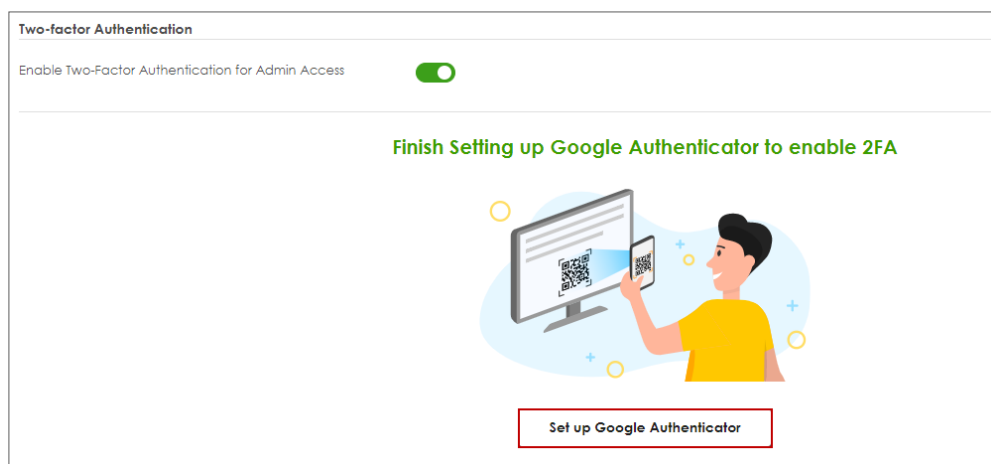
Reauthentication Time: 1440 minutes

Two-factor Authentication

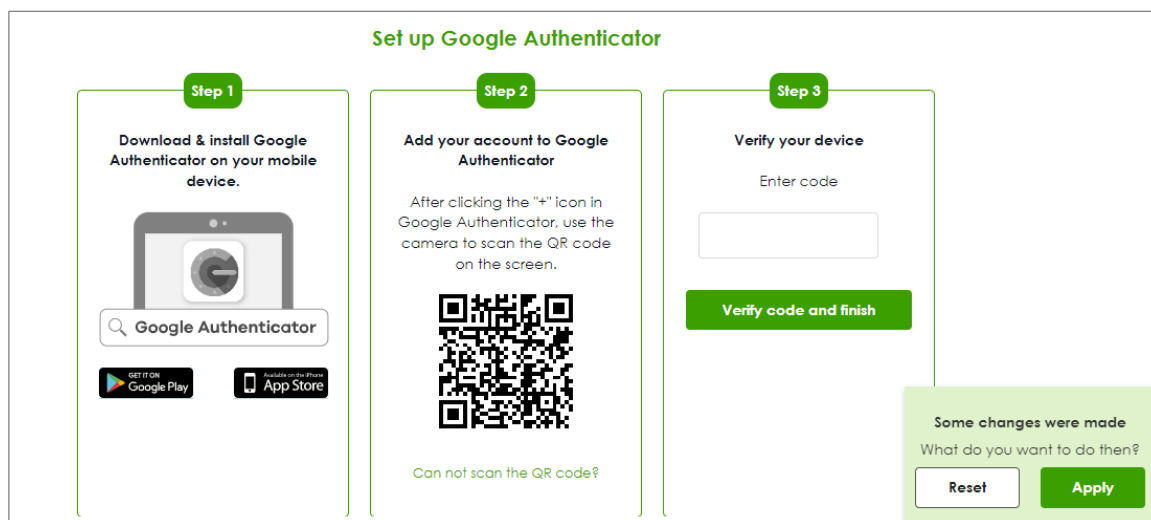
Enable Two-Factor Authentication for Admin Access ☒

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

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



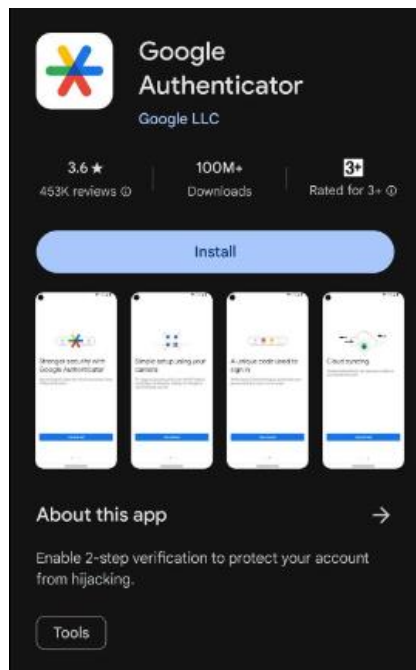
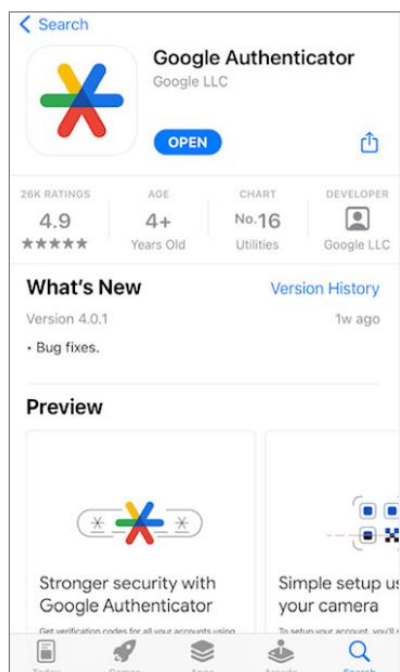
Set up Google Authenticator



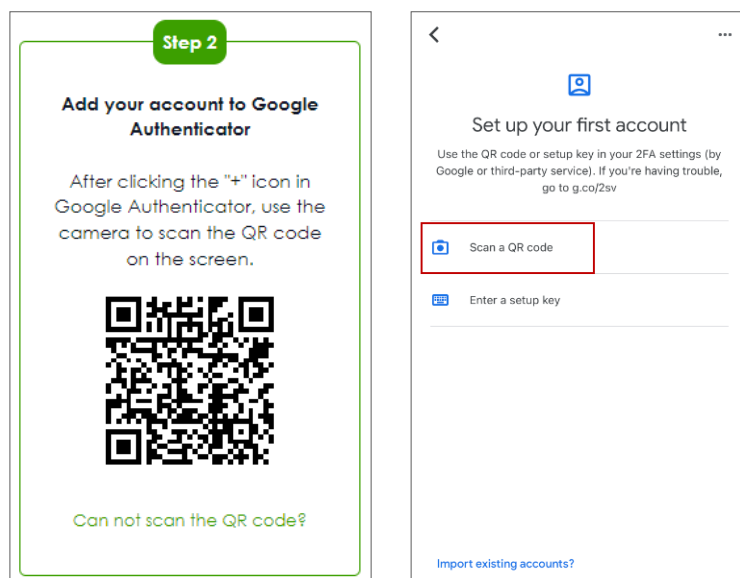
1. Download and install Google Authenticator on your mobile device.

Apple Store

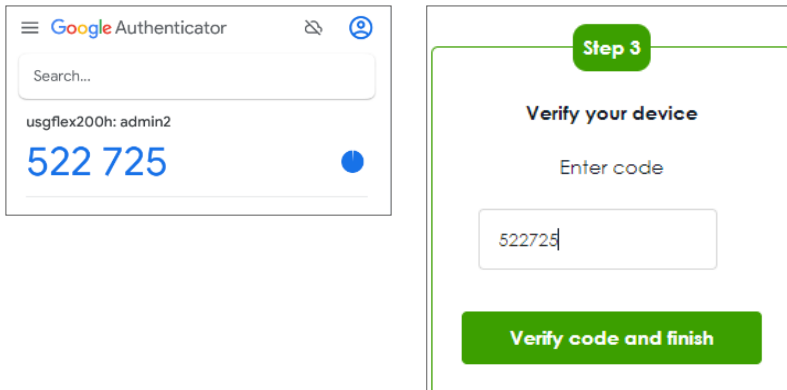
Google Play



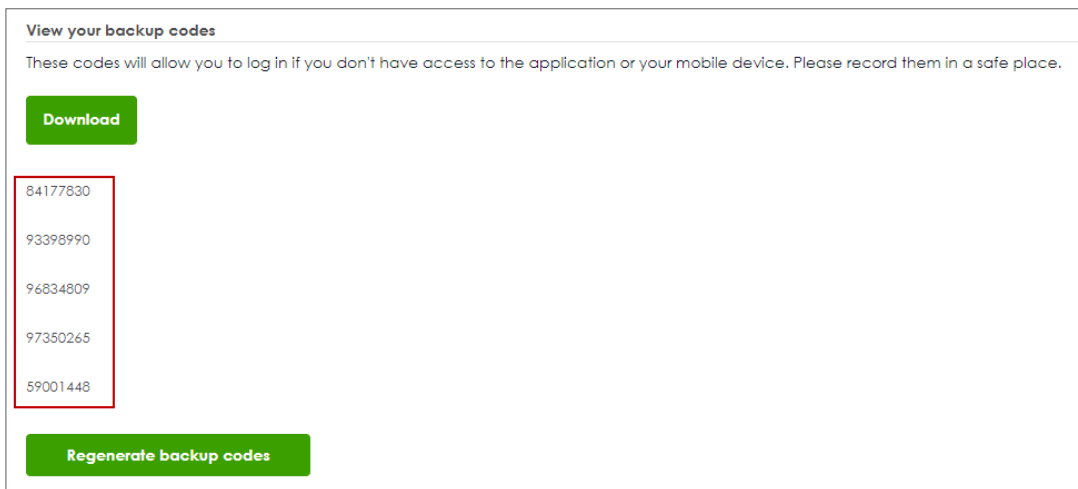
2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



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.



4. 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.



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

3

(1-5 minutes)

Two-factor Authentication for Services:

Web

SSH

Test the Result

1. Login with the admin account "admin2".

USG FLEX 200H

Enter User Name/Password and click to login.

User Name *

admin2

Password *

••••|

Login

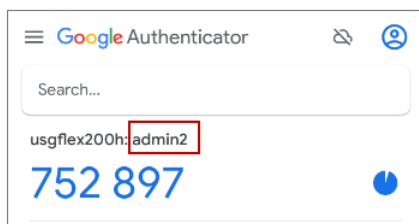
2. A pop-up window appears for administrator to enter the verification code.

USG FLEX 200H

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

Pin 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.



USG FLEX 200H

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

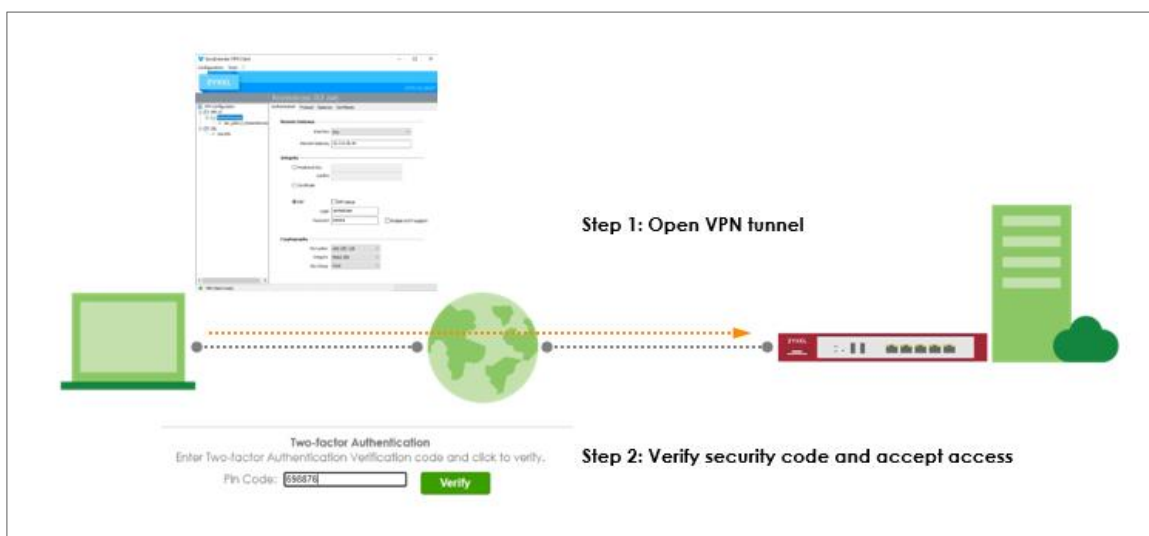
Pin code

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

Category User Filter Refresh Clear Log Search insights						
#	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

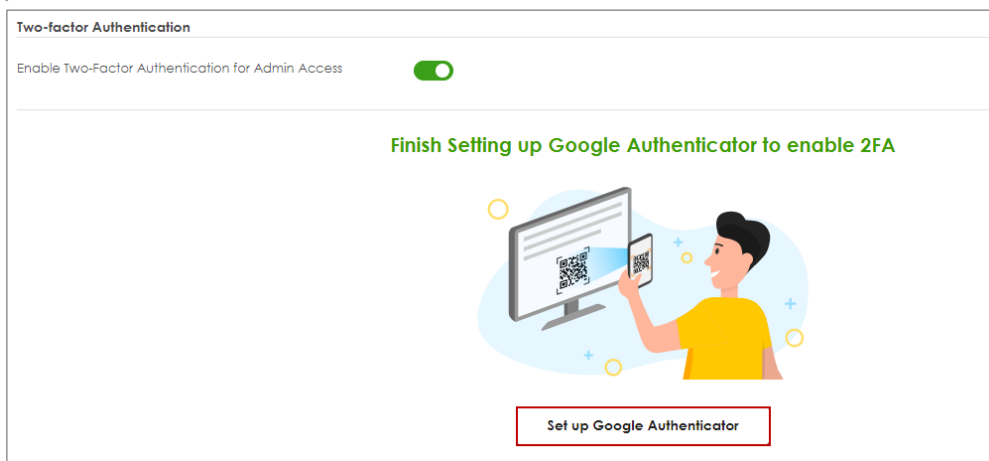
Profile Management

User Name	vpntestuser		
User Type	user		
Password			
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

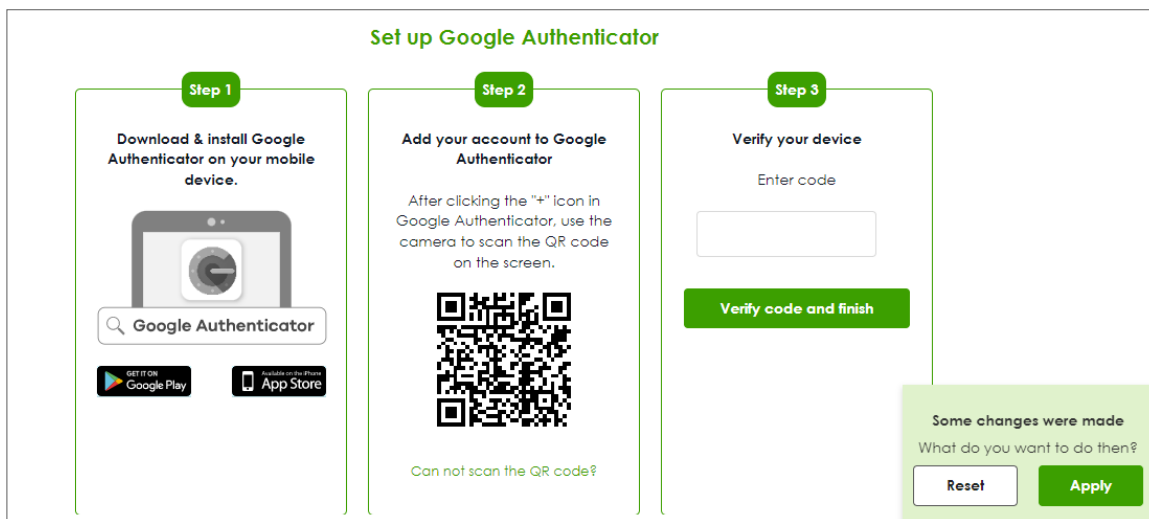
Two-factor Authentication

Enable Two-Factor Authentication for VPN Access ☒

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

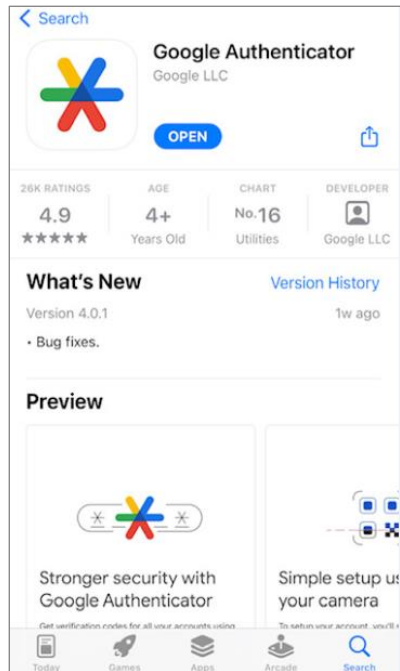


Set up Google Authenticator

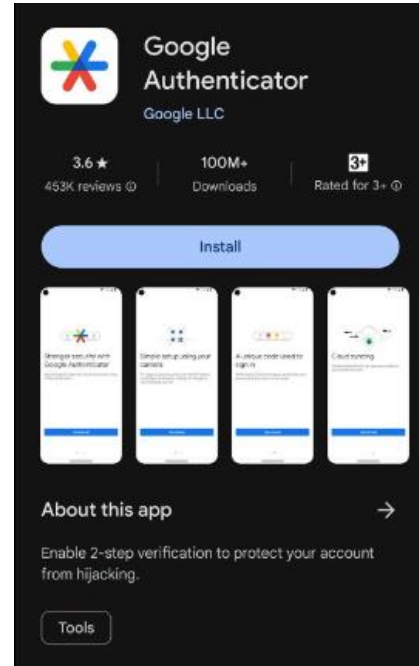


- Download and install Google Authenticator on your mobile device.

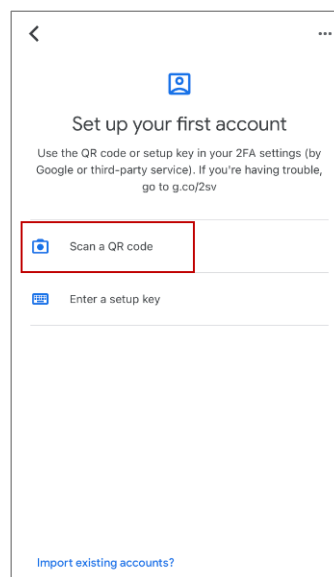
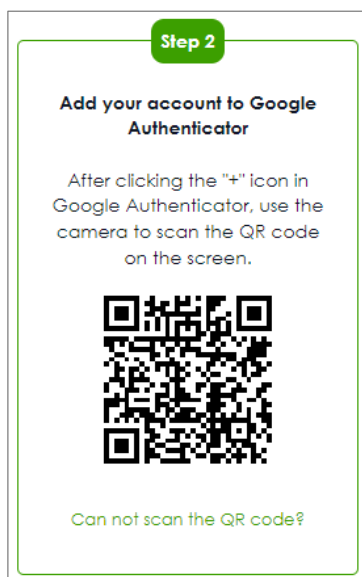
Apple Store



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

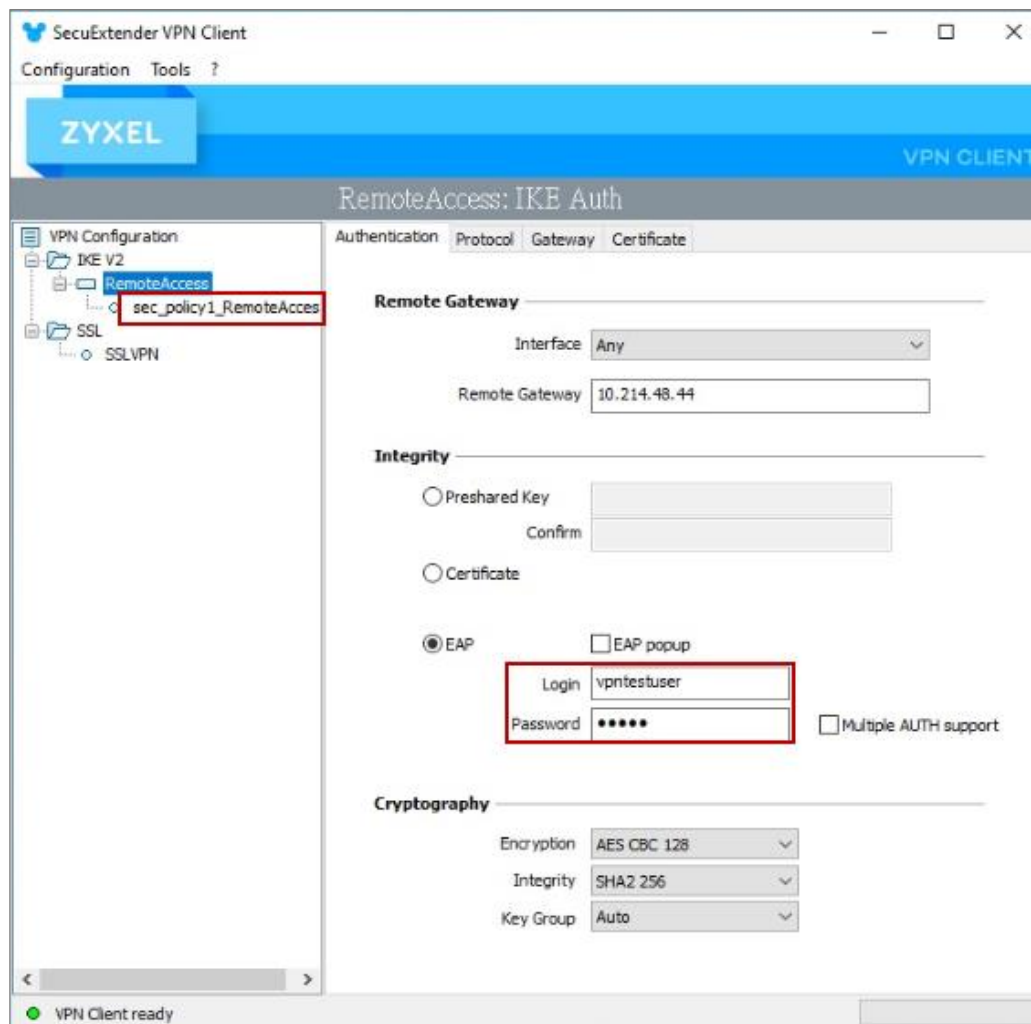
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the 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	☒		
Valid Time	3	(1-5 minutes)	
Two-factor Authentication for Services			
	☐ Web	☐ SSH	
VPN Access			
Enable	☒		
Valid Time	3	(1-5 minutes)	
Two-factor Authentication for Services			
	☒ SSL VPN Access	☒ IPSec VPN Access	
Delivery Settings			
Authorize Link URL Address	HTTPS	From Interface	ge3
Authorized Port	8008	(1-65535)	

Test the Result

Remote Access VPN (IKEv2)

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



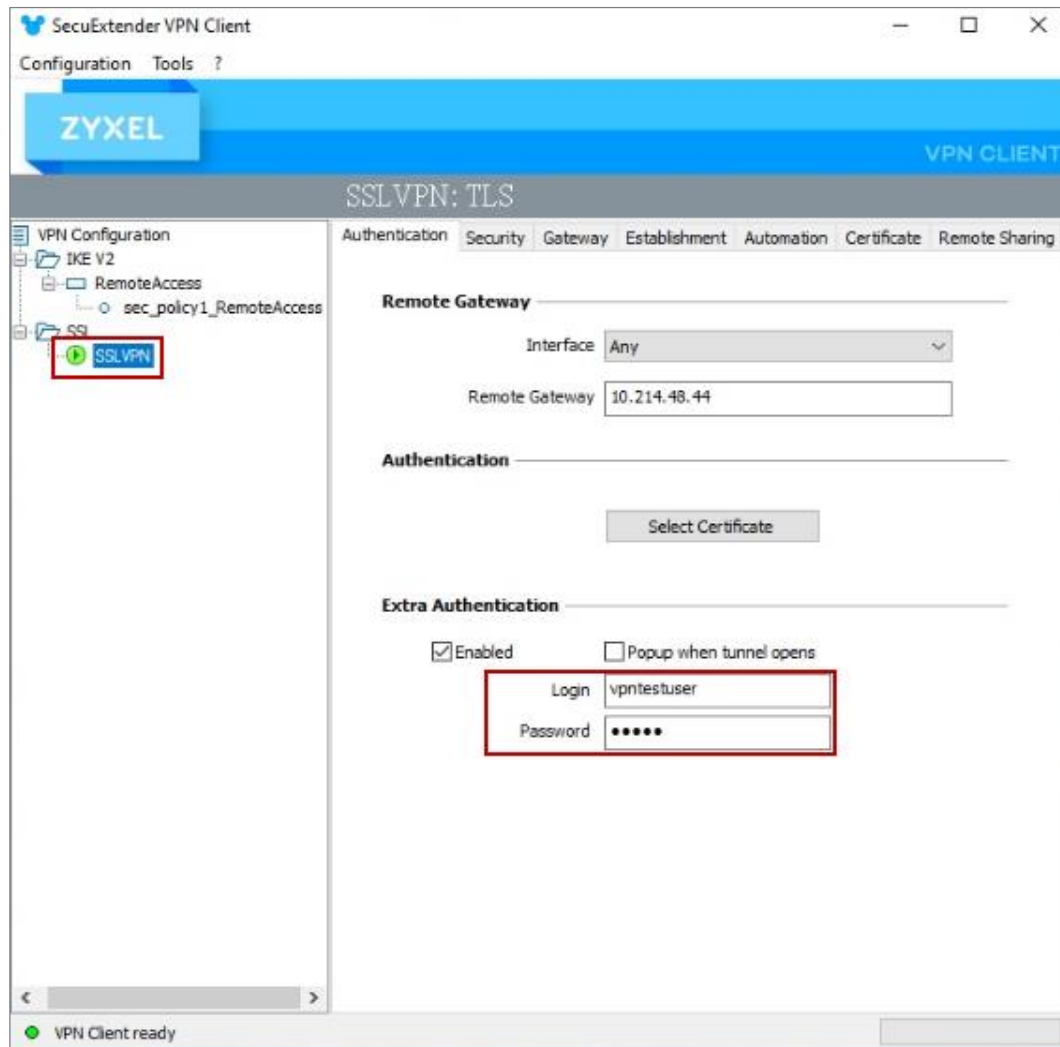
- The browser will pop up authentication page to enter the verification code. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.

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

#	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.

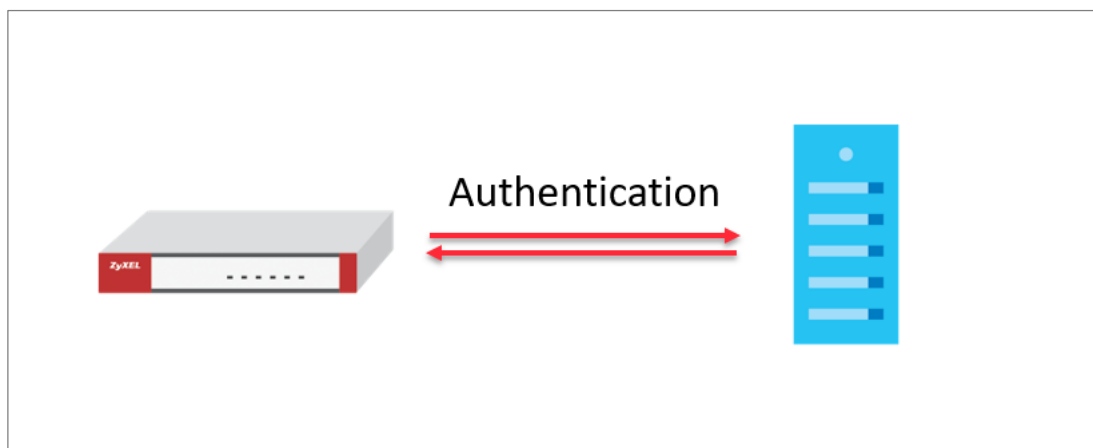
Two-factor Authentication

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

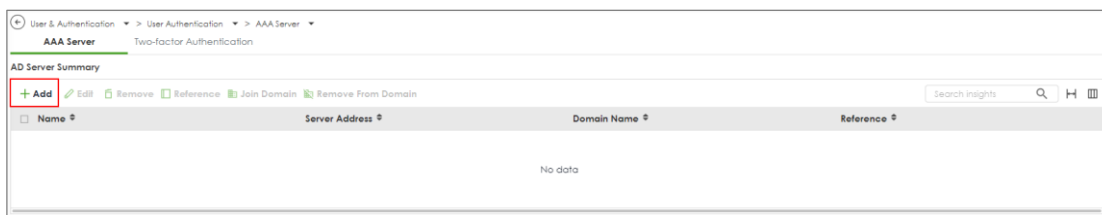
How to set up AD authentication with Microsoft AD

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.

The screenshot shows the 'Configuration' page for the 'Microsoft_AD' profile. The left sidebar contains navigation options like Dashboard, Traffic Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Services, User & Authentication, System, Log & Report, and Maintenance. The main configuration area includes the following sections:

- Configuration:** Name (Microsoft_AD), Description (Optional).
- Server Settings:** Server Address (10.214.48.XX), Backup Server Address (Optional), Port (389), Use SSL (unchecked), Search time limit (5), Case-sensitive User Names (checked).
- Server Authentication:** Domain Name (cso.com), User Name (Administrator), Password (masked), Retype to Confirm (masked).
- Advanced Settings:** Configuration Validation section with a message: 'Please enter an existing user account in this server to validate the above settings.' and a 'Test' button.

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
☐ 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	
☒ 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	
☒ 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	Reference
☐ Microsoft_AD	10.214.48.20	cso.com	☒	1

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	cs0.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

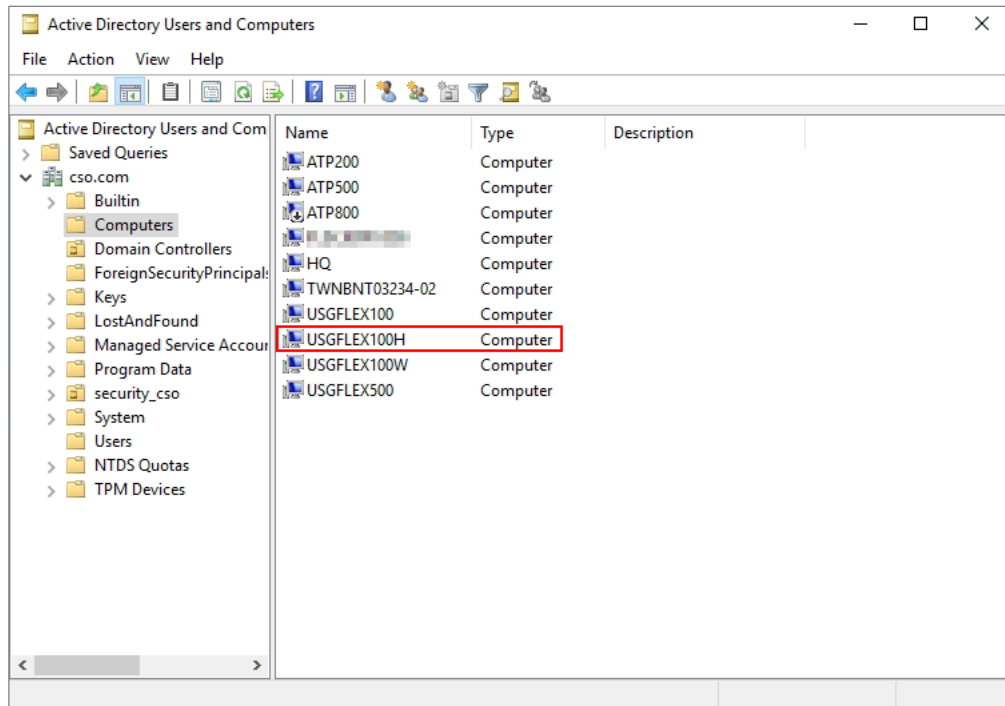
OK

Returned User Attributes

```

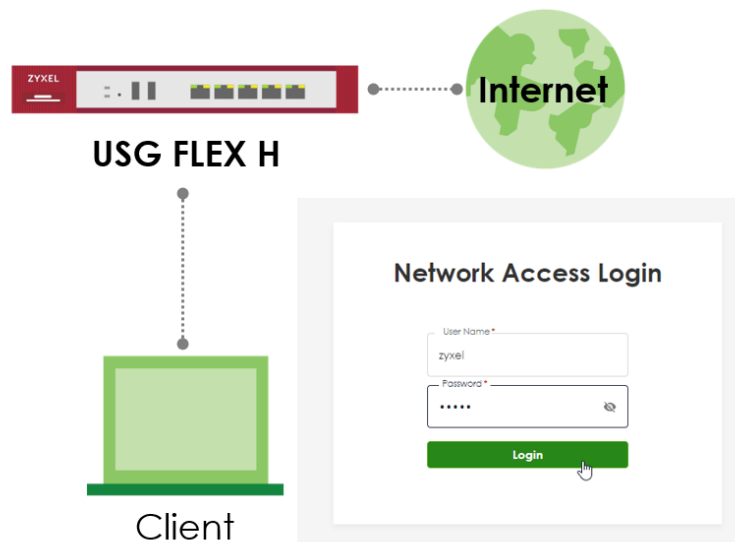
dn: CN=stanley,CN=Users,DC=cs0,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: Stanley
distinguishedName: CN=stanley,CN=Users,DC=cs0,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: Stanley
    
```

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



How to Set Up Captive Portal?

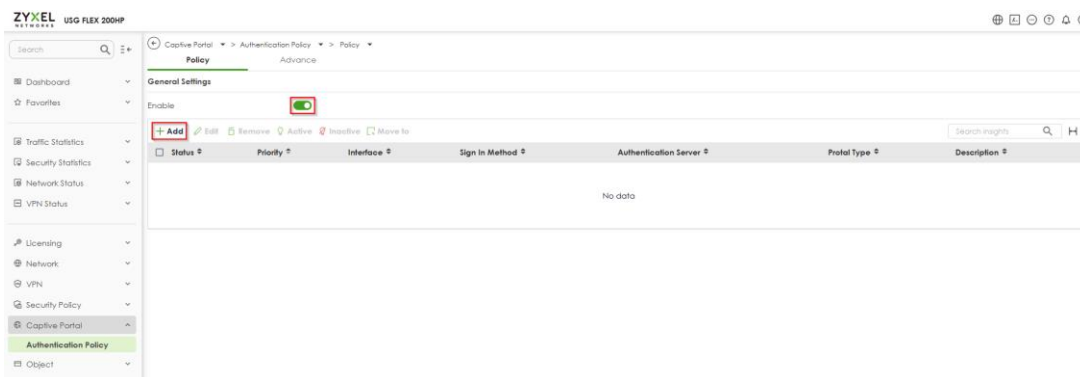
The Captive Portal feature provides functionality that requires LAN client users to complete the authentication procedure of Network Access Login page before accessing the internet. This article will guide users on how to set up and verify this feature.



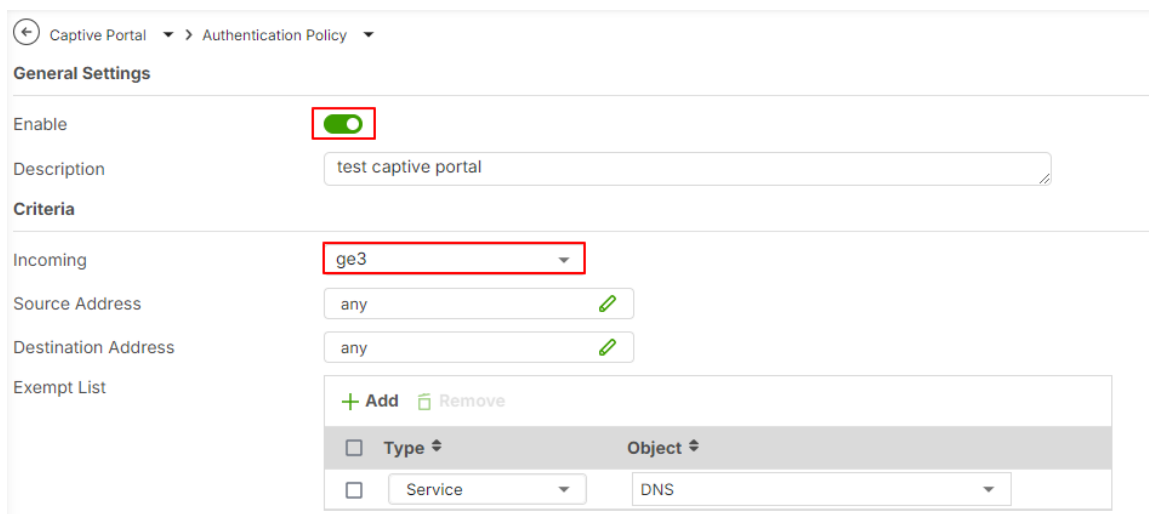
 Note: Captive Portal is supported on USG Flex 100H, USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.32).

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, Advanced Settings and enable Log.



Enable Walled Garden ☐

Walled Garden List

☐ Type	Object
No data	

Sign-in Method

☐ Click-to-continue
Users must view and agree the captive portal page in order to access the network

☒ Sign-on With Local

Users must enter a username and password in order to access the network

Portal Type

☒ Internal Default

☐ External

URL

In this example, users will be redirected to the Promotion URL after logging in.

Advanced Settings ^

After the Captive Portal Page Where the User Should Go? ☐ Stay on Captive Portal Authenticated Successfully Page

☐ Stay on Login Session Page

☒ To Promotion URL: https://www.zyxel.com

Redirect TCP Port 443 Traffic to Login Page ☒

Idle Timeout ☐

Log log

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

← Captive Portal > > Authentication Policy > > Policy >

Policy Advance

General Settings

Enable ☒

+ Add Edit Remove Active Inactive Move to

Search insights

☐ Status	Pri.	Incoming	Source	Destination	Sign-in Method	Sign-on With	Portal Type	Description
☐ Active	1	ge3	any	any	sign-on	local	internal	test 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.

ZYXEL USG FLEX 200HP

Search []

Dashboard, Favorites, Traffic Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, **Captive Portal**, Authentication Policy, Object

Captive Portal > Authentication Policy > Advance

Advance

General Settings

Server Address	6.6.6.6
Redirect FQDN	
HTTP	Enable
HTTP Port	1080
Redirect HTTPS	Enable
HTTPS	Enable
HTTPS Port	1443
Authenticate Client Certificates	Disable
Server Certificate	default

Verify the Captive Portal function

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

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

Welcome

Username/Email

Password:

Login

Powered by **ZYXEL**

5. Enter the login User Name and Password.

Welcome

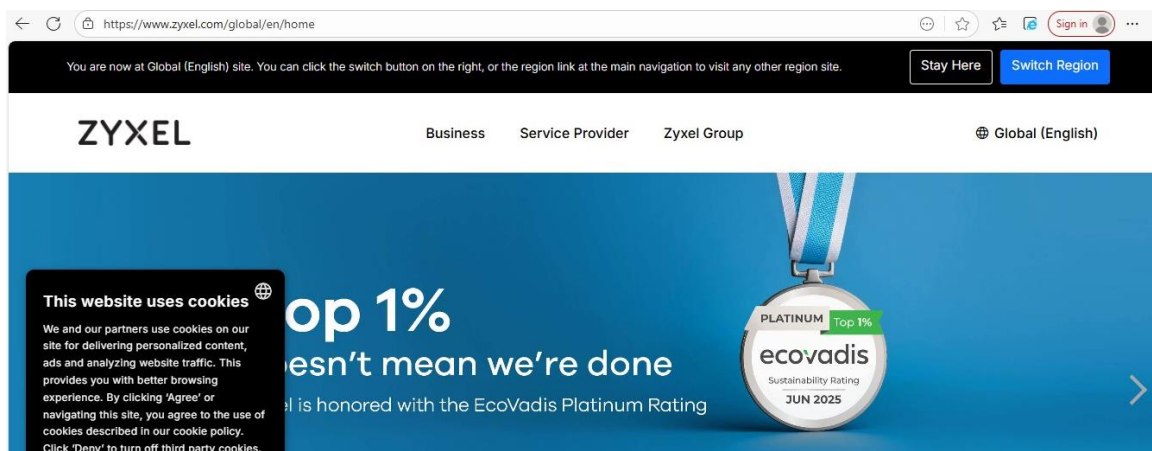
Username/Email

Password:

Login

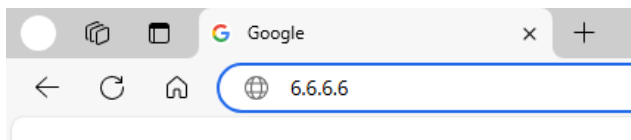
Powered by **ZYXEL**

6. Once successfully logged into the Network Access Login page, the client will be redirected to the URL configured in "To Promotion URL". The client can access the Internet successfully.



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".

Welcome!

You have successfully connected to the network. Here are your connection details:

IP address: 192.168.168.33

Lease Remaining Time: 23:57:25 

Access Timeout: 23:57:25

☐ Updating lease time automatically

[Logout](#)

Powered by **ZYXEL**

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.

Welcome

Username/Email

Password:

[Login](#)

Powered by **ZYXEL**

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

Search

Dashboard
Favorites
Traffic Statistics
Security Statistics
Network Status
Interface
Device Insight
Login Users
DHCP Table
VPN Status

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	23:58:37	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 APC AP

Category All Log Clear Log Export Refresh

#	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 APC AP

Category User Clear Log Export Refresh

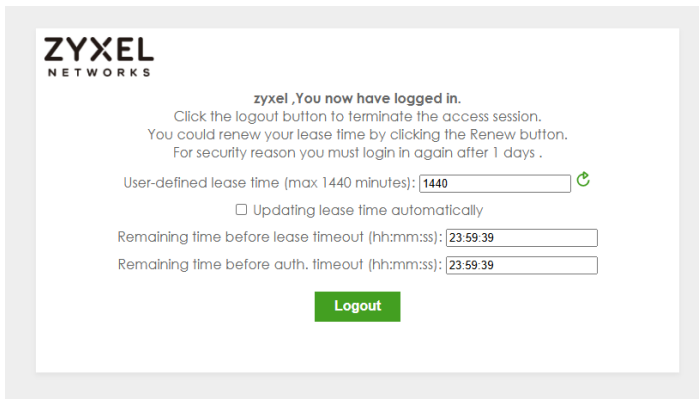
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
59	2025-03-17 14:13:34	User	User zyxel from captive portal has logged out Device	192.168.168.35	192.168.168.1	0	Account: zyxel

Feature Change:

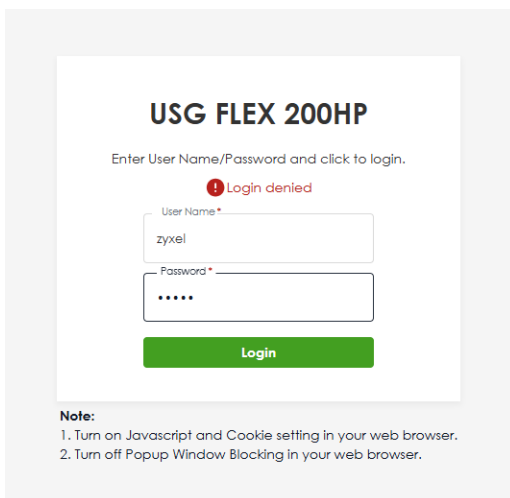


Starting from firmware version uOS 1.32, the user must log in to the Captive Portal before using the User Aware function for security policy or BWM policy utilization.

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.

Welcome

Username/Email

zyxel

Password:

• • • • •

Login

Powered by **ZYXEL**

Welcome

Success!

Powered by **ZYXEL**

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 ☒

Status	Pri.	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Hits	Profile
☒	1	For_The_User	LAN	any (Excluding ZyWALL)	any	any	any	zyxel	none	allow	no	3	

Network > BWM

General Settings

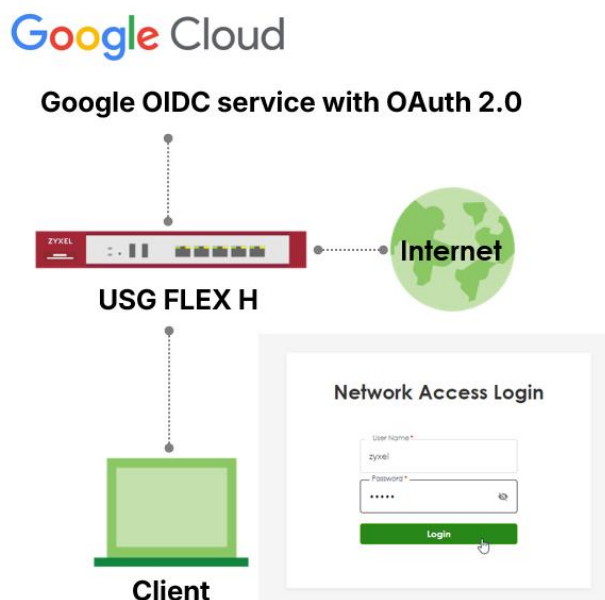
Enable ☒

Configuration

Status	Pri.	Name	Description	User	Incoming Interface	Outgoing Interface	Source	Destination	Service	BWM Download/Upload/Pri
☒	1	For_The_User		zyxel	ge3	ge1	any	any	any	0/0/4

Captive Portal authentication with Google

This article describes how to configure Captive Portal authentication on the USG FLEX H series using Google (OIDC). It covers application registration in Google Workspace/Cloud and the required firewall settings to enable OIDC-based authentication, allowing users to sign in with their existing Google accounts instead of local credentials.



Before You Begin

Before you begin, make sure you have:

- Application Administrator role in your Google Workspace/Cloud
- USG FLEX H Series firewall (Firmware in uOS1.37 or later)
- Valid licenses for your identity provider (Google Workspace/Cloud)
- Network connectivity between your device and Google Workspace/Cloud
- DNS and HTTPS access for the firewall
- SSL certificates properly configured
 - **FQDN1** for **OIDC redirect address** (resolve to your WAN IP)
 - **FQDN2** for **Captive portal Server** (resolve to your captive portal server address, default is 6.6.6.6)
 - The **certificate** must be issued by a **trusted CA**
 - The **Common Name (CN)** and **SAN (Subject Alternative Name)** of the certificate that include above 2 FQDNs.

The Captive Portal uses **HTTPS** to protect user authentication traffic and to support redirection to external Identity Providers (IdPs) such as Google Workspace/Cloud.

If the SSL certificate is not trusted or does not match the Captive Portal address, client devices will display browser warnings or may block the authentication flow.

Supported Certificate Types

One of the following certificate types must be used:

- **Public (Commercial) CA–signed certificate**
 - Automatically trusted by most client devices
 - Recommended for guest or BYOD environments
- **Internal CA–signed certificate**
 - The internal CA root certificate must be installed and trusted on all client devices
 - Suitable for managed corporate environments

Self-signed certificates are **not recommended** for Captive Portal authentication.

Certificate Naming Requirements

The SSL certificate must meet the following requirements:

- The **Common Name (CN)** or **Subject Alternative Name (SAN)** must be a **Fully Qualified Domain Name (FQDN)**
- The FQDN must resolve to the **Captive Portal server address**
 - Default Captive Portal address: 6.6.6.6

Example:

- FQDN: portal.company.com
- Certificate CN or SAN: portal.company.com
- DNS resolution: portal.company.com → 6.6.6.6

Uploading the Certificate to the USG FLEX H Series

1. Log in to the USG FLEX H series web interface.
2. Navigate to **System > Certificate**.
3. Import the SSL certificate and private key.
4. Verify that the certificate status is valid.

Import Certificates
×

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

Binary X.509
 PEM (Base-64) encoded X.509
 Binary PKCS#7
 PEM (Base-64) encoded PKCS#7
 Binary PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.

File Path

Password (PKCS#12 only)

Browse...
Upload

Assigning the Certificate to Captive Portal

1. Go to **Captive Portal > Authentication Policy > Settings**.
2. Locate the **HTTPS / Server Certificate** settings.
3. Select the imported certificate.
4. Apply the configuration.

The screenshot shows the 'Settings' tab of the Captive Portal configuration. Under 'Server Settings', the following options are visible:

- Server Address:** 6.6.6.6
- Redirect FQDN:** portal.company.com
- HTTP:** Enabled (toggle on), HTTP Port: 1080
- Redirect HTTPS:** Disabled (toggle off)
- HTTPS:** Enabled (toggle on), HTTPS Port: 1443
- Authenticate Client Certificates:** Disabled (toggle off)
- Server Certificate:** portal.company.com (dropdown menu)

Authentication Proxy

Navigate to **User & Authentication > User Authentication > Advanced**.

To prevent certificate warnings during the authentication phase, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve to the WAN IP of your firewall.

← User & Authentication > User Authentication > Advanced >

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

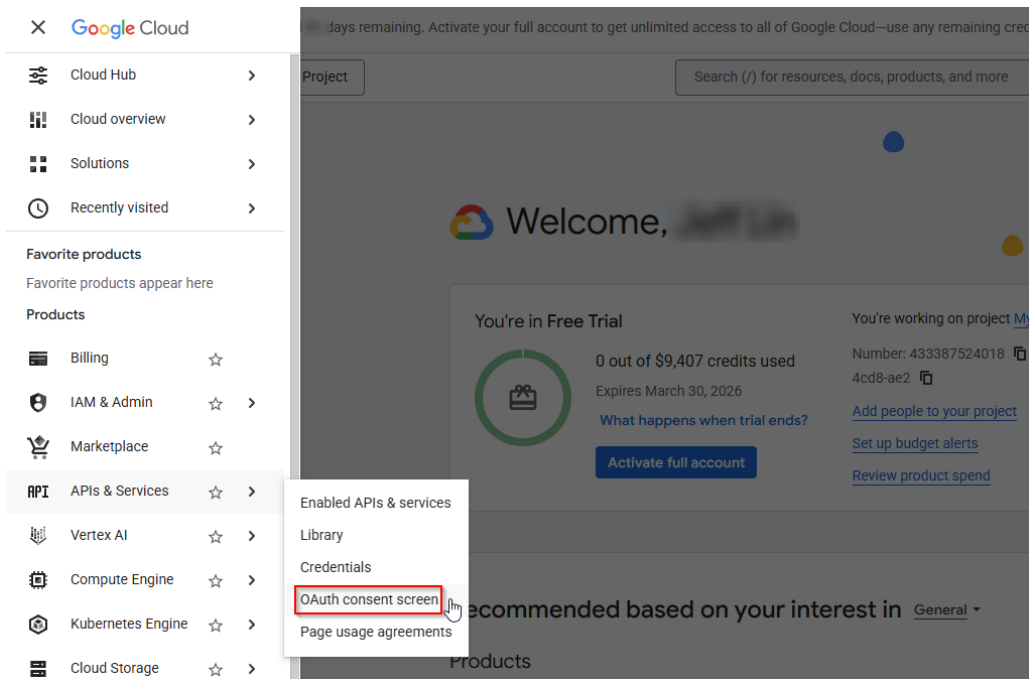
HTTPS Port

Server Certificate

 Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

Google Workspace/Cloud

Go to Google Cloud Console > APIs & Services > OAuth consent screen.



The screenshot shows the Google Cloud Console interface. On the left is a navigation menu with categories like 'Cloud Hub', 'Cloud overview', 'Solutions', and 'Recently visited'. Under 'Favorite products', there is a list of products including 'Billing', 'IAM & Admin', 'Marketplace', 'APIs & Services', 'Vertex AI', 'Compute Engine', 'Kubernetes Engine', and 'Cloud Storage'. The 'APIs & Services' item is selected, and a dropdown menu is open, showing options: 'Enabled APIs & services', 'Library', 'Credentials', 'OAuth consent screen', and 'Page usage agreements'. The 'OAuth consent screen' option is highlighted with a red box. The main content area shows a 'Welcome' message and a 'You're in Free Trial' notification.

Follow the setup wizard to enter your application details. Create a project name.

Google Auth Platform / Overview / Create branding

Overview

- Branding
- Audience
- Clients
- Data Access
- Verification Center
- Settings

Project configuration

1 App Information

App name *
OIDC
The name of the app asking for consent

User support email *
[redacted]@gmail.com
For users to contact you with questions about their consent. [Learn more](#)

Next

2 Audience

3 Contact Information

4 Finish

Create Cancel

The Audience is set to Internal to restrict API access exclusively to authorized workshop participants and ensure environment isolation.

Google Auth Platform / Overview / Create branding

Overview

Branding

Audience

Clients

Data Access

Verification Center

Project configuration

1 App Information

2 Audience

☒ Internal ?

Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☐ External ?

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

Next

 Note: For External Type, to maintain strict access control, you must restrict login permissions under the Audience > Test Users section. Only Google accounts manually added to this whitelist will be authorized to access the application.

Enter Contact Information and Create.

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

✓ App Information

✓ Audience

3 Contact Information

Email addresses *

1@gmail.com

These email addresses are for Google to notify you about any changes to your project.

Next

4 Finish

Create

Cancel

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

✓ App Information

✓ Audience

✓ Contact Information

✓ Finish

Create

Cancel

Continue with the setup wizard to create your OAuth client.

Select Application type as "Web application". Assign a recognizable name to your client.

Configure OIDC on USG FLEX H Series

1. Login to the USG FLEX H
2. Go to **User & Authentication > User Authentication > Advanced**
 - (1) **Enable** the Authentication Proxy
 - (2) Sec the **HTTPS Port** to **1003**
 - (3) Select the **Server Certificate**

← User & Authentication > User Authentication > Advanced

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

HTTPS Port

Server Certificate

Overview your OAuth Client IDs, you need to copy "Client ID", "Client secret" for Firewall setup.

Google Auth Platform / Clients / Client: esub2oagv05a8c0d39u91vjdne956tf8.apps.googleusercontent.com

← Client ID for Web application Delete

Name *
Captive-Portal
The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins For use with requests from a browser
[+ Add URI](#)

Authorized redirect URIs For use with requests from a web server
[+ Add URI](#)

Note: It may take 5 minutes to a few hours for settings to take effect.

[Save](#) [Cancel](#)

Additional information

Client ID

Creation date December 29, 2025, 4:53:52 PM GMT+8

Last used date December 29, 2025 (Note: this data could be delayed by a day or more.)

Inactive OAuth clients are subject to deletion if they are not used for 6 months. You will be notified of deletion due to inactivity, and can restore clients up to 30 days after deletion. [Learn more](#)

Client secrets
If you are in the process of changing client secrets, you can manually rotate them without downtime. [Learn more](#)

Starting in November 2025, viewing and downloading client secrets will no longer be available. If you have lost the secret below, please add a new one. Remember to store client secrets securely and treat them with extreme care. Secrets should never be checked into code repositories. [Learn more](#)

Client secret [Download](#)

Creation date December 29, 2025, 4:53:52 PM GMT+8

Status Enabled

[+ Add secret](#)

Navigate to User & Authentication > User Authentication > AAA Server. Add OIDC Server

OIDC Server

[+ Add](#) [Edit](#) [Remove](#) [Reference](#)

Fill in Server details

Issuer URL: https://accounts.google.com

Client ID: {Client ID}

Client Secret: {Client Secret}

Redirect Address: {FQDN}



Note: The hostname of the redirect URI should be a FQDN. And the FQDN should match the certificate settings of Authentication proxy on your firewall.

Copy the following "Redirect URL" back to Google OAuth 2.0 Client IDs and paste in Authorized redirect URLs

← User & Authentication > User Authentication > AAA Server >

Configuration

Name:

Description: (Optional)

Server Settings

Issuer URL:

Client ID:

Client Secret:

Redirect Address: (IP or FQDN)

Redirect URI: 

Advanced Settings

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

Google Auth Platform / Clients / Client:

← Client ID for Web application 

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Name *
Captive-Portal

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

 The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains [Learn more](#)

Authorized JavaScript origins 

For use with requests from a browser

[+ Add URI](#)

Authorized redirect URIs 

For use with requests from a web server

URIs 1 *
 

[+ Add URI](#)

Note: It may take 5 minutes to a few hours for settings to take effect

[Save](#) [Cancel](#)

Additional information

Client ID
eaub2oagv05a8c0d39u91vjd6956tf8.apps.googleusercontent.com

Creation date
December 29, 2025, 4:53:52 PM GMT+8

Last used date
December 29, 2025 (Note: this data could be delayed by a day or more.)

 Inactive OAuth clients are subject to deletion if they are not used for 6 months. You will be notified of deletion due to inactivity, and can restore clients up to 30 days after deletion. [Learn more](#)

Client secrets

If you are in the process of changing client secrets, you can manually rotate them without downtime. [Learn more](#)

 Starting in November 2025, viewing and downloading client secrets will no longer be available. If you have lost the secret below, please add a new one. Remember to store client secrets securely and treat them with extreme care. Secrets should never be checked into code repositories. [Learn more](#)

Client secret ****s06h  

Creation date
December 29, 2025, 4:53:52 PM GMT+8

Status
Enabled

[+ Add secret](#)

Go back to the USG FLEX H, OIDC Server page, at **Configuration Validation** and click **Test**.

← User & Authentication > > User Authentication > > AAA Server >

Configuration

Name: **Google**

Description: (Optional)

Server Settings

Issuer URL:

Client ID:

Client Secret:

Redirect Address: (IP or FQDN)

Redirect URI:

Advanced Settings ▾

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

You should see "OIDC Authentication Successful."

OIDC Authentication Test

OIDC Authentication Successful (Verified)

Username: [redacted]@gmail.com
 user_attr_name: email
 state: t_ce13fddfacae4fd97192f748b1a32077

ID Token Claims

- iss: https://accounts.google.com
- azp: [redacted]oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- aud: [redacted]oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- sub: [redacted]10187679099756
- email: [redacted]@gmail.com
- email_verified: True
- at_hash: [redacted]fmGGTZYWh0w
- nonce: 513b49252a78755197b3516dc28c767e
- iat: 1767070662
- exp: 1767074262

Note: The **Advanced Settings** at USG FLEX H GUI are **optional**.

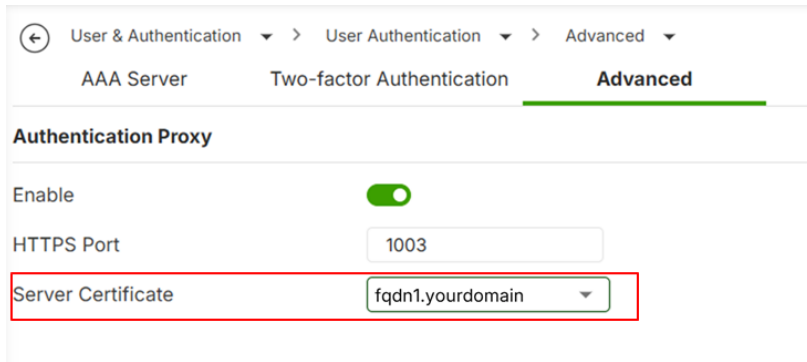
- **Additional Scope:** Specifies additional scopes to include in the OIDC authentication request. To request multiple scopes, separate them with spaces. The recommended value is **email**.
- **Login Name Attribute:** Set user-attr-name field for login username. The recommended value is **email**.

Configure Portal Service Settings on USG FLEX H Series

To ensure a smooth and secure Captive Portal authentication experience, proper certificate and DNS preparation is required before configuring OIDC authentication.

1. Configure the Certificate of the OIDC Server

- (1) Go to **User & Authentication > User Authentication > Advanced**.
- (2) Select the **Server Certificate** that you prepared (FQDN1).



The screenshot shows the configuration page for 'User Authentication > Advanced'. Under the 'Authentication Proxy' section, the 'Enable' toggle is turned on. The 'HTTPS Port' is set to 1003. The 'Server Certificate' dropdown menu is highlighted with a red box and shows 'fqdn1.yourdomain' as the selected option.



Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

2. Configure the Certificate of the Captive Portal Server

- (1) Go to **Captive Portal > Authentication Policy > Settings**
- (2) Set the **Redirect FQDN**
- (3) Select **Server Certificate** that you prepared (FQDN2)

← Captive Portal > Authentication Policy > Settings >

Policy **Settings**

Server Settings

Server Address 6.6.6.6

Redirect FQDN fqdn2.yourdomain

HTTP Enable ☒

HTTP Port 1080

Redirect HTTPS ☐

HTTPS Enable ☒

HTTPS Port 1443

Authenticate Client Certificates ☐

Server Certificate fqdn2.yourdomain

3. **Configure DNS Records** for Captive Portal Access

Captive Portal authentication requires:

- A dedicated **FQDN** for the Captive Portal
- DNS resolution of the FQDN to the Captive Portal server address
- Default address: 6.6.6.6

Client devices must be able to resolve this FQDN **before authentication**.

Scenario 1: Client DNS Points to an Internal DNS Server

If client devices use an internal DNS server (for example, Active Directory DNS), create a **static DNS record** that resolves the Captive Portal FQDN to the Captive Portal server address (default is 6.6.6.6).

Scenario 2: Client DNS Points to the USG FLEX H Series

If client devices use the USG FLEX H series as their DNS server, configure a static DNS entry using the firewall's built-in DNS feature.

Edit as following:

- (1). Go to **System > DNS & DDNS > DNS**
- (2). Add an **Address Record**
- (3). Leave the Hostname empty
- (4). Select or +Add a **Domain** fqdn2.yourdomain
- (5). Fill-in **IP address** in 6.6.6.6
- (6). Click **Apply**

The screenshot shows the ZyXel web interface for DNS configuration. The breadcrumb trail is 'System > DNS & DDNS > DNS'. The 'DNS' tab is selected, and the 'Address Record' section is active. Below the 'Address Record' header, there are '+ Add' and 'Remove' buttons. A table with three columns: 'Hostname', 'Domain', and 'IP Address' is shown. The first row has an empty 'Hostname' field, 'fqdn2.yourdomain' in the 'Domain' field, and '6.6.6.6' in the 'IP Address' field. Below this table, there are sections for 'CNAME Record', 'MX Record', and 'Domain Zone Forwarder', each with its own '+ Add' and 'Remove' buttons. At the bottom right, a green notification box states 'Some changes were made' and asks 'What do you want to do then?' with 'Cancel' and 'Apply' buttons. The 'Apply' button is highlighted with a red border.

Configure Captive Portal on USG FLEX H Series

1. Go to **Captive Portal > Authentication Policy > Policy**
2. **Add** a Policy and enable and configure the policy criteria details.
3. In the **Walled Garden List**, click **OIDC Providers** and select **Google**.
4. Select **Sign-on With > OIDC** server at **Sign-in Method**.
5. Click **Apply**

Click OIDC Providers and select Google.

Captive Portal > Authentication Policy

General Settings

Enable ☒

Description Google

Criteria

Incoming ge3

Source Address any

Destination Address any

Exempt List

+ Add Remove

☐ Type Object

☐ Service DNS

Enable Walled Garden ☒

Walled Garden List

+ Add **OIDC Providers** Remove

☐ Type **OIDC Providers**

No data

OIDC Providers

☒ Google

☐ Microsoft

Select Sign-on With > OIDC server at Sign-in Method.

+ Add
OIDC Providers
Remove

Type	Object
☐ Domain Name	accounts.google.com
☐ Domain Name	apis.google.com
☐ Domain Name	*.client-channel.google.com
☐ Domain Name	clients*.google.com
☐ Domain Name	contacts.google.com
☐ Domain Name	*.googleusercontent.com
☐ Domain Name	mail.google.com
☐ Domain Name	mail-attachment.google.com
☐ Domain Name	ogs.google.com
☐ Domain Name	play.google.com
☐ Domain Name	ssl.gstatic.com
☐ Domain Name	www.gstatic.com
☐ Domain Name	oauth2.googleapis.com
☐ Domain Name	accounts.google.com.*
☐ Domain Name	fonts.gstatic.com
☐ Domain Name	signaler-pa.googleapis.com

Sign-in Method

☐ Click-to-continue
Users must view and agree the captive portal page in order to access the network

☒ Sign-on With

OIDC /Google

Users must enter a username and password in order to access the network

☒ Internal

Default

☐ External

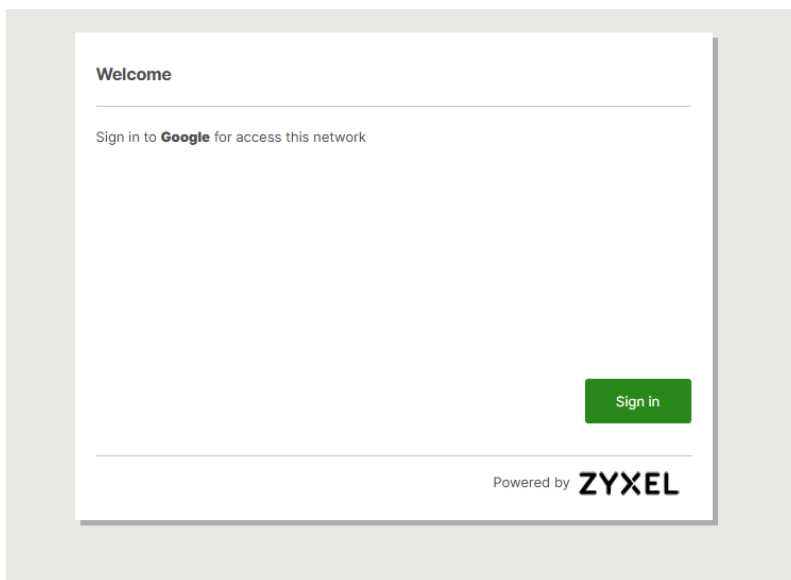
URL

Portal Type

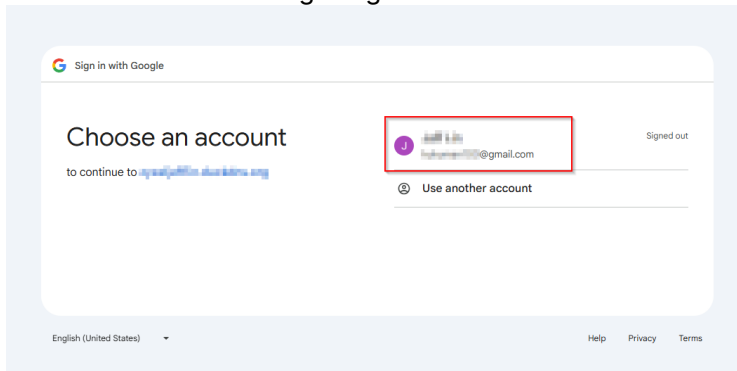
Verification- Test User Login

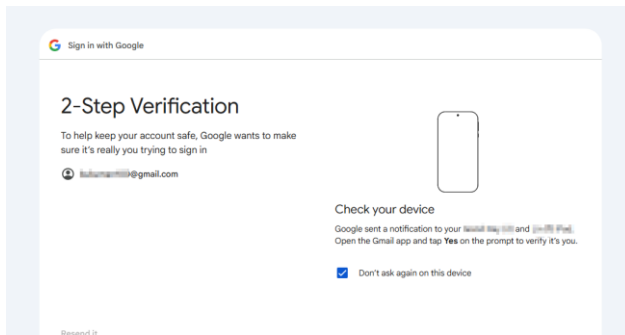
Verify that the Captive Portal correctly redirects unauthenticated users to Google Workspace/Cloud and grants access after successful authentication.

1. Connect a client device
2. Open a browser, display the Captive Portal page, and then click Sign in

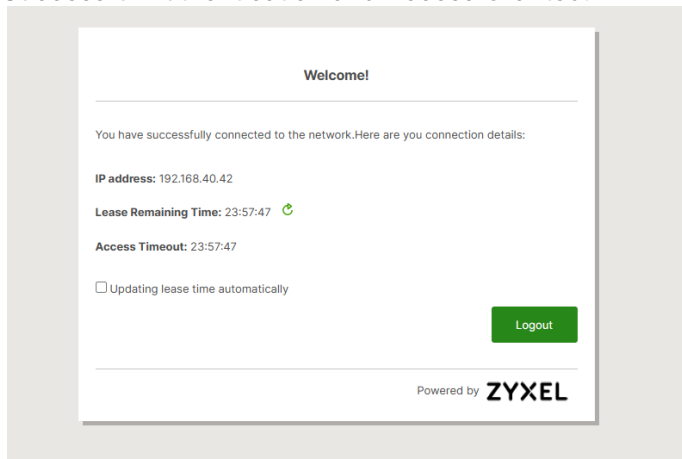


3. Confirm redirect to Google login





4. Successful Authentication and Access Granted.



Internet access is successful.



- Check login user status at **Network Status > Login Users > Login Users**
User shown as authenticated via OIDC

Network Status > Login Users > Login Users

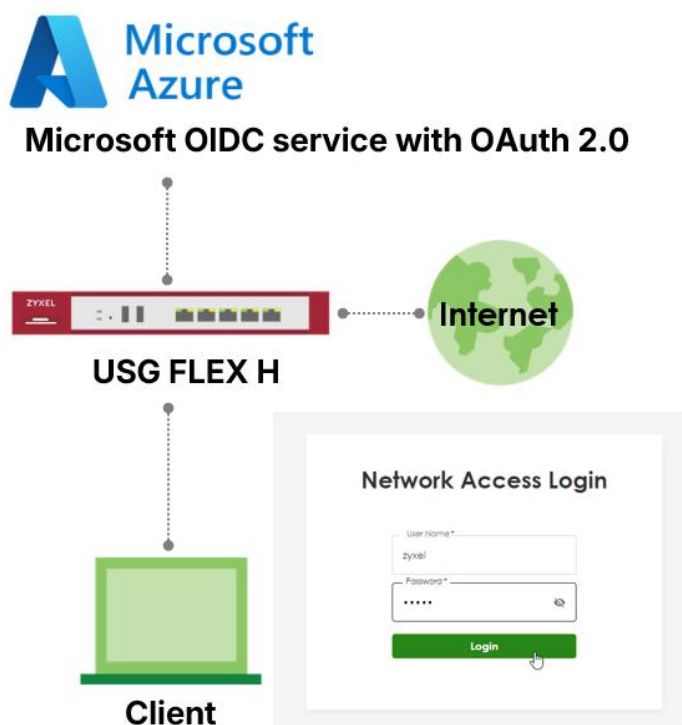
Login Users Lockout IPs

Force Log Out Search Insights

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1			192.168.40.42	0:03:36	captive portal	0.0.0.0	23:56:24	ext-user(oidc-users)
2			192.168.40.42	0:03:36	captive portal	0.0.0.0	23:56:24	ext-user(oidc-users)
3			192.168.40.42	0:03:36	captive portal	0.0.0.0	23:56:24	ext-user(oidc-users)
4	testuser@gmail.com	user	192.168.40.42	0:03:36	captive portal	0.0.0.0	23:56:24	ext-user(oidc-users)

Captive Portal authentication with Microsoft Entra ID

This article describes how to configure Captive Portal authentication on the USG FLEX H series using Microsoft Entra ID (OIDC). It covers application registration in Microsoft Entra ID and the required firewall settings to enable OIDC-based authentication, allowing users to sign in with their existing Microsoft accounts instead of local credentials.



Before You Begin

Before you begin, make sure you have:

- Application Administrator role in your Microsoft Entra ID
- USG FLEX H Series firewall (Firmware in uOS1.37 or later)
- Valid licenses for your identity provider (Microsoft Entra ID)
- Network connectivity between your device and Microsoft Entra ID
- DNS and HTTPS access for the firewall
- SSL certificates properly configured
 - **FQDN1** for **OIDC redirect address** (resolve to your WAN IP)
 - **FQDN2** for **Captive portal Server** (resolve to your captive portal server address, default is 6.6.6.6)
 - The **certificate** must be issued by a **trusted CA**
 - The **Common Name (CN)** and **SAN (Subject Alternative Name)** of the certificate that include above 2 FQDNs.

The Captive Portal uses **HTTPS** to protect user authentication traffic and to support redirection to external Identity Providers (IdPs) such as Microsoft Entra ID.

If the SSL certificate is not trusted or does not match the Captive Portal address, client devices will display browser warnings or may block the authentication flow.

Supported Certificate Types

One of the following certificate types must be used:

- **Public (Commercial) CA-signed certificate**
 - Automatically trusted by most client devices
 - Recommended for guest or BYOD environments
- **Internal CA-signed certificate**
 - The internal CA root certificate must be installed and trusted on all client devices
 - Suitable for managed corporate environments

Self-signed certificates are **not recommended** for Captive Portal authentication.

Certificate Naming Requirements

The SSL certificate must meet the following requirements:

- The **Common Name (CN)** or **Subject Alternative Name (SAN)** must be a **Fully Qualified Domain Name (FQDN)**
- The FQDN must resolve to the **Captive Portal server address**
 - Default Captive Portal address: 6.6.6.6

Example:

- FQDN: portal.company.com
- Certificate CN or SAN: portal.company.com
- DNS resolution: portal.company.com → 6.6.6.6

Uploading the Certificate to the USG FLEX H Series

5. Log in to the USG FLEX H series web interface.
6. Navigate to **System > Certificate**.
7. Import the SSL certificate and private key.
8. Verify that the certificate status is valid.

Import Certificates

×

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

Binary X.509
 PEM (Base-64) encoded X.509
 Binary PKCS#7
 PEM (Base-64) encoded PKCS#7
 Binary PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.

File Path

Browse...

Upload

Password

(PKCS#12 only)

Assigning the Certificate to Captive Portal

5. Go to **Captive Portal > Authentication Policy > Settings**.
6. Locate the **HTTPS / Server Certificate** settings.
7. Select the imported certificate.
8. Apply the configuration.

The screenshot shows the 'Settings' tab of the Captive Portal configuration. The 'Server Settings' section is active. The configuration includes:

- Server Address:** 6.6.6.6
- Redirect FQDN:** portal.company.com
- HTTP:** Enabled (toggle on), HTTP Port: 1080
- Redirect HTTPS:** Disabled (toggle off)
- HTTPS:** Enabled (toggle on), HTTPS Port: 1443
- Authenticate Client Certificates:** Disabled (toggle off)
- Server Certificate:** portal.company.com (dropdown menu)

Authentication Proxy

Navigate to **User & Authentication > User Authentication > Advanced**.

To prevent certificate warnings during the authentication, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve to the WAN IP of your firewall.

← User & Authentication > User Authentication > Advanced >

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

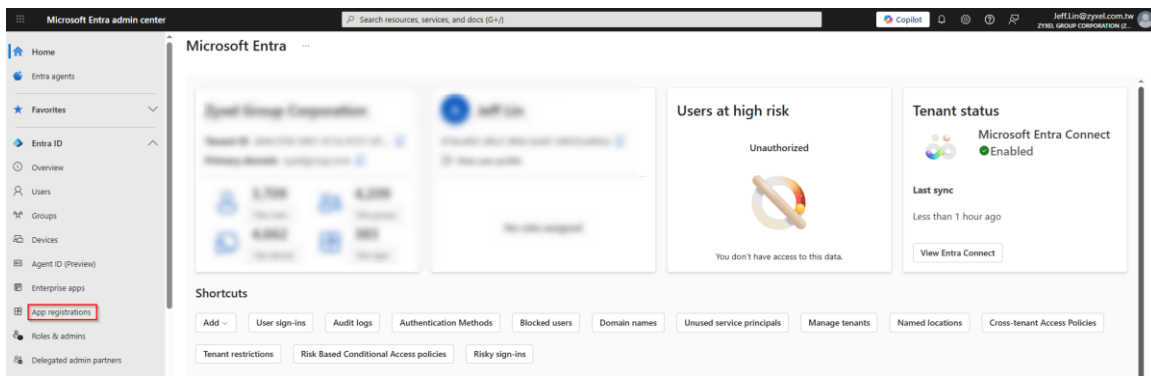
HTTPS Port

Server Certificate

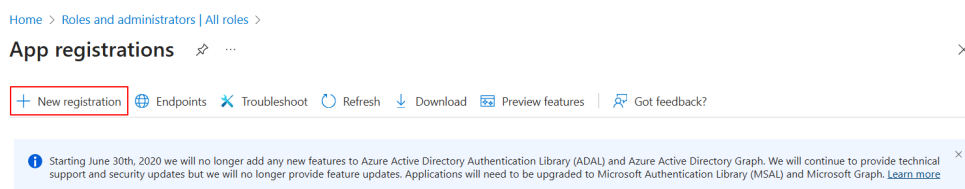
 **Note:** Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

Microsoft Entra ID

Navigate to Entra ID Portal > App registrations > New registration.



Select **+New registration** in the top menu.



On the Register an application page, provide the following information:

Enter a descriptive name for your application, such as Captive-Portal.

Under **Supported account types**, select which Microsoft account types should have access to USG FLEX H.

Select **Accounts in this organizational directory only (Default directory only - Single tenant)**.

[Home](#) > [App registrations](#) >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Captive-Portal

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

1. Under **Redirect URI (optional)**, in the **Select a platform** list, select **Web**.

You don't need to specify a URL in the next field.

2. Click **Register**.

Microsoft Entra Portal shows the details of the application you created.

3. **Note** the following details:

- **Application (client) ID**
- **Directory (tenant) ID**

You must enter these details when adding a Microsoft Entra ID server to the firewall (USG FLEX H).

[Home](#) > [App registrations](#) > [Captive-Portal | Token configuration](#) > [App registrations](#) >

Captive-Portal ...

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Captive-Portal

Application (client) ID : 00000000-0000-0000-0000-000000000000

Object ID : 00000000-0000-0000-0000-000000000000

Directory (tenant) ID : 00000000-0000-0000-0000-000000000000

Supported account types : My organization only

Client credentials : 0 certificate_1_secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in L... : Captive-Portal

Navigate to Manage > Certificate & secret > New client secret.

Home > App registrations > Captive-Portal

Captive-Portal | Certificates & secrets

Search Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** 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
No client secrets have been created for this application.			

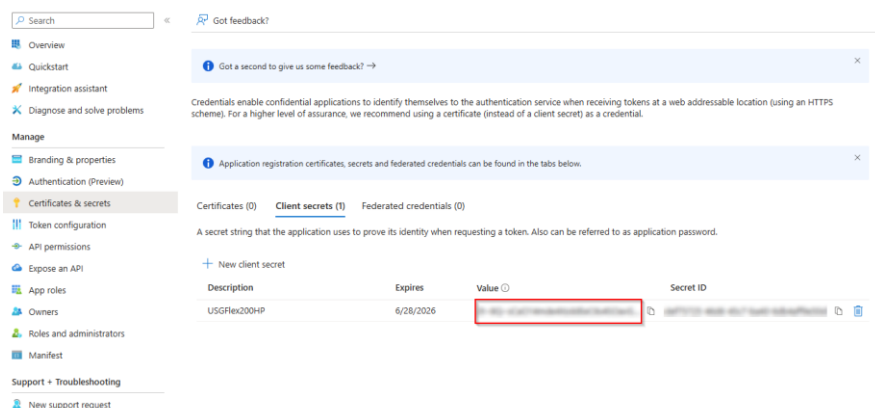
Add a client secret

Description

Expires

Add

Create a secret and copy the Secret Value immediately. You will need this for the Firewall setup.



Search Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage
Branding & properties
Authentication (Preview)
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request

Got a second to give us some feedback? →

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)

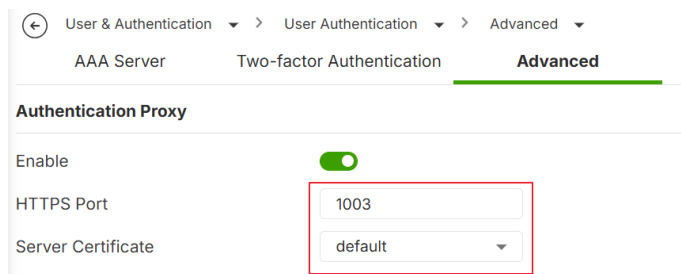
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
USGFlex200HP	6/28/2026	USGFlex200HP	

Configure OIDC on USG FLEX H Series

3. Login to the USG FLEX H
4. Go to **User & Authentication > User Authentication > Advanced**
 - (1) **Enable** the Authentication Proxy
 - (2) Set the **HTTPS Port** to **1003**
 - (3) Select the **Server Certificate**



User & Authentication > User Authentication > Advanced

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

HTTPS Port

Server Certificate

Overview your Entra App, you need to copy "Client ID", "Tenant ID" for Firewall setup.

Home > App registrations > Captive-Portal | Token configuration > App registrations >

Captive-Portal ✕ ...

Search < Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: Captive-Portal	Client credentials	: 0 certificate_1 secret
Application (client) ID	: [REDACTED]	Redirect URIs	: Add a Redirect URI
Object ID	: [REDACTED]	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: [REDACTED]	Managed application in L...	: Captive-Portal

Supported account types : My organization only

Navigate to User & Authentication > User Authentication > AAA Server. Add OIDC Server

OIDC Server ⓘ

+ Add Edit Remove Reference

Search insights 🔍

Fill in Server details

Issuer URL: https://login.microsoftonline.com/{Tenant ID}/v2.0

Client ID: {Client ID}

Client Secret: {You already have Secret at "Manage > Certificate & secrets"}

Redirect Address: {FQDN}



Note: The hostname of the redirect URI should be a FQDN. And the FQDN should match the certificate settings of Authentication proxy on your firewall.

← User & Authentication > User Authentication > AAA Server >

Configuration

Name: MS

Description: (Optional)

Server Settings

Issuer URL: https://login.microsoftonline.com/.../v2.0

Client ID: ...

Client Secret:

Redirect Address: zyxeltest.com (IP or FQDN)

Redirect URI: https://zyxeltest.com:1003/oauth2/callback

Copy the above "Redirect URL" and back to Entra Portal Overview > Add a Redirect URI > Add a platform > Web. Go to the application you created for the firewall, and under **Essentials** > **Redirect URIs**, click **Add a Redirect URI**.

^ Essentials

Display name	: Captive-Portal	Client credentials	: 0 certificate_1 secret
Application (client) ID	: ...	Redirect URIs	: Add a Redirect URI
Object ID	: ...	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: ...	Managed application in L...	: Captive-Portal

Supported account types : [My organization only](#)

Copy the above "Redirect URL" and back to Entra Portal Overview > Add a Redirect URI > Add a platform.

Go to **Add a platform > Web**, in **Redirect URIs**, paste the URL (you copied from USG FLEX H GUI) and click **Configure**.

Select a platform to add redirect URI



To understand which platform you should select, please [learn more](#).

Web applications

 **Web**

Build, host, and deploy a web server application. .NET, Java, Python

[Select →](#)

 **Single-page application**

Configure browser client applications and progressive web applications. Javascript.

[Select →](#)

Paste the URL.

Edit Redirect URI



Web platform



Quickstart



Docs

Redirect URI

✓
🗑️

Go back to the USG FLEX H, OIDC Server page, at **Configuration Validation** and Click **Test**.

Configuration

Name **MS**

Description (Optional)

Server Settings

Issuer URL

Client ID

Client Secret

Redirect Address (IP or FQDN)

Redirect URI: https://zyxetest.com:1003/oauth2/callback 🔗

Advanced Settings ▾

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

You should see "OIDC Authentication Successful."

OIDC Authentication Test

OIDC Authentication Successful (Verified)

Username: [REDACTED]@zyxel.com.tw
 user_attr_name: email
 state: t_497e05af708f2dd3395b08d18b186efd

ID Token Claims

- aud: [REDACTED]
- iss: https://login.microsoftonline.com/[REDACTED] v2.0
- iat: 1767087729
- nbf: 1767087729
- exp: 1767091629
- email: [REDACTED]@zyxel.com.tw
- nonce: [REDACTED]35083fad1b10adc815177
- rh: 1 [REDACTED]9feRWmF6OM8ODCn7x1Dh6Vp23TTIU4sAZJUAA.
- sub: [REDACTED]7ha6V6KD7kJgCu2bdoy19HKDg
- tid: [REDACTED]7de456985e8
- uti: r [REDACTED]
- ver: 2.0

Note: The **Advanced Settings** at USG FLEX H GUI are **optional**.

- **Additional Scope:** Specifies additional scopes to include in the OIDC authentication request. To request multiple scopes, separate them with spaces. The recommended value is **email**.
- **Login Name Attribute:** Set user-attr-name field for login username. The recommended value is **email**.

Configure Portal Service Settings on USG FLEX H Series

To ensure a smooth and secure Captive Portal authentication experience, proper certificate and DNS preparation is required before configuring OIDC authentication.

4. Configure the Certificate of the OIDC Server

- (1) Go to **User & Authentication > User Authentication > Advanced**.
- (2) Select the **Server Certificate** that you prepared (FQDN1).

← User & Authentication > User Authentication > Advanced >

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

HTTPS Port

Server Certificate

 Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

5. Configure the Certificate of the Captive Portal Server

- (1) Go to **Captive Portal > Authentication Policy > Settings**
- (2) Set the **Redirect FQDN**
- (3) Select **Server Certificate** that you prepared (FQDN2)

← Captive Portal > Authentication Policy > Settings >

Policy **Settings**

Server Settings

Server Address

Redirect FQDN

HTTP Enable ☒

HTTP Port

Redirect HTTPS ☐

HTTPS Enable ☒

HTTPS Port

Authenticate Client Certificates ☐

Server Certificate

6. Configure DNS Records for Captive Portal Access

Captive Portal authentication requires:

- A dedicated **FQDN** for the Captive Portal
- DNS resolution of the FQDN to the Captive Portal server address
- Default address: 6.6.6.6

Client devices must be able to resolve this FQDN **before authentication**.

Scenario 1: Client DNS Points to an Internal DNS Server

If client devices use an internal DNS server (for example, Active Directory DNS), create a **static DNS record** that resolves the Captive Portal FQDN to the Captive Portal server address (default is 6.6.6.6).

Scenario 2: Client DNS Points to the USG FLEX H Series

If client devices use the USG FLEX H series as their DNS server, configure a static DNS entry using the firewall's built-in DNS feature.

Edit as following:

- (7). Go to **System > DNS & DDNS > DNS**
- (8). Add an **Address Record**
- (9). Leave the Hostname empty
- (10). Select or +Add a **Domain** fqdn2.yourdomain
- (11). Fill-in **IP address** in 6.6.6.6
- (12). Click **Apply**

The screenshot shows the Zyxel web interface for DNS configuration. The breadcrumb trail is System > DNS & DDNS > DNS. The 'DNS' tab is selected. The 'Address Record' section contains a table with columns: Hostname, Domain, and IP Address. A record is added with Domain 'fqdn2.yourdomain' and IP Address '6.6.6.6'. The 'CNAME Record' section is empty with the message 'No data'. The 'MX Record' section is also empty with the message 'No data'. The 'Domain Zone Forwarder' section has columns for Domain, DNS Server, and Query Via. A green notification box at the bottom right states 'Some changes were made' and asks 'What do you want to do then?' with 'Cancel' and 'Apply' buttons.

Configure Captive Portal on USG FLEX H Series

6. Go to **Captive Portal > Authentication Policy > Policy**
 7. **Add** a Policy and enable and configure the policy criteria details.
 8. In the **Walled Garden List**, click **OIDC Providers** and select **Microsoft**.
 9. Select **Sign-on With > OIDC** server at **Sign-in Method**.
 10. Click **Apply**
- Click **OIDC Providers** and select **Microsoft**.

☐ Captive Portal > ☒ Authentication Policy

Enable ☒

Description

Criteria

Incoming

Source Address

Destination Address

Exempt List

☐	Type	Object
☐	Service	DNS

Enable Walled Garden ☒

Walled Garden List

☐	Type	OIDC Providers
No data		

Sign-in Method

☐ Click-to-continue
 Users must view and agree the captive portal page in order to access the network

☒ Sign-on With

 Users must enter a username and password in order to access the network

Portal Type

☒ Internal

☐ External

OIDC Providers

☐ Google

☒ Microsoft

Select Sign-on With > OIDC server at Sign-in Method.

Captive Portal > Authentication Policy

Enable Walled Garden ☒

Walled Garden List

+ Add ☒ OIDC Providers ☐ Remove

Type #	Object #
☐ Domain Name	*aadcdn.msftauth.net
☐ Domain Name	*aadcdn.msftauthimages.net
☐ Domain Name	*aadcdn.msauthimages.net
☐ Domain Name	*logincdn.msftauth.net
☐ Domain Name	*msauth.net
☐ Domain Name	*aadcdn.microsoftonline-p.com
☐ Domain Name	*microsoftonline-p.com
☐ Domain Name	aadcdn.msftauth.net
☐ Domain Name	aadcdn.msftauthimages.net
☐ Domain Name	aadcdn.msauthimages.net
☐ Domain Name	logincdn.msftauth.net
☐ Domain Name	msauth.net
☐ Domain Name	aadcdn.microsoftonline-p.com
☐ Domain Name	microsoftonline-p.com
☐ Domain Name	login.microsoftonline.com
☐ Domain Name	login.live.com
☐ Domain Name	autologon.microsoftazuread-ssso.com
☐ Domain Name	graph.microsoft.com
☐ Domain Name	login.microsoft.com
☐ Domain Name	sts.windows.net
☐ Domain Name	browser.events.data.microsoft.com

Rows per page: 50 1-21 of 21 < 1 >

Sign-in Method

☐ Click-to-continue
Users must view and agree the captive portal page in order to access the network

☒ Sign-on With

Users must enter a username and password in order to access the network

Portal Type

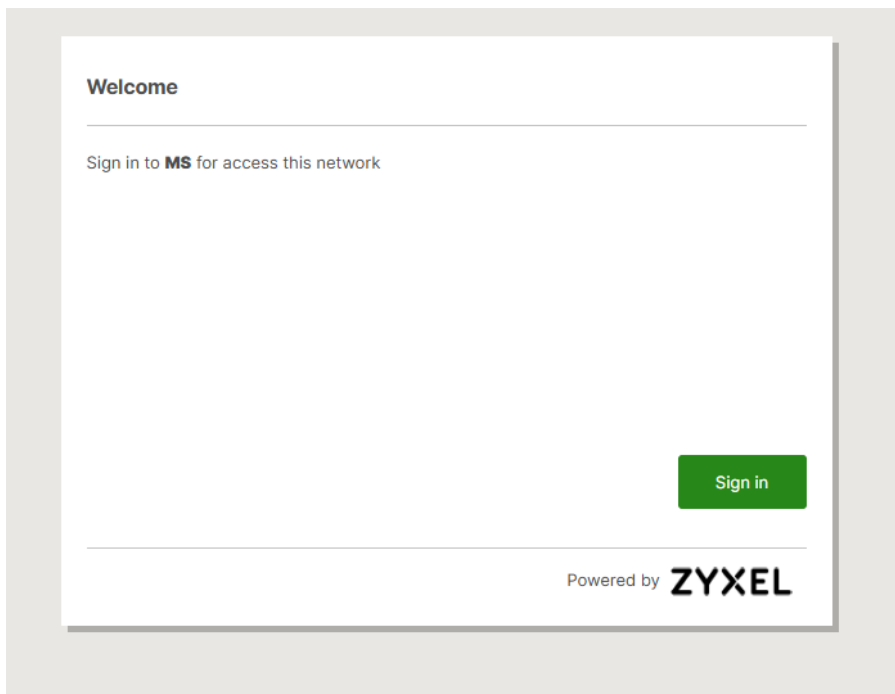
☒ Internal

☐ External

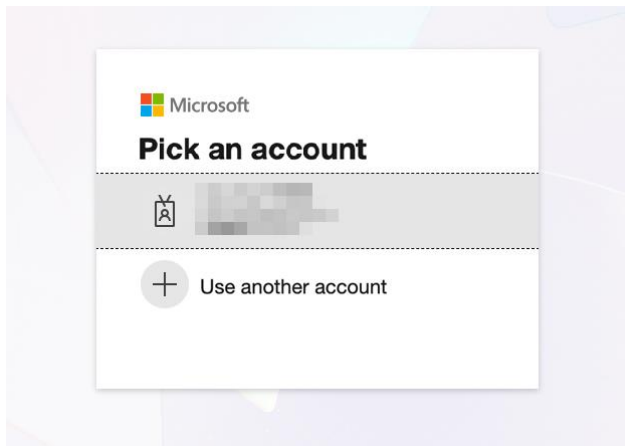
Verification- Test User Login

Verify that the Captive Portal correctly redirects unauthenticated users to Microsoft Entra ID and grants access after successful authentication.

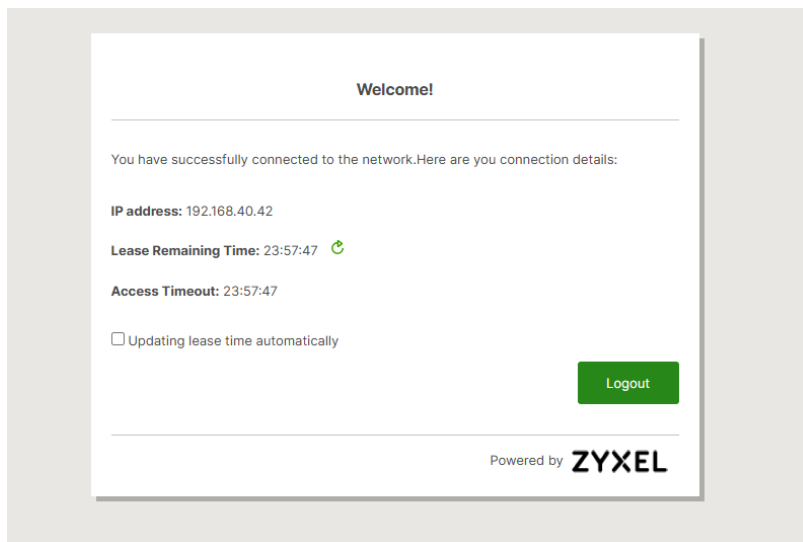
6. Connect a client device
7. Open a browser, display the Captive Portal page, and then click Sign in



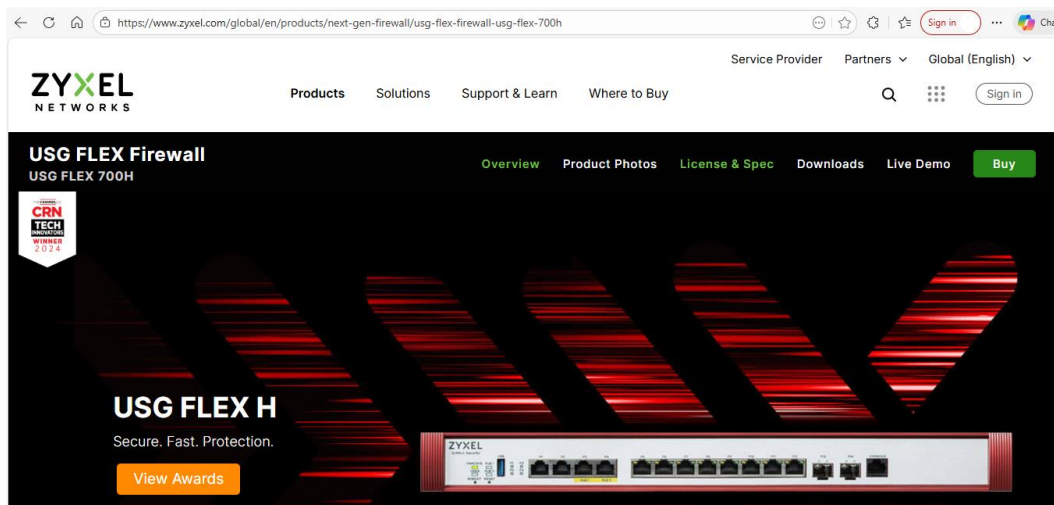
8. Confirm redirect to Microsoft login



9. Successful Authentication and Access Granted.



Internet access is successful.



10. Check login user status at **Network Status > Login Users > Login Users**.

User shown as authenticated via OIDC

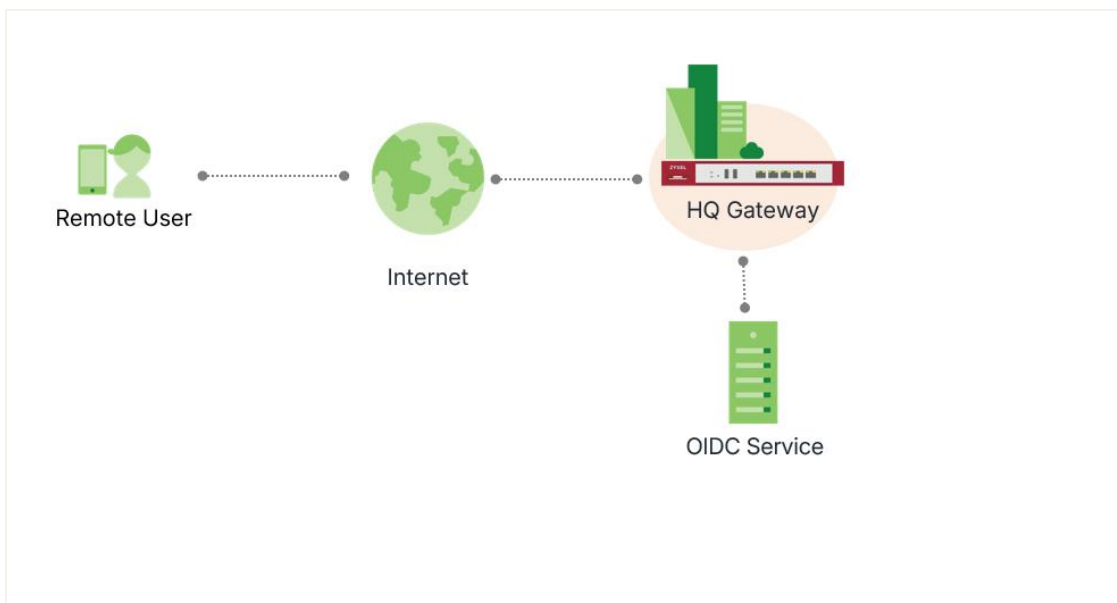
Network Status > Login Users > Login Users

Force Log Out

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1	admin	admin	192.168.40.100	0:07:00	http/https	0.0.0.0	23:25:16	admin(admin)
2	admin	admin	192.168.40.100	0:00:04	http/https	0.0.0.0	23:25:16	admin(admin)
3	admin	admin	192.168.40.100	0:00:04	http/https	0.0.0.0	23:25:16	admin(admin)
4	admin	admin	192.168.40.100	0:00:04	http/https	0.0.0.0	1 day, 0:00:00	admin(admin)
5	ext-user(oidc-users)	user	192.168.40.100	0:00:00	captive portal	0.0.0.0	23:46:23	ext-user(oidc-users)
6	admin@zyxel.com.tw	user	192.168.40.42	0:04:15	captive portal	0.0.0.0	23:55:45	ext-user(oidc-users)

SSLVPN authentication with Google

OpenID Connect (OIDC) is a modern authentication protocol built on OAuth 2.0. We now support OIDC integration with Google for SSLVPN authentication. This integration allows us to leverage their existing identity provider for a seamless login experience while centralizing account management and reducing the risks associated with traditional passwords.



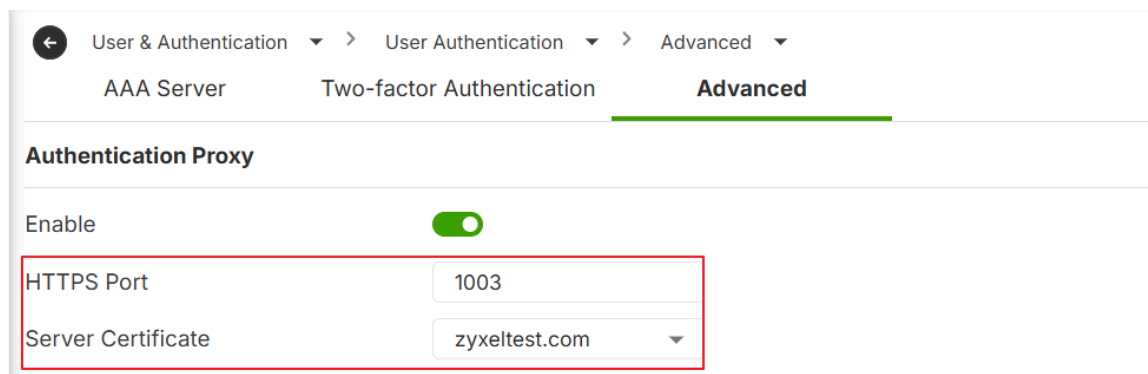
Before You Begin

Before configuring the firewall, you must complete the required setup on your identity provider.

Authentication Proxy

Navigate to User & Authentication > User Authentication > Advanced.

To prevent certificate warnings during the VPN client dial-up, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve to the WAN IP of your firewall.



← User & Authentication > User Authentication > Advanced

AAA Server Two-factor Authentication **Advanced**

Authentication Proxy

Enable ☒

HTTPS Port 1003

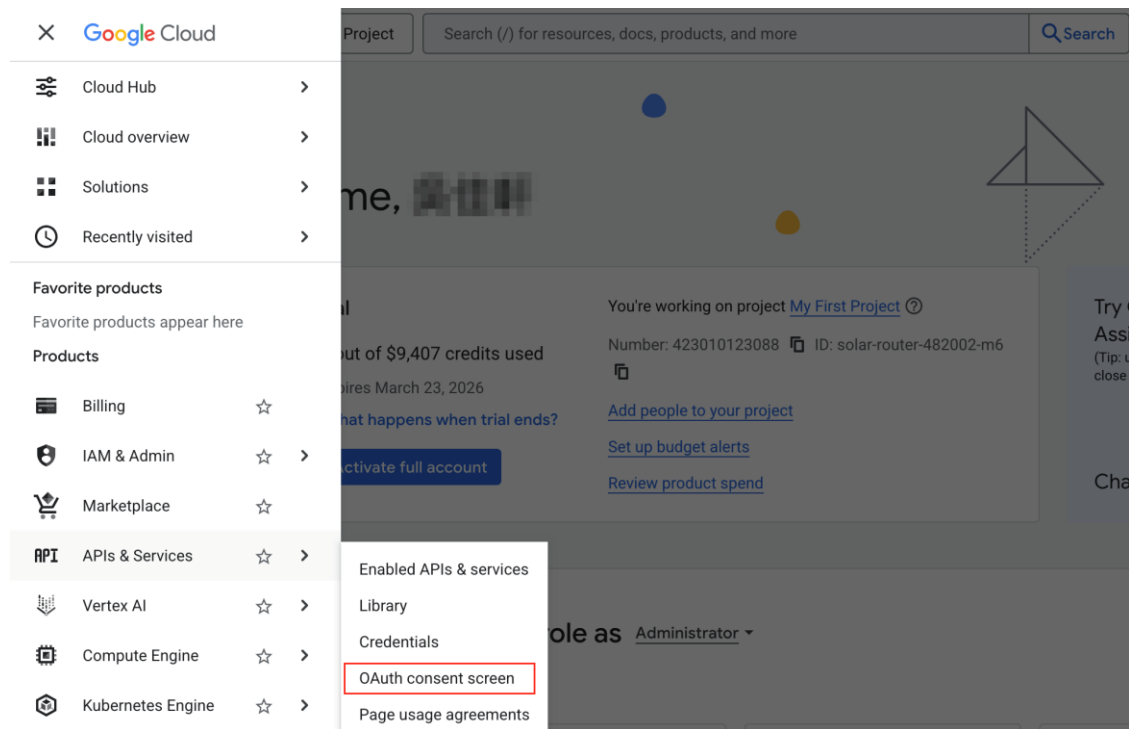
Server Certificate zyxeltest.com



Note: Allow Authentication proxy port (default TCP 1003) at your WAN to ZyWALL secure-policy

Register an APIs & Services in Google

1. Go to Google Cloud Console > APIs & Services > OAuth consent screen



2. Follow the setup wizard to enter your application details. Create a project name

Google Auth Platform / Overview / Create branding

Overview

- Branding
- Audience
- Clients
- Data Access
- Verification Center
- Settings

Project configuration

1 App Information

App name *
OIDC

The name of the app asking for consent

User support email *
[redacted]@gmail.com

For users to contact you with questions about their consent. [Learn more](#)

[Next](#)

2 Audience

3 Contact Information

4 Finish

3. The Audience is set to Internal to restrict API access exclusively to authorized workshop participants and ensure environment isolation

Google Auth Platform / Overview / Create branding

Overview

 Branding

 Audience

 Clients

 Data Access

 Verification Center

Project configuration

App Information

|

 Audience

☒ Internal ?

Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☐ External ?

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

Next

Note: For External Type, to maintain strict access control, you must restrict login permissions under the Audience > Test Users section. Only Google accounts manually added to this whitelist will be authorized to access the application.

4. Enter Contact Information and Create

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

✓ App Information

✓ Audience

3 Contact Information

Email addresses *

1@gmail.com

These email addresses are for Google to notify you about any changes to your project.

Next

4 Finish

Create

Cancel

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

✓ App Information

✓ Audience

✓ Contact Information

✓ Finish

Create

Cancel

5. Continue with the setup wizard to create your OAuth client

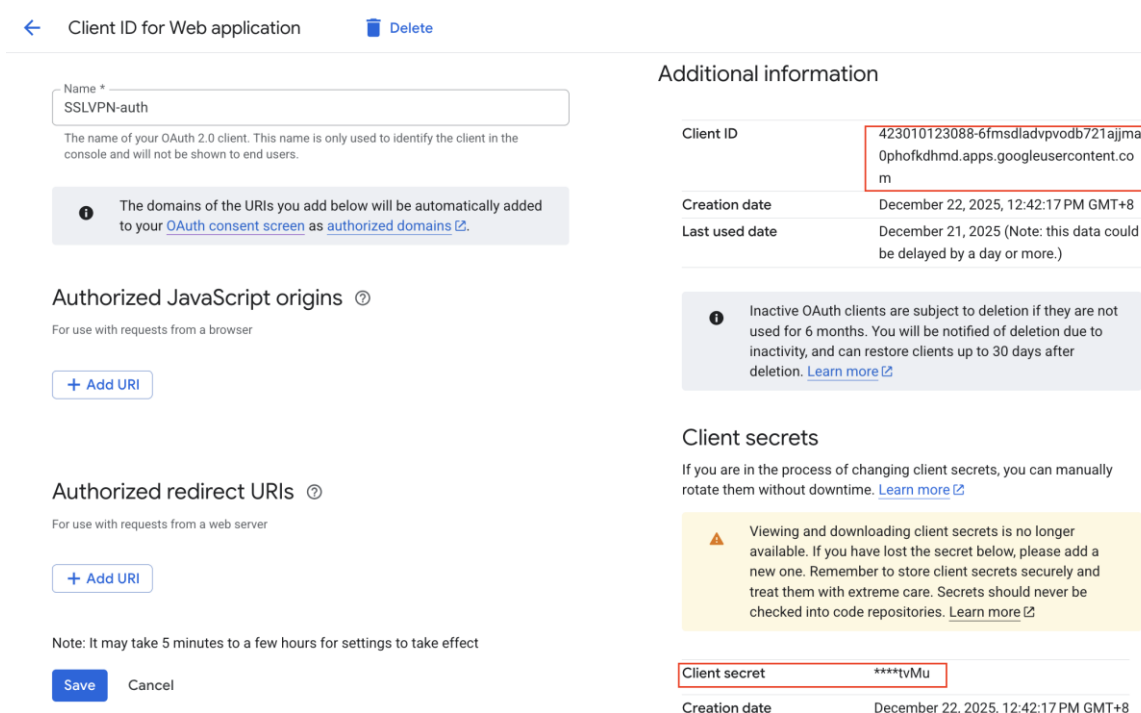
6. Select Application type as "Web application". Assign a recognizable name to your client.

Create OIDC AAA Server

1. Login to the USG FLEX H and navigate to User & Authentication > User Authentication > AAA Server. Add OIDC Server.



Overview your OAuth Client IDs, you need "Client ID", "Client secret" for Firewall setup.



2. Fill in Server details

Issuer URL: <https://accounts.google.com>

Client ID: *{Client ID}*

Client Secret: *{Client Secret}*

Redirect Address: *{FQDN}*



Note: The hostname of the redirect URI should be a FQDN. And the FQDN should match the certificate settings of Authentication proxy on your firewall.

← User & Authentication > User Authentication > AAA Server >

Configuration

Name: **Google**

Description: (Optional)

Server Settings

Issuer URL:

Client ID:

Client Secret:

Redirect Address: (IP or FQDN)

Redirect URI:

Advanced Settings

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

3. Copy the above "Redirect URI" back to Oauth 2.0 Client IDs and paste in Authorized redirect URIs

← Client ID for Web application  Delete

Name *
SSLVPN-auth

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

 The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins

For use with requests from a browser

[+ Add URI](#)

Authorized redirect URIs

For use with requests from a web server

URIs 1 *
<https://zyxelttest.com:1003/oauth2/callback>

[+ Add URI](#)

Additional information

Client ID	423010123088-6fmsdladvpodb721ajjma0phofkdhmd.apps.googleusercontent.com
Creation date	December 22, 2025, 12:42:17 PM GMT+8
Last used date	December 21, 2025 (Note: this data could be delayed by a day or more.)

 Inactive OAuth clients are subject to deletion if they are not used for 6 months. You will be notified of deletion due to inactivity, and can restore clients up to 30 days after deletion. [Learn more](#)

Client secrets

If you are in the process of changing client secrets, you can manually rotate them without downtime. [Learn more](#)

 Viewing and downloading client secrets is no longer available. If you have lost the secret below, please add a new one. Remember to store client secrets securely and treat them with extreme care. Secrets should never be checked into code repositories. [Learn more](#)

Client secret *****tvMu

4. Go back to the USG FLEX H, OIDC Server page, at Configuration Validation.

5. Click Test on the Firewall.

Configuration

Name

Google

Description

(Optional)

Server Settings

Issuer URL

https://accounts.google.com

Client ID

423010123088-6fmsdladvpodb721ajjma0phofkdhmd.apps.googleusercontent.com

Client Secret

.....

Redirect Address

zyxeltest.com

(IP or FQDN)

Redirect URI: https://zyxeltest.com:1003/oauth2/callback

Advanced Settings

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

6. You should see "OIDC Authentication Successful."

OIDC Authentication Test

OIDC Authentication Successful (Verified)

Username: [REDACTED]@gmail.com

user_attr_name: email

state: t_0b406296c52318b61e131871389ad59e

SSLVPN setting on USG FLEX H Series

1. Configure SSLVPN and set OIDC as the Primary Server and Set Allowed User to oidc-users.

Please note you cannot choose another Auth Server if you want to use OIDC.

Authentication ⓘ

Primary Server

OIDC / Google ▼

Secondary Server

none ▼

User

oidc-users  ⓘ

Advanced Settings ▼

Verification

1. Connected VPN via OpenVPN Connect Client
2. A browser will automatically open the Google login page.
3. Authenticate with your Google account.



Note: The OIDC only support OpenVPN Connect Client

 Sign in with Google

Choose an account

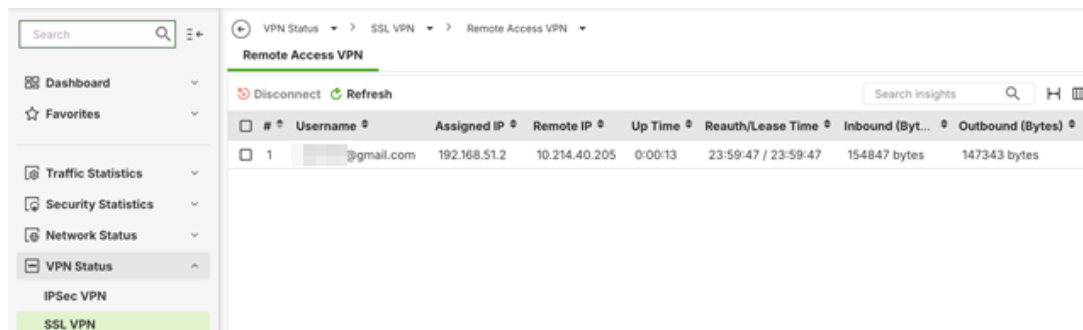
to continue to [zyxeltest.com](#)




 gmail.com

 Use another account

4. Check status at VPN Status > SSL VPN > Remote Access VPN.

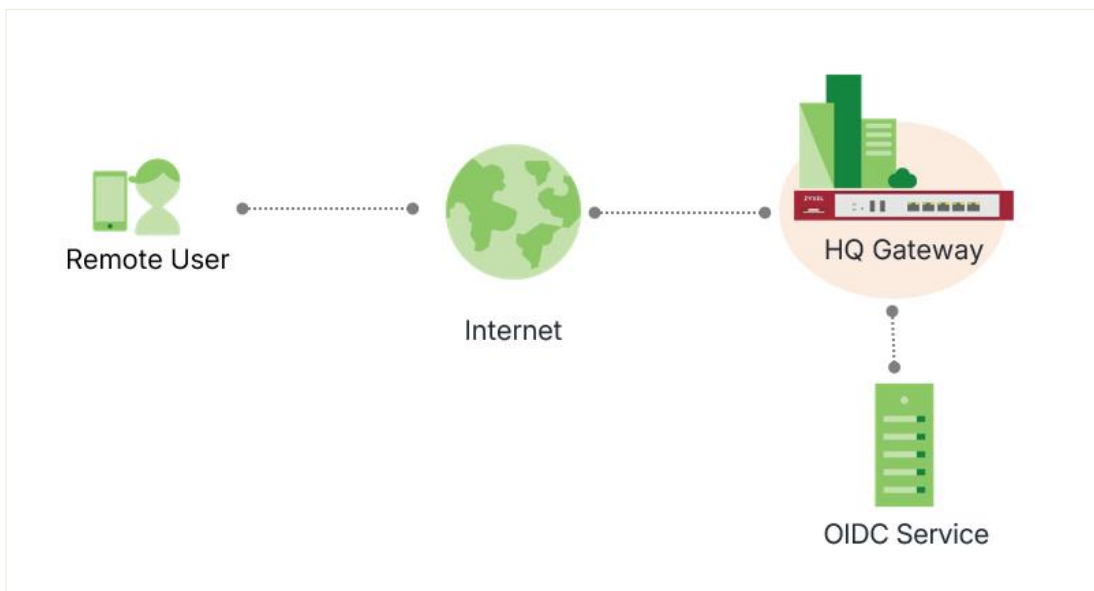


The screenshot shows the ZyXEL management interface. On the left is a sidebar with navigation links: Dashboard, Favorites, Traffic Statistics, Security Statistics, Network Status, VPN Status (selected), IPsec VPN, and SSL VPN. The main content area shows the breadcrumb path: VPN Status > SSL VPN > Remote Access VPN. Below this is a section titled 'Remote Access VPN' with a 'Disconnect' button and a 'Refresh' button. A table displays the status of active VPN connections.

#	Username	Assigned IP	Remote IP	Up Time	Reauth/Lease Time	Inbound (Bytes)	Outbound (Bytes)
1	@gmail.com	192.168.51.2	10.214.40.205	0:00:13	23:59:47 / 23:59:47	154847 bytes	147343 bytes

SSLVPN authentication with Microsoft Entra ID

OpenID Connect (OIDC) is a modern authentication protocol built on OAuth 2.0. We now support OIDC integration with Microsoft Entra ID for SSLVPN authentication. This integration allows us to leverage their existing identity provider for a seamless login experience while centralizing account management and reducing the risks associated with traditional passwords.



Before You Begin

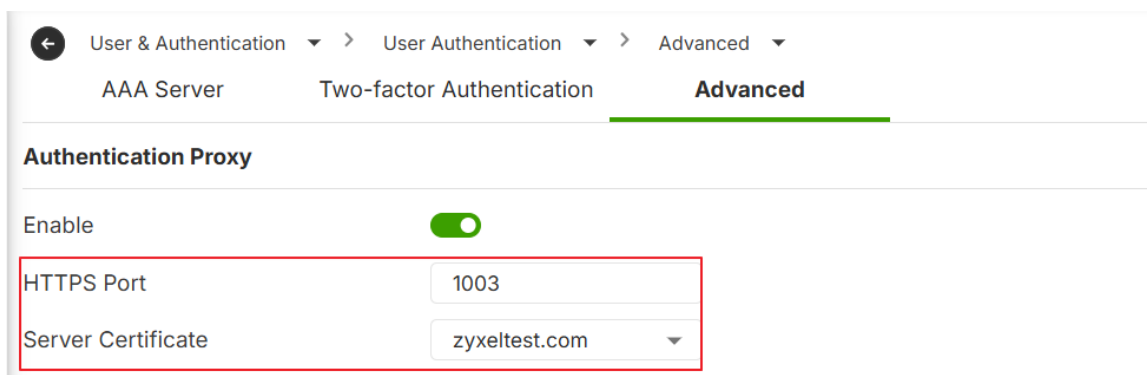
Before configuring the firewall, you must complete the required setup.

- Application Administrator role in your Microsoft Entra ID
- USG FLEX H Series firewall (Firmware in uOS1.37 or later)
- Valid licenses for your identity provider (Microsoft Entra ID)
- Network connectivity between your device and Microsoft Entra ID

Authentication Proxy

Navigate to **User & Authentication > User Authentication > Advanced**

To prevent certificate warnings during the VPN client dial-up, this should be a commercial **CA-signed certificate** or your internal CA's certificate must be distributed to all client devices. And the **Common Name (CN) or SAN (Subject Alternative Name)** of the certificate should be a FQDN that can be resolve to the WAN IP of your firewall.

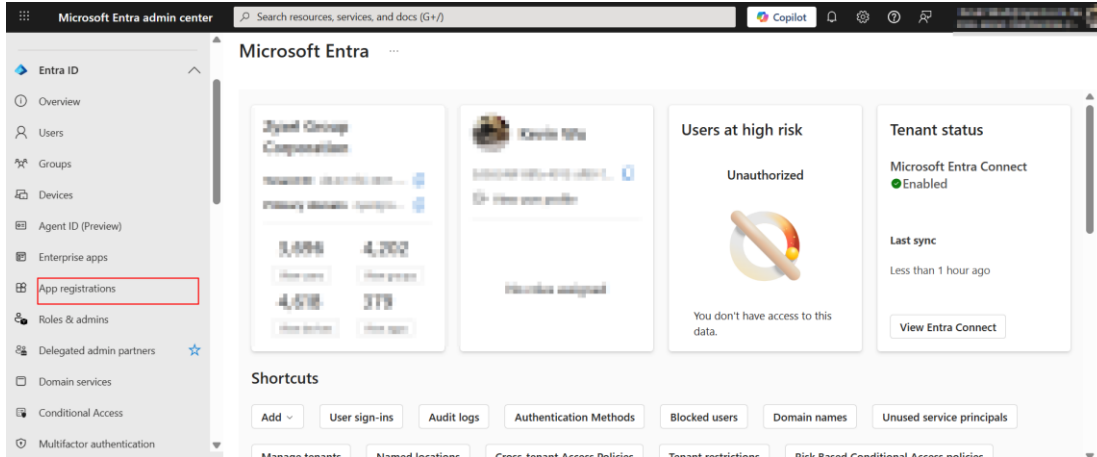


The screenshot shows the 'Advanced' tab of the 'User Authentication' configuration page. Under the 'Authentication Proxy' section, the 'Enable' toggle is turned on. Below it, a red box highlights the 'HTTPS Port' field set to '1003' and the 'Server Certificate' dropdown menu, which currently shows 'zyxeltest.com'.

 Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

Register an Application in Microsoft Entra ID

1. Go to Entra ID Portal > App registrations > New registration.



Home > Roles and administrators | All roles >

App registrations

+ New registration | Endpoints | Troubleshoot | Refresh | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

2. Enter a display name

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SSLVPN-Auth

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)

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

3. Navigate to Manage > API permissions > Add a permissions

Search Refresh Got feedback?

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Zyxel Group Corporation

API / Permissions na...	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
email	Delegated	View users' email address	No	✓ Granted for Zyxel Group...
offline_access	Delegated	Maintain access to data you have give...	No	✓ Granted for Zyxel Group...
openid	Delegated	Sign users in	No	✓ Granted for Zyxel Group...
profile	Delegated	View users' basic profile	No	✓ Granted for Zyxel Group...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Zyxel Group...

4. Please allow "email", "offline_access", "openid", "profile" and "User.Read"

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Zyxel Group Corporation

API / Permissions na...	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
email	Delegated	View users' email address	No	✓ Granted for Zyxel Group...
offline_access	Delegated	Maintain access to data you have give...	No	✓ Granted for Zyxel Group...
openid	Delegated	Sign users in	No	✓ Granted for Zyxel Group...
profile	Delegated	View users' basic profile	No	✓ Granted for Zyxel Group...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Zyxel Group...

5. Navigate to Manage > Certificate & secret > New client secret.

Search Got feedback?

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API

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 (0)** 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
No client secrets have been created for this application.			

SSLVPN-Auth

Search

Delete

Endpoints

Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name

SSLVPN-Auth

Application (client) ID

Object ID

Directory (tenant) ID

Supported account types

My organization only

Client credentials

Add a certificate or secret

Redirect URIs

Add a Redirect URI

Application ID URI

Add an Application ID URI

Managed application in local directory

SSLVPN-Auth

2. Fill in Server details

Issuer URL: `https://login.microsoftonline.com/{Tenant ID}/v2.0`

Client ID: `{Client ID}`

Client Secret: `{You already have Secret at "Manage > Certificate & secrets"}`

Redirect Address: `{FQDN}`

 **Note:** The hostname of the redirect URI should be a FQDN. And the FQDN should match the certificate settings of Authentication proxy on your firewall.

Configuration

Name

MS

Description

(Optional)

Server Settings

Issuer URL

https://login.microsoftonline.com/{Tenant ID}/v2.0

Client ID

Client Secret

.....

Redirect Address

zyxeltest.com

(IP or FQDN)

Redirect URI: https://zyxeltest.com:1003/oauth2/callback

3. Copy the above "Redirect URI" and back to Entra Portal Overview > Add a Redirect URI > Add a platform > Web.

^ Essentials

Display name SSLVPN-Auth	Client credentials Add a certificate or secret
Application (client) ID [REDACTED]	Redirect URIs Add a Redirect URI
Object ID [REDACTED]	Application ID URI Add an Application ID URI
Directory (tenant) ID [REDACTED]	Managed application in local directory SSLVPN-Auth
Supported account types My organization only	

Select a platform to add redirect URI



To understand which platform you should select, please [learn more](#).

Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python
[Select →](#)

Single-page application
Configure browser client applications and progressive web applications. Javascript.
[Select →](#)

4. Paste the URI and Configure

Edit Redirect URI



Web platform



Quickstart



Docs

Redirect URI

https://zyxetest.com:1003/oauth2/callback



e.g. https://example.com/auth

5. Go back to the USG FLEX H, OIDC Server page, at Configuration Validation.

6. Click Test on the Firewall

Configuration

Name **MS**

Description (Optional)

Server Settings

Issuer URL

Client ID

Client Secret

Redirect Address (IP or FQDN)

Redirect URI: https://zyxetest.com:1003/oauth2/callback

Advanced Settings

Configuration Validation

To validate the above settings, click Test button to login OIDC server at new tab.

Test

7. You should see "OIDC Authentication Successful."

OIDC Authentication Test

OIDC Authentication Successful (Verified)

Username: [redacted]@zyxel.com.tw
user_attr_name: email
state: t_8aba663b2ba241e904b80d688df04946

SSLVPN setting on USG FLEX H Series

1. Configure SSLVPN and set OIDC as the Primary Server and Set Allowed User to oidc-users.

Please note you cannot choose another Auth Server if you want to use OIDC.

Authentication 

Primary Server	OIDC / MS	
Secondary Server	none	
User	oidc-users	 

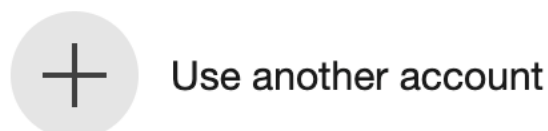
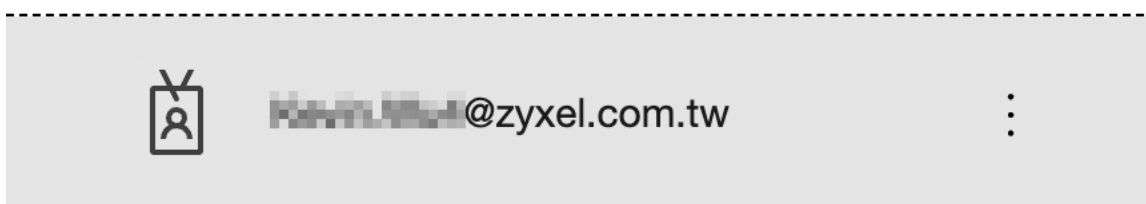
Advanced Settings 

Verification

1. Connected VPN via OpenVPN Connect Client
2. A browser will automatically open the Microsoft login page.
3. Authenticate with your Microsoft account



Pick an account



4. Check status at VPN Status > SSL VPN > Remote Access VPN.

Search

VPN Status

Security Statistics

Network Status

VPN Status

IPSec VPN

SSL VPN

Tailscale

Wireless Status

VPN Status > SSL VPN > Remote Access VPN

Remote Access VPN

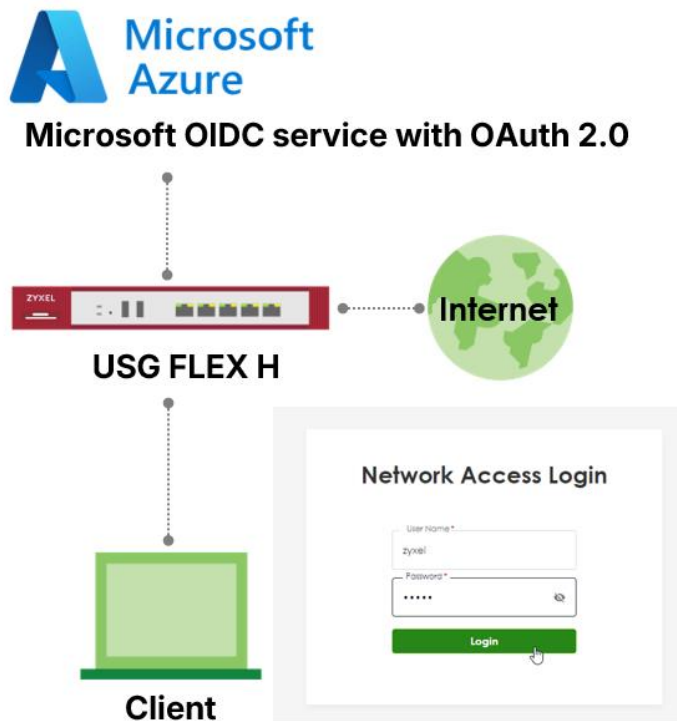
Disconnect Refresh

Search insights

#	Username	Assigned...	Remote IP	Up Time	Reauth/Lease Ti...	Inbound (Byt...	Outbound (Byt...
1	Remote IP: @zyxel.com.tw	192.168.51.2	10.214.40.205	0:00:37	23:59:23 / 23:59:23	258719 bytes	314786 bytes

Captive Portal authentication with Microsoft Entra ID Group

This article describes how to configure Captive Portal authentication on the USG FLEX H series using Microsoft Entra ID (OIDC) and create matching group profiles on the Firewall to map OIDC claims, allowing users to authenticate with their Microsoft account under specific group policies.



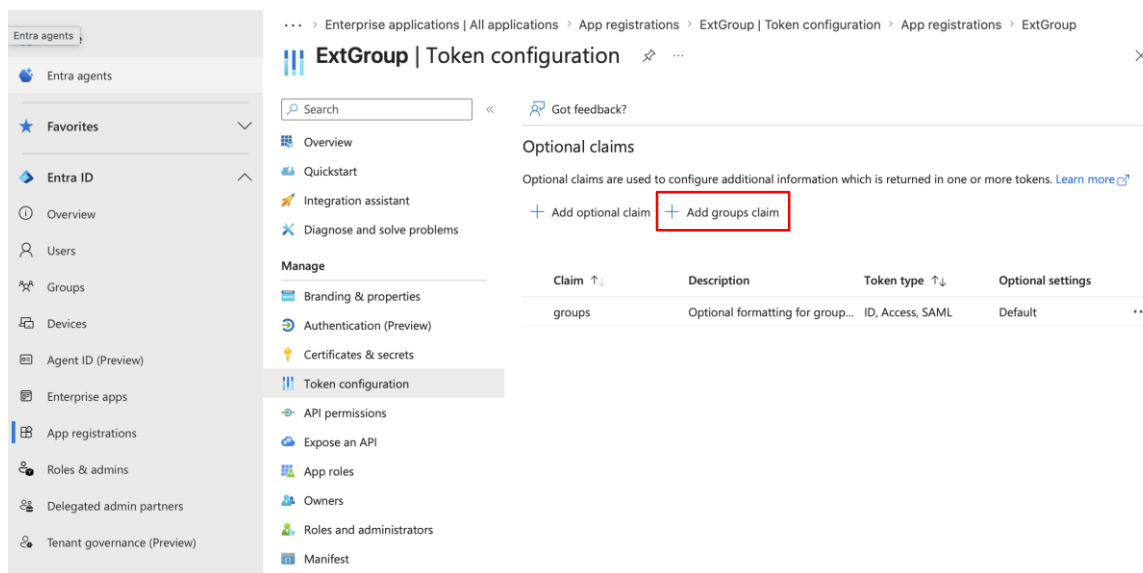
Before You Begin

Before you begin, make sure you have:

- Your firewall has completed the setting with Microsoft Entra ID, please refer to chapter: Captive Portal authentication with Microsoft Entra ID.
- There are already Users and Groups in your Entra.

Add groups claim

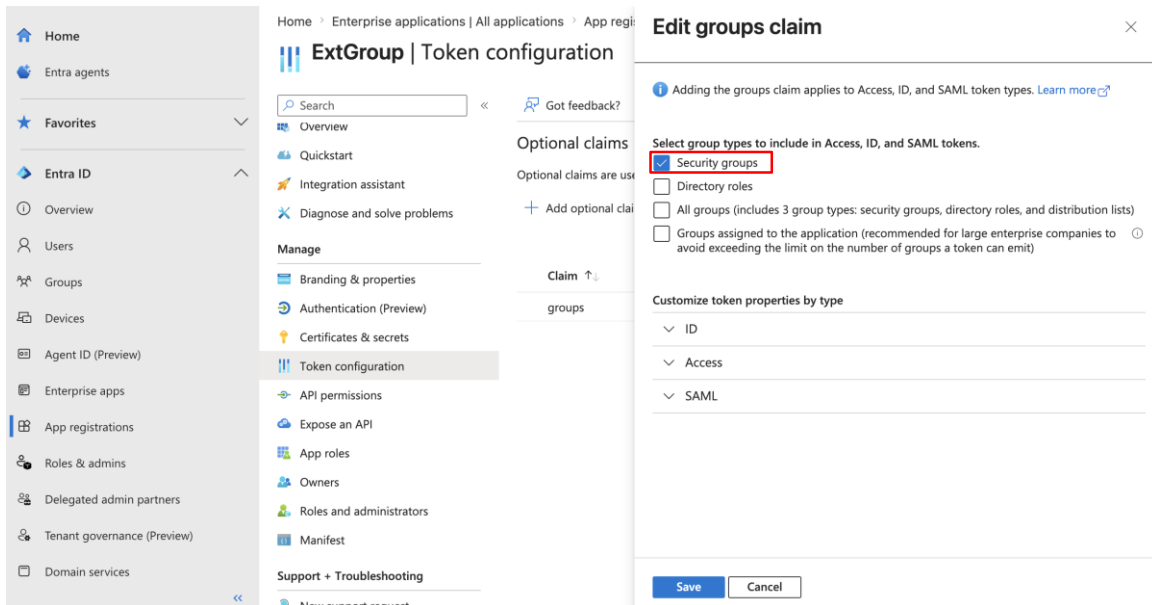
Open Entra Portal, navigate to App registrations > Manage > Token Configuration > Add groups claim



The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar contains navigation links for 'Entra agents', 'Favorites', 'Entra ID', 'Overview', 'Users', 'Groups', 'Devices', 'Agent ID (Preview)', 'Enterprise apps', 'App registrations', 'Roles & admins', 'Delegated admin partners', and 'Tenant governance (Preview)'. The main content area is titled 'ExtGroup | Token configuration'. It includes a search bar, a 'Got feedback?' link, and a list of navigation options: 'Overview', 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage' (with sub-options: 'Branding & properties', 'Authentication (Preview)', 'Certificates & secrets', 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', 'Roles and administrators', and 'Manifest'), and 'Token configuration'. The 'Token configuration' section is active, showing 'Optional claims'. A text description states: 'Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)'. Below this, there are two buttons: '+ Add optional claim' and '+ Add groups claim', with the latter being highlighted by a red box. At the bottom, there is a table with columns: 'Claim', 'Description', 'Token type', and 'Optional settings'. The table contains one row for 'groups' with the description 'Optional formatting for group...', token type 'ID, Access, SAML', and default settings.

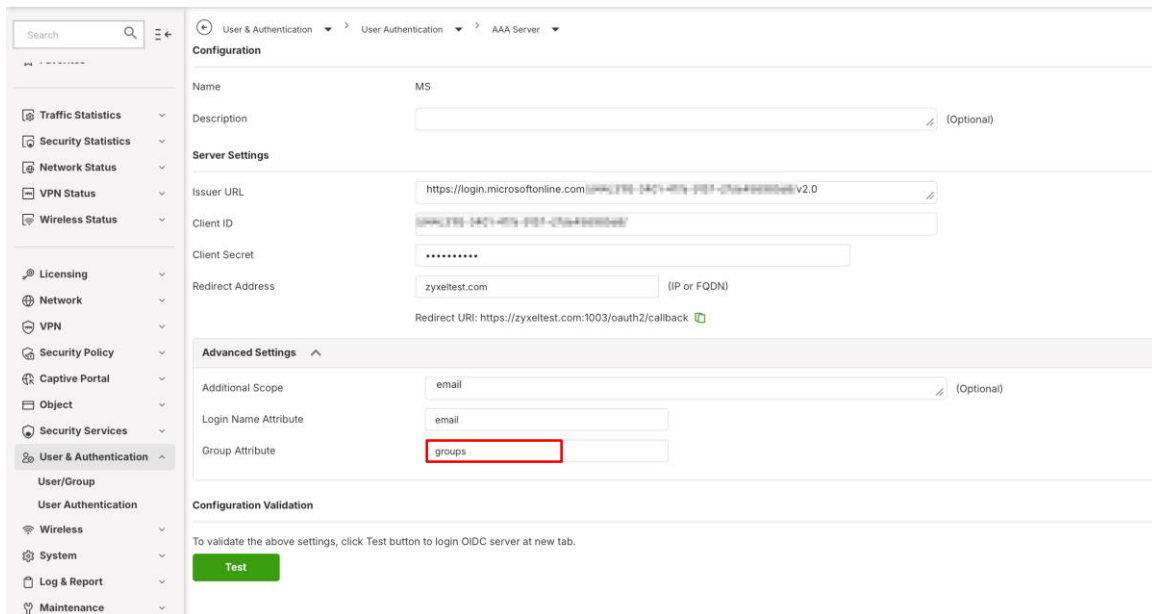
Claim	Description	Token type	Optional settings
groups	Optional formatting for group...	ID, Access, SAML	Default

We recommend **only selecting 'Security groups'**. Choosing 'All Groups' may bloat the token with unnecessary data, potentially causing errors or overage claim issues.



Add Group Attribute on H series

Navigate to User & Authentication > User Authentication > AAA Server, edit the OIDC server which you already created. Add Group Attribute to "groups".



Navigate to User & Authentication > User Authentication > User/Group, Add User with type External Group User, and paste the Group Identifier.

Search

VPN Status

Wireless Status

Licensing

Network

VPN

Security Policy

Captive Portal

Object

Security Services

User & Authentication

User/Group

User Authentication

User & Authentication > User/Group > User

Profile Management

User Name: CSO_Security

User Type: External Group User

Authentication Server: MS / OIDC

Group Identifier: XXXXXXXXXXXX

Description:

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

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Add Captive Portal Policy

Navigate to Captive Portal > Authentication Policy. You must enable Walled Garden and select Trusted Identity Provider to Microsoft Entra ID.

Search

Captive Portal > Authentication Policy

General Settings

Enable ☒

Description

Criteria

Incoming LAN

Source Address any

Destination Address any

Exempt List

+ Add - Remove

Type	Object
Service	DNS

Enable Walled Garden ☒

Trusted Identity Provider Microsoft Entra ID

Walled Garden List

+ Add - Remove

Type	Object
No data	

Select Sign-in Method to OIDC server.

Search

Captive Portal > Authentication Policy

Incoming LAN

Source Address any

Destination Address any

Exempt List

+ Add - Remove

Type	Object
Service	DNS

Enable Walled Garden ☒

Trusted Identity Provider Microsoft Entra ID

Walled Garden List

+ Add - Remove

Type	Object
No data	

Sign-in Method

☐ Click-to-continue

Users must view and agree the captive portal page in order to access the network

☒ Sign-on With OIDC /MS

Users must enter a username and password in order to access the network

☒ Internal Default

☐ External

URL

Verification

After the client completes the Captive Portal Login, you can see the OIDC login information at

Network Status > Login Users.

Search

Network Status > Login Users > Login Users

Login Users Lockout IPs

Force Log Out

Search Insights

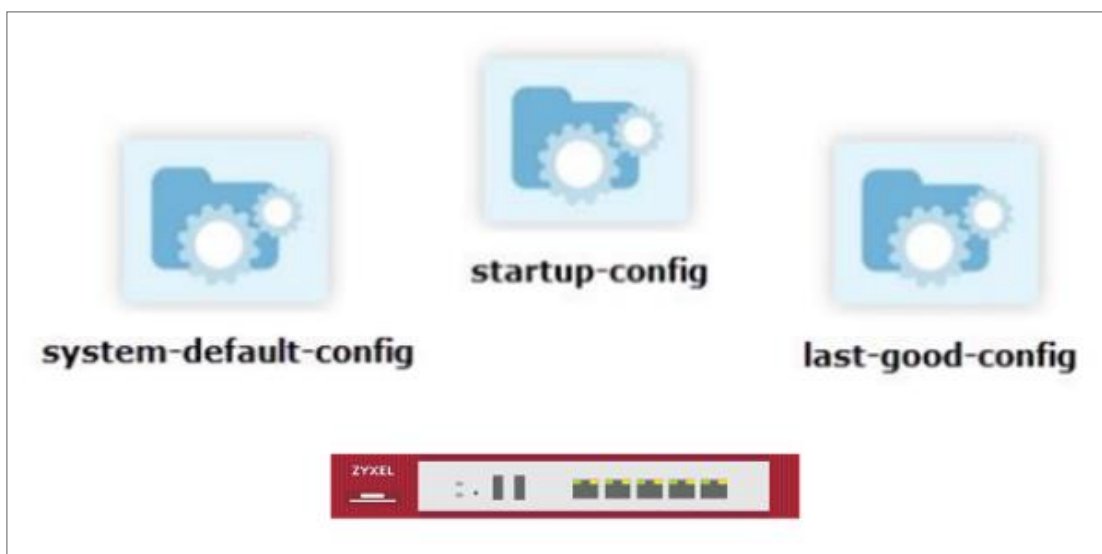
#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1	admin	admin	192.168.168.88	0:02:26	http/https	0.0.0.0	23:59:59	admin(admin)
2	[redacted]@zyxel.com.tw	user	192.168.168.88	0:00:15	captive portal	0.0.0.0	23:59:45	ext-group-user:SSO_Security ext-user(oidc-users)

Interface
Device Insight
Login Users
DHCP Table

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.

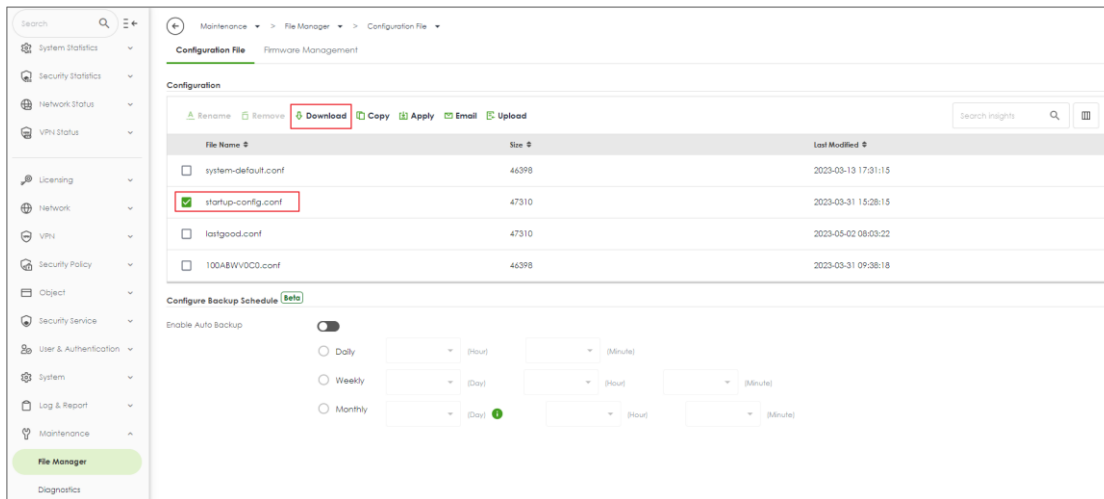
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

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".

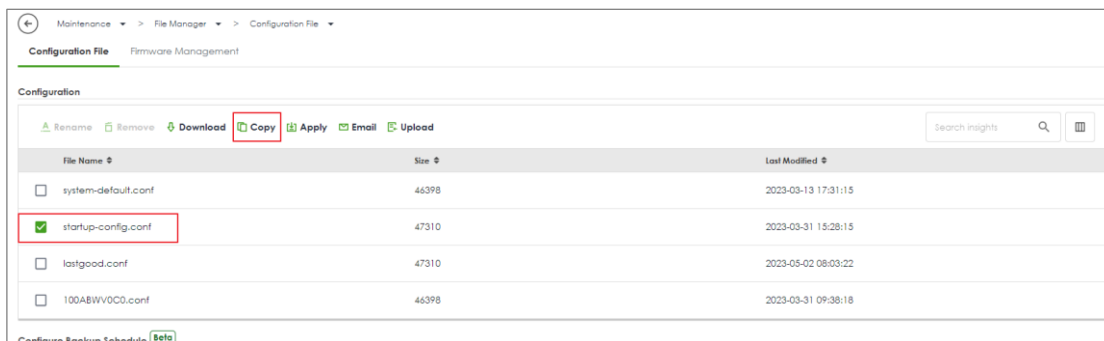


The screenshot shows the ZyXel File Manager interface. On the left is a sidebar with navigation options: System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, Log & Report, Maintenance, File Manager (highlighted), and Diagnostics. The main area is titled 'Configuration File' under 'Firmware Management'. It includes a 'Configuration' section with buttons: Rename, Remove, Download (highlighted with a red box), Copy, Apply, Email, and Upload. Below this is a table with columns 'File Name', 'Size', and 'Last Modified'. The table contains four rows: 'system-default.conf' (46398, 2023-03-13 17:31:15), 'startup-config.conf' (47310, 2023-03-31 15:28:15) which is selected with a green checkmark, 'lastgood.conf' (47310, 2023-05-02 08:03:22), and '100ABWVOC0.conf' (46398, 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

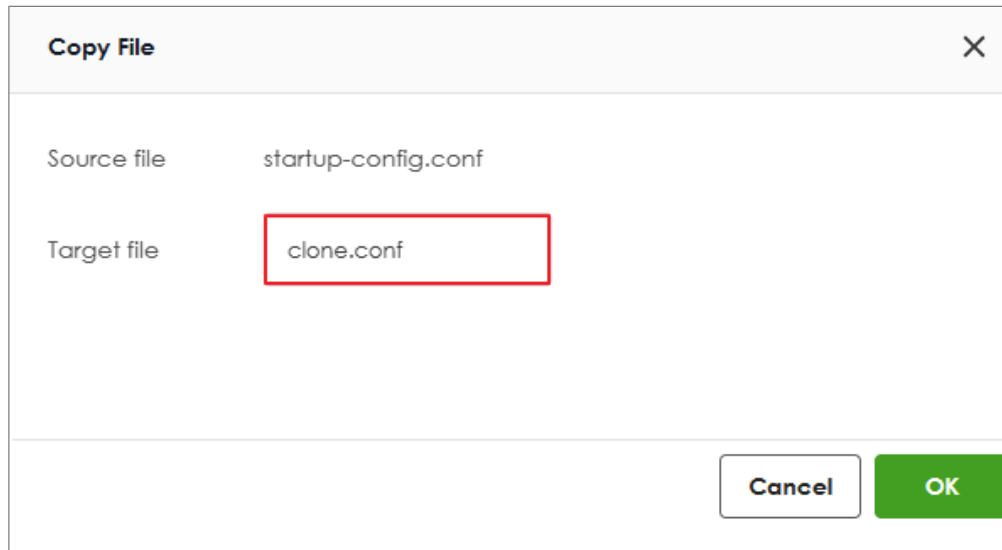
Select the file and click "Copy".



This screenshot is similar to the previous one, showing the same ZyXel File Manager interface. In this view, the 'Copy' button in the 'Configuration' section is highlighted with a red box. The 'startup-config.conf' file remains selected with a green checkmark in the table below.

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

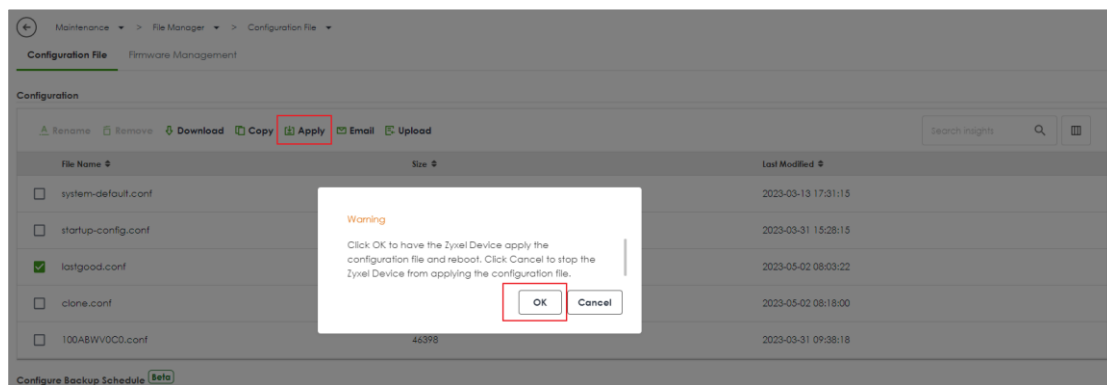


The image shows a 'Copy File' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Source file' with the value 'startup-config.conf' and 'Target file' with the value 'clone.conf'. The 'Target file' field is highlighted with a red rectangular border. At the bottom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

Apply the Configuration Files

Maintenance > File Manager > Configuration File

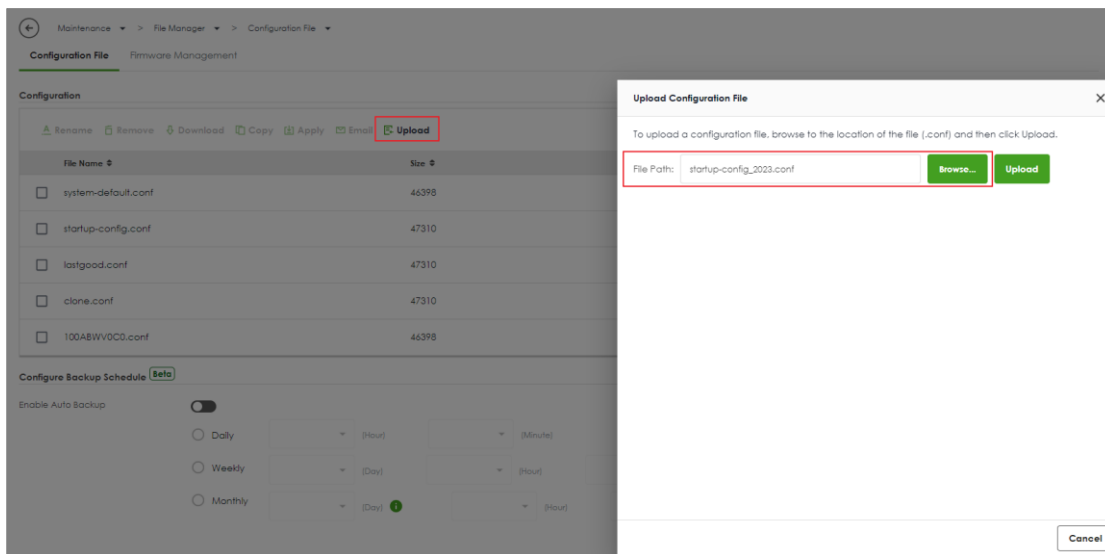
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when 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](https://portal.myzyxel.com/my/firmwares) portal.
(<https://portal.myzyxel.com/my/firmwares>)

Maintenance > File Manager > Firmware Management				
Configuration File Firmware Management				
Firmware Status				
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.

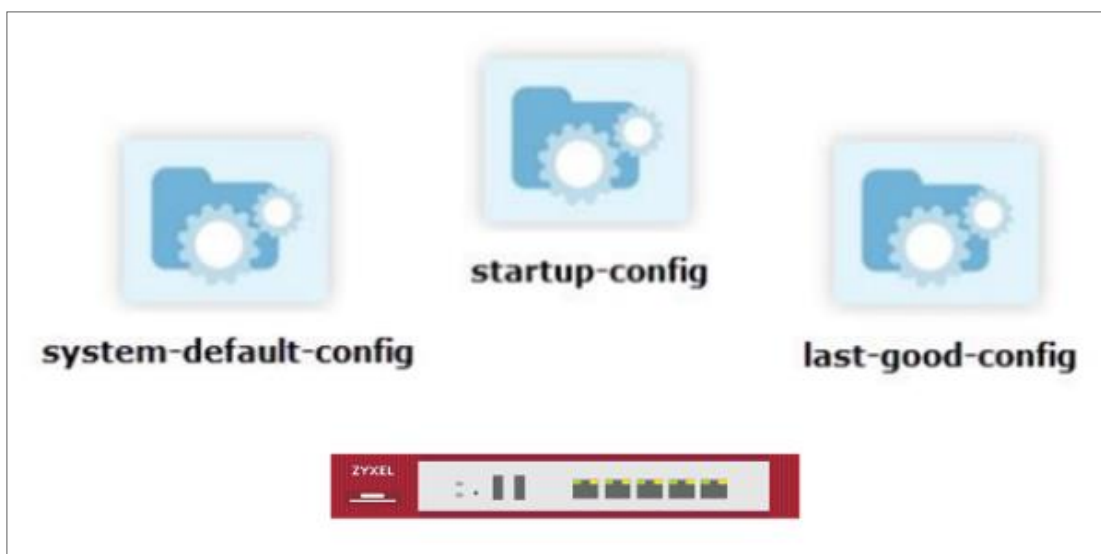
Furthermore, the "Auto Update" feature can be activated to automatically download firmware to your firewall first and reboot your device within a specified time frame.

Cloud Firmware Information

Latest Version	None	Check Now
Release Date	None	
Auto Update	☒ ☐ Daily (Hour) ☐ Weekly (Day) (Hour)	
Auto Reboot ☐		

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.

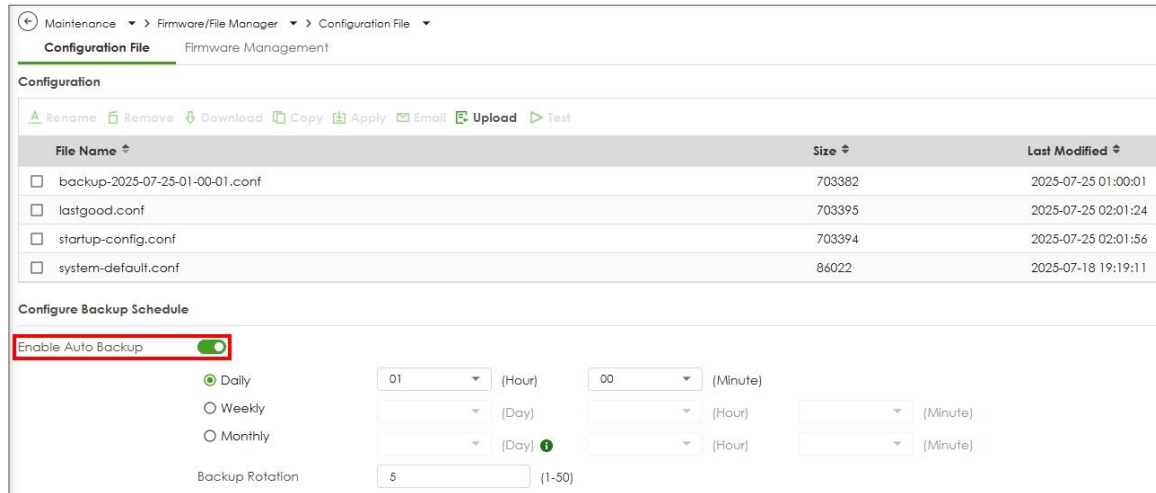


 Note: The **system-default.conf** file contains the default settings. This configuration file is included when you upload a firmware package.

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
☐ backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
☐ lastgood.conf	703395	2025-07-25 02:01:24
☐ startup-config.conf	703394	2025-07-25 02:01:56
☐ system-default.conf	86022	2025-07-18 19:19:11

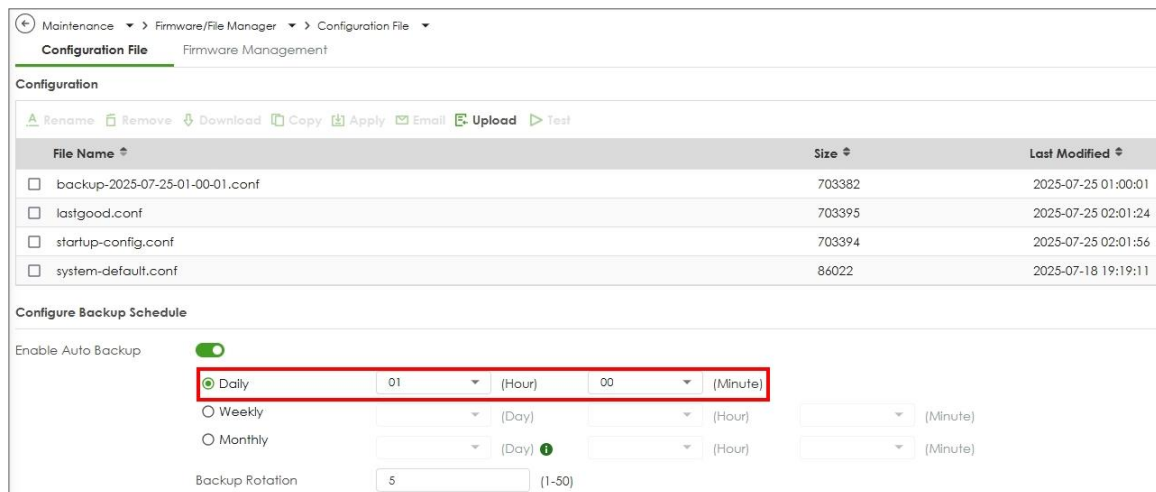
Configure Backup Schedule

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
☐ backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
☐ lastgood.conf	703395	2025-07-25 02:01:24
☐ startup-config.conf	703394	2025-07-25 02:01:56
☐ 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
☐ backup-2025-07-25-01-00-01.conf	703382	2025-07-25 01:00:01
☐ lastgood.conf	703395	2025-07-25 02:01:24
☐ startup-config.conf	703394	2025-07-25 02:01:56
☐ 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
☐ backup-2025-07-25-01-00-01.conf	703382
☐ backup-2025-07-26-01-00-01.conf	703382
☐ backup-2025-07-27-01-00-01.conf	703382
☐ backup-2025-07-28-01-00-01.conf	703382
☐ backup-2025-07-29-01-00-01.conf	703382
☐ lastgood.conf	703395
☐ startup-config.conf	703473
☐ 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							
Search Insights							
#	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							
Search Insights							
#	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 exceeded	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)

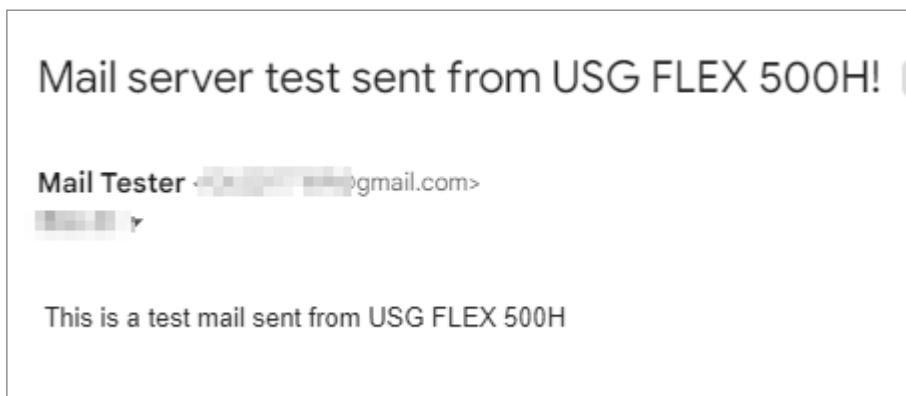
Send From

@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3:45

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

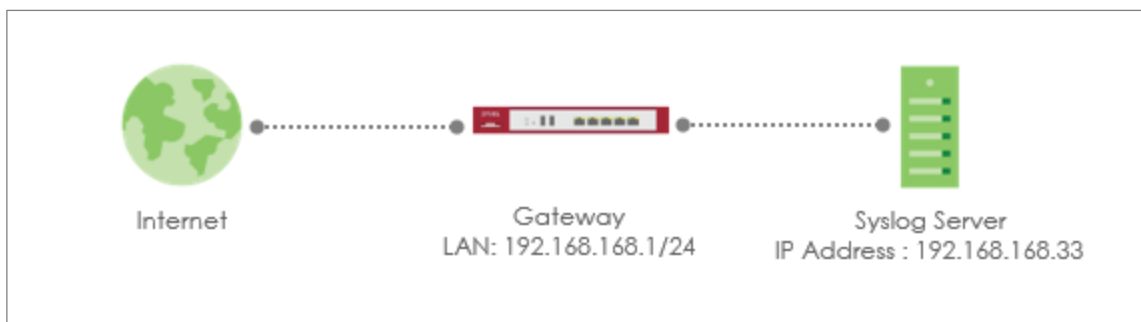
System Name:

usgflex500h

System Resource Usage

How to Setup and Send Logs to a Syslog Server

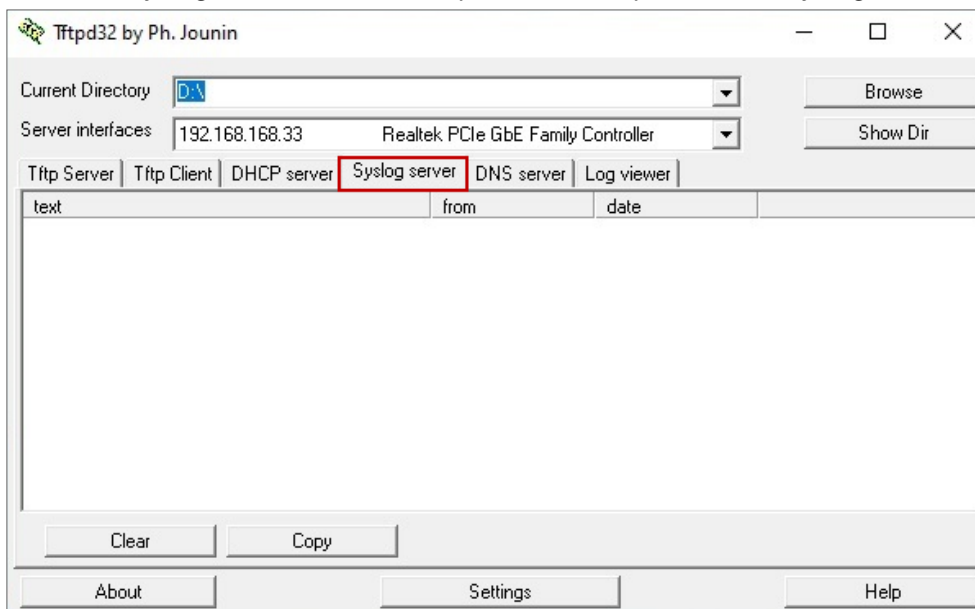
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system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

Set Up the Syslog Server

Install the syslog server. In this example, we use tftpd32 as the syslog server.



Set Up Remote Server Setting 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

Q

System Log

disablenormaldebug

USB Storage

disablenormaldebug

Remote Server 1

disablenormaldebug

Remote Server 2

disablenormaldebug

Count

>Authenticate

9

>Security

0

>System

13

>Security Service

6

>VPN

0

>License

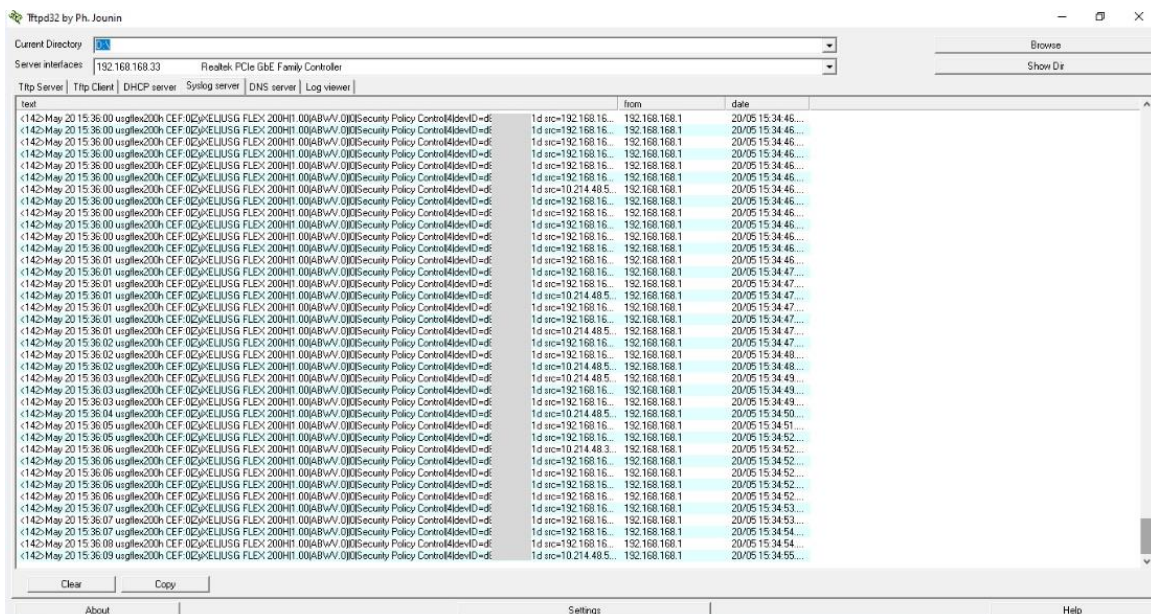
130

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	
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
	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	
> Authenticate	☐	☒	☐	☒	☐	☐	☒	☐	☐	☒	☐	☐	3
▼ Security	☐	☒	☐	☐	☐	☐	☒	☐	☐	☒	☐	☐	1
Security Policy Control	☐	☒	☐	☐	☒	☐	☒	☐	☐	☒	☐	☐	1
DoS Prevention	☐	☒	☐	☒	☐	☐	☒	☐	☐	☒	☐	☐	0
> System	☐	☐	☐	☐	☐	☐	☒	☐	☐	☒	☐	☐	0
> Security Service	☐	☐	☐	☒	☐	☐	☒	☐	☐	☒	☐	☐	0
> VPN	☐	☒	☐	☒	☐	☐	☒	☐	☐	☒	☐	☐	0
> License	☐	☒	☐	☒	☐	☐	☒	☐	☐	☒	☐	☐	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

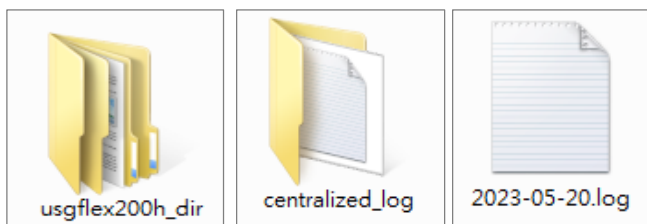
Go to Maintenance > Diagnostics > System Log. Select a file and click “Download” to view the log.

System Log Archives in USB Storage			
☐ Remove	☒ Download	Search insights Search List	
☒	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

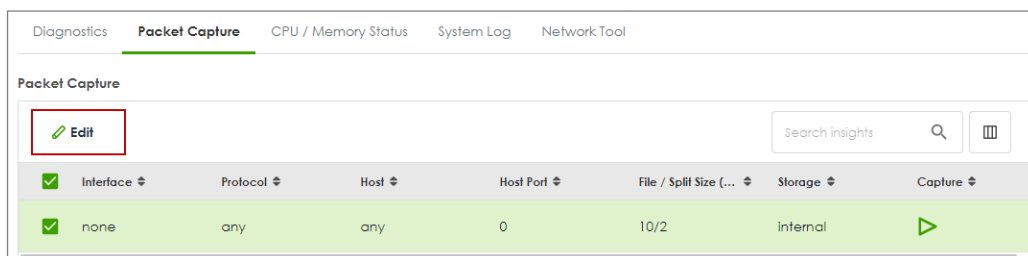
This example shows how to use the Packet Capture feature to capture network traffic going through the device's interfaces. Studying these packet captures may help you analyze network problems.



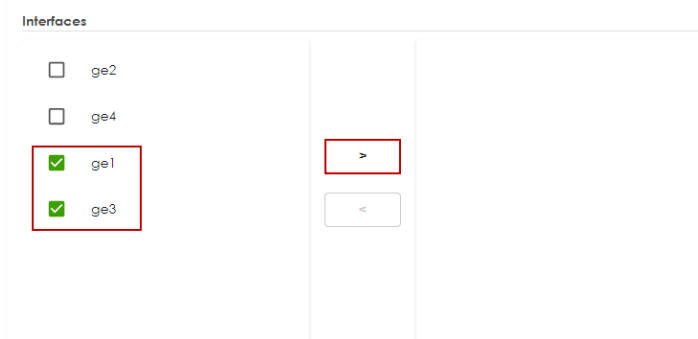
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the Packet Capture Feature

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



- 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.

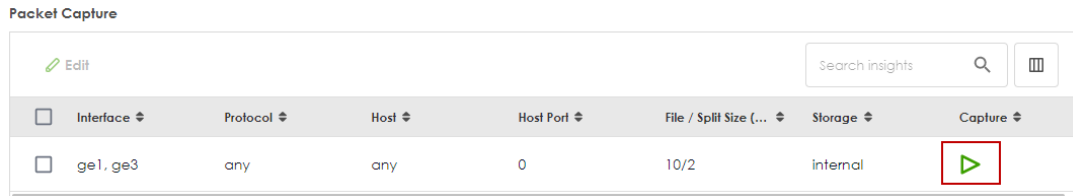
Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

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

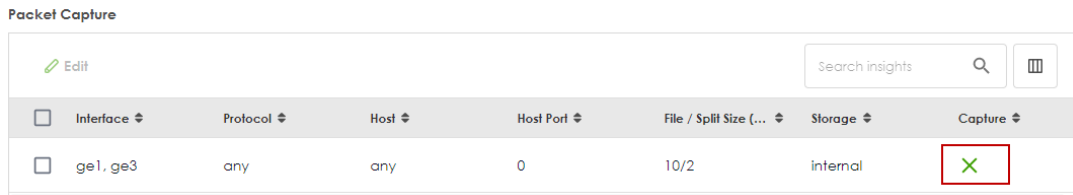
8. In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".

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
☒ Save data to onboard storage only ☐ Save data to USB storage ☐ Save data to ftp server	

- Click the icon to start capturing packets.

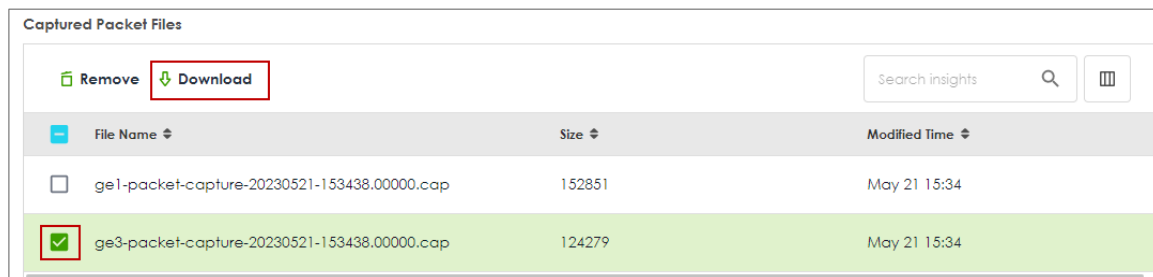


- Click the icon to stop capturing packets.



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>"

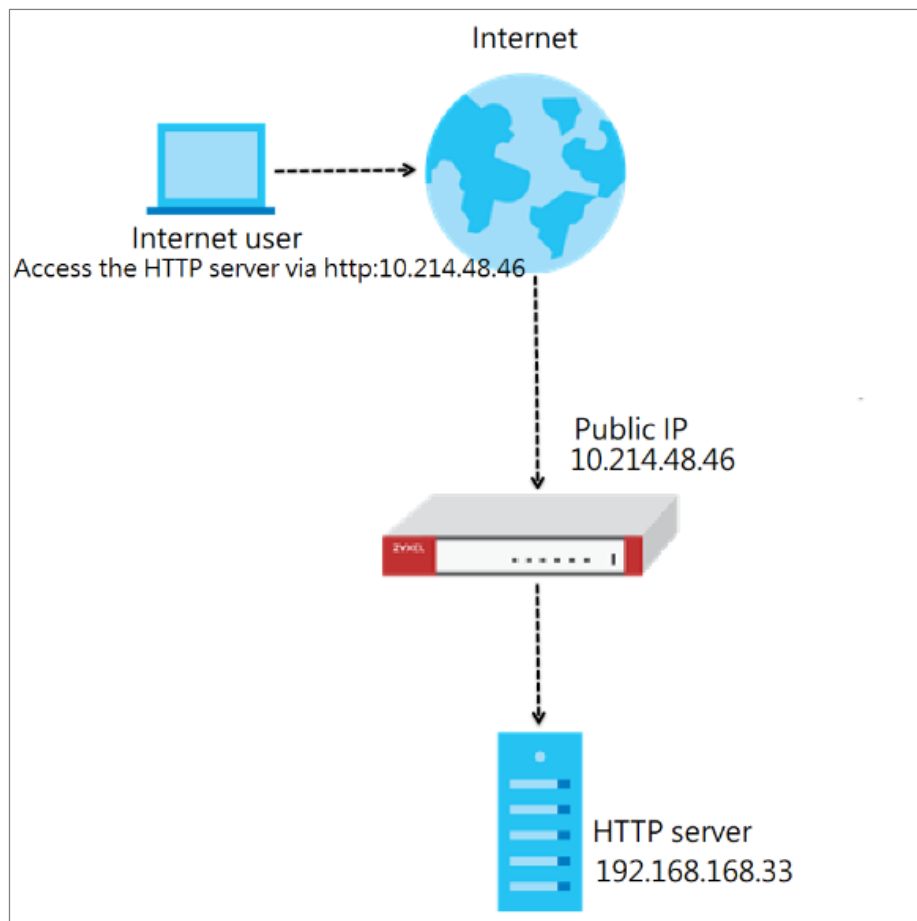
cmd traffic-capture <interface name> filter "port <port number>"

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 web interface for configuring NAT. The 'Port Mapping Type' section is active, with 'Virtual Server' 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', which is highlighted with a red box. A 'Select Address' dialog box is open on the right, showing the 'Add Object' button highlighted with a red box. The dialog box also shows a list of objects: 'user defined (default)', 'IP6to4-Relay', 'executives1', and 'executives2'.

- 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

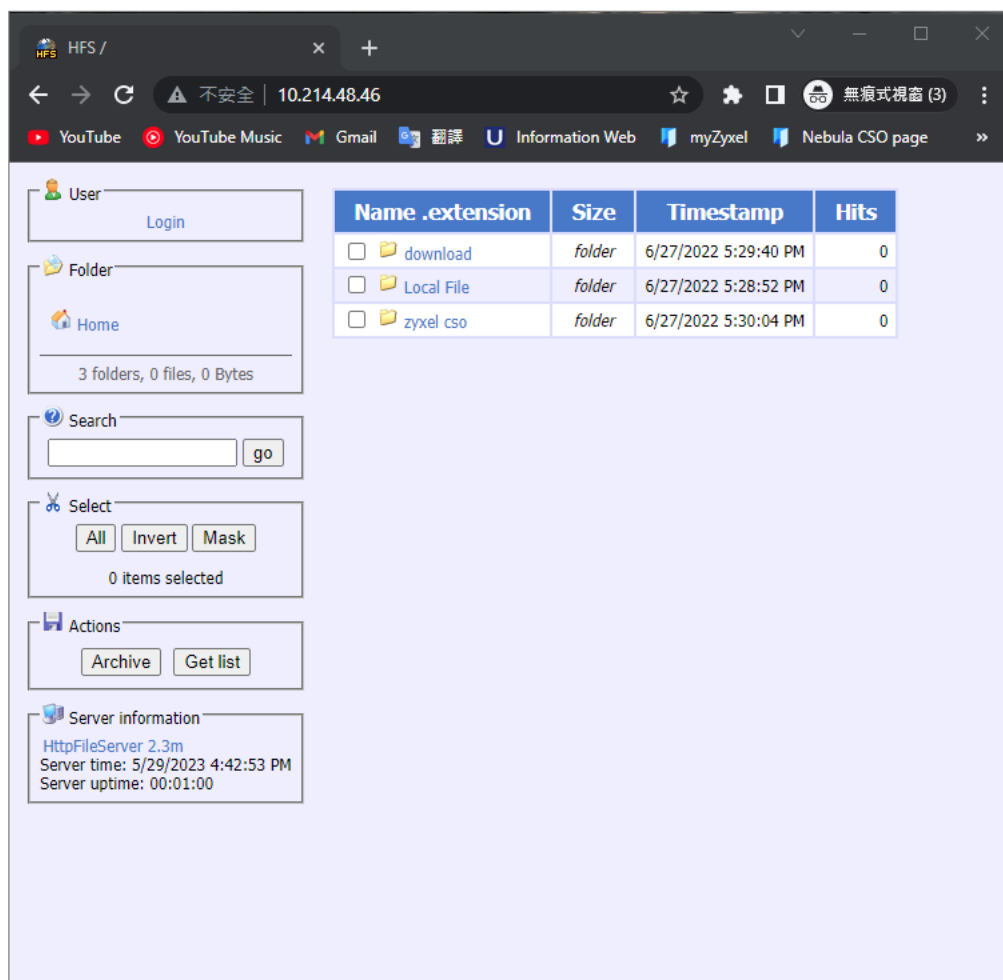
Port Mapping Type Service

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 is titled "HFS /" and shows a sidebar on the left with the following sections:

- 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

The main content area displays a table with the following data:

	Name .extension	Size	Timestamp	Hits
☐	download	folder	6/27/2022 5:29:40 PM	0
☐	Local File	folder	6/27/2022 5:28:52 PM	0
☐	zyxel cs0	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.

← Network > Interface >

General Settings

Enable Interface ☒

Interface Properties

Role external

Interface Type Ethernet

Interface Name ge1

Port p1 (ge1)

Zone WAN

MAC Address

Description

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.

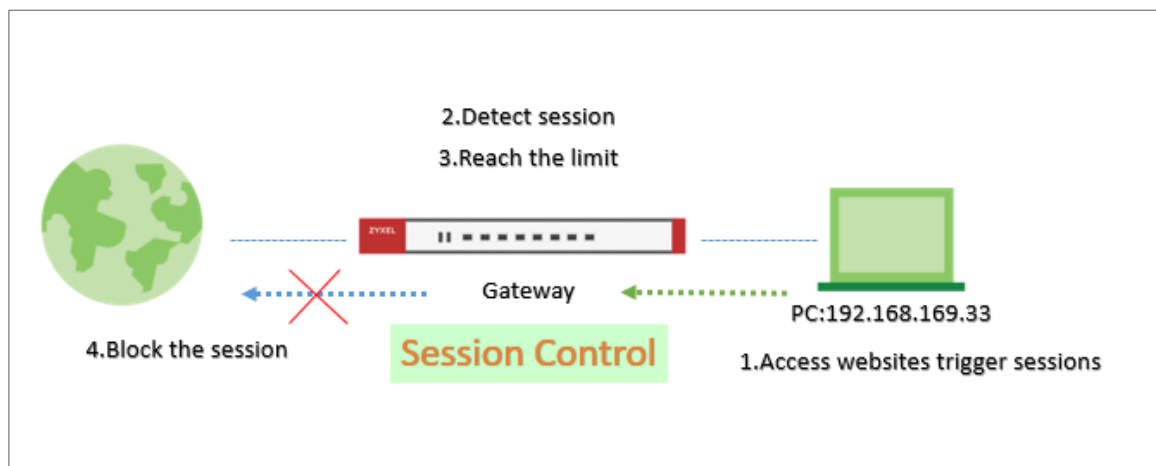
```

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

```

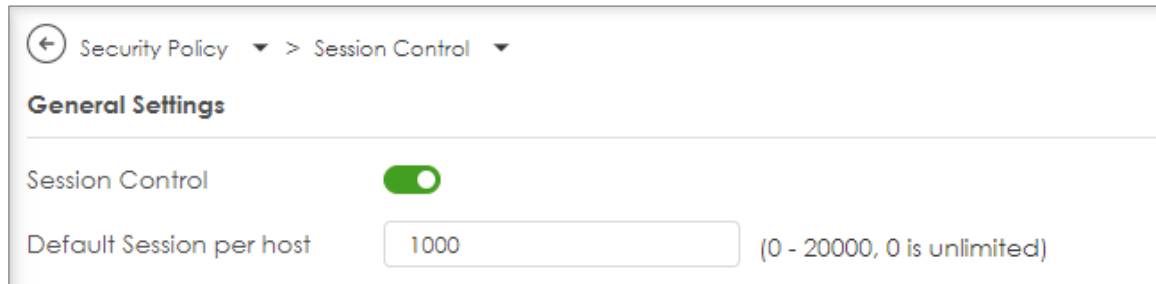
How to Configure Session Control

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

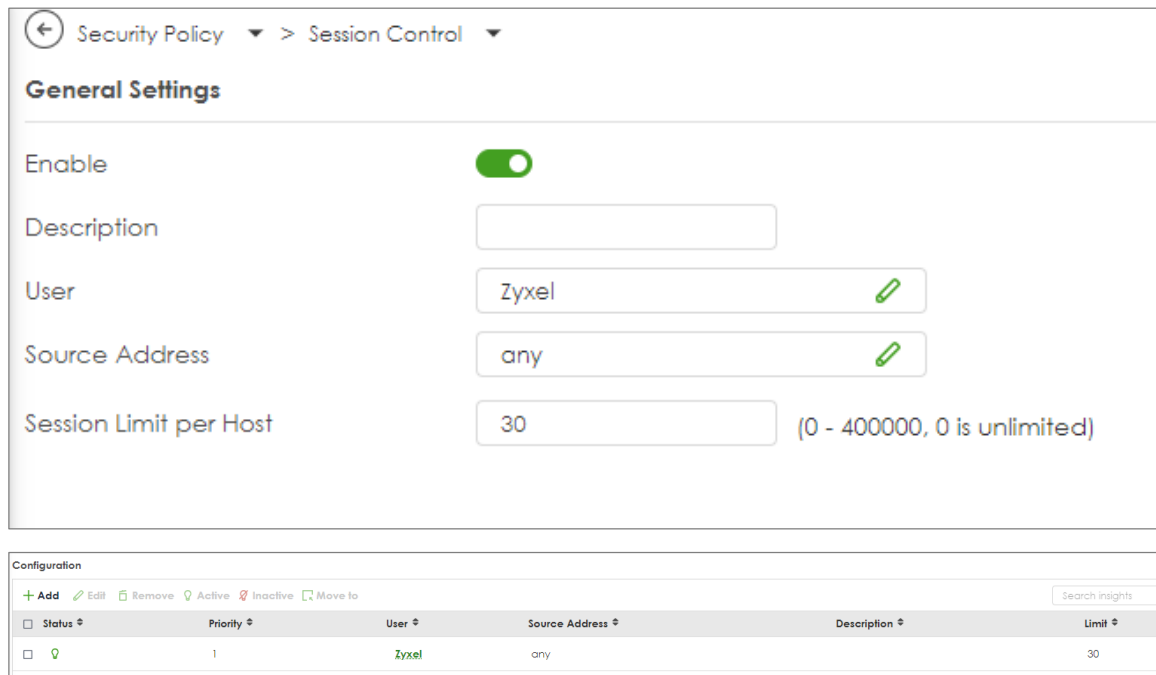
Configuration

+ 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
☒	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

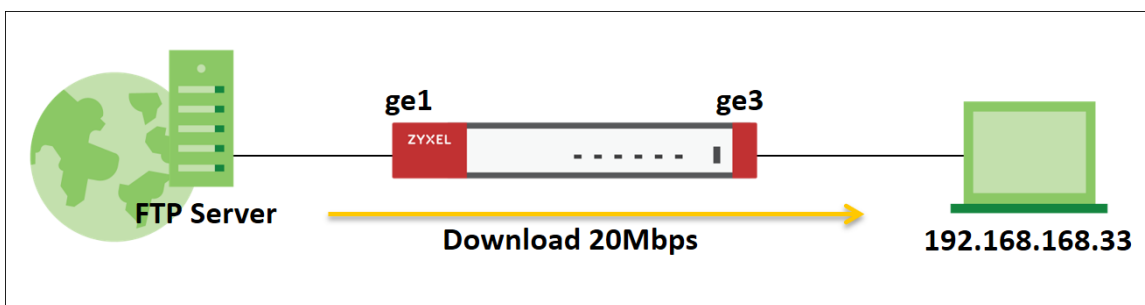
Try to access web browser to hit the session limit

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

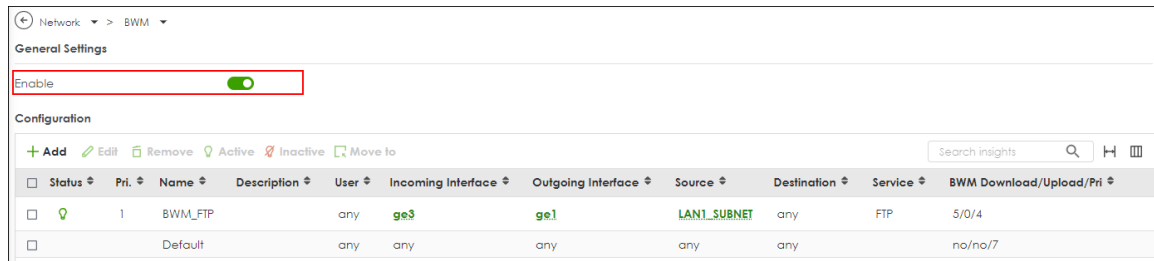
If you select the "Per-Source-IP" setting in the BWM rule, each selected IP address will have a limited bandwidth.

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



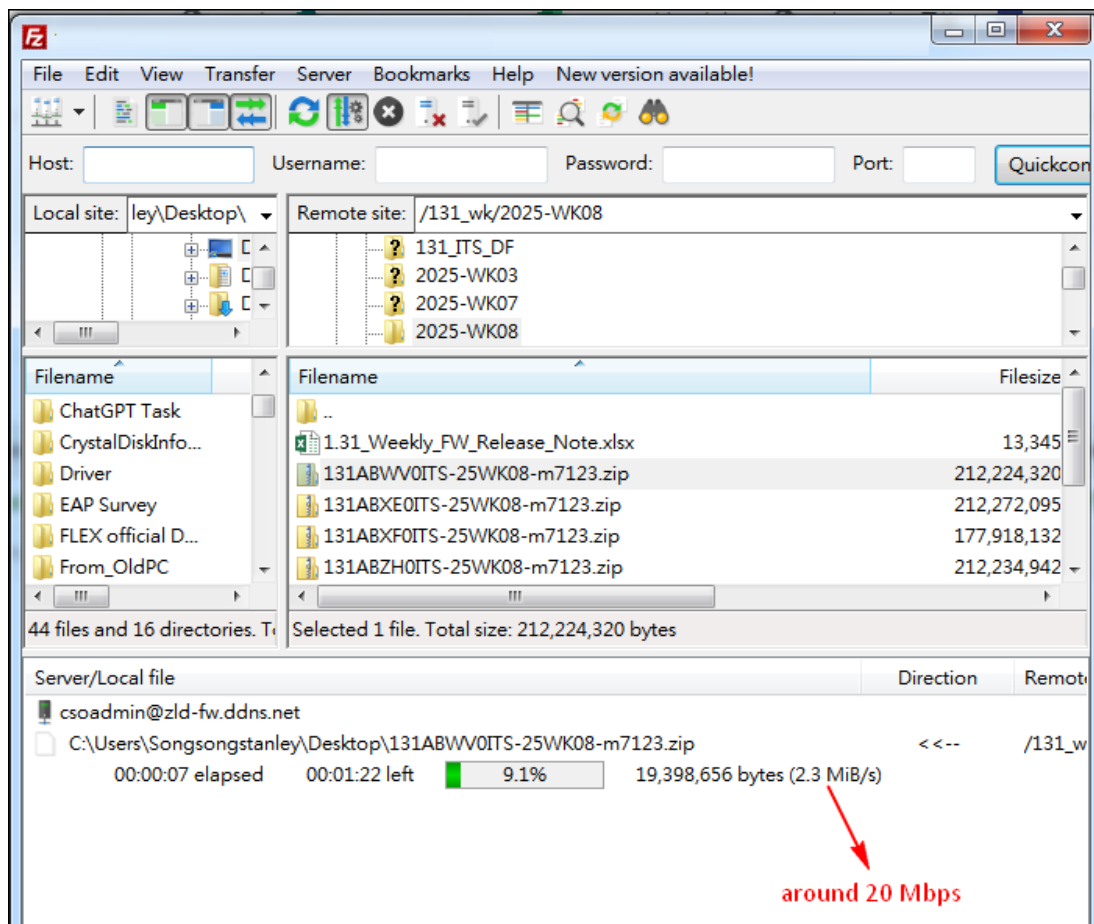
Note: If you select the "Per User" option or configure "User" as a condition, the Captive Portal service must be enabled, and the PC must be authenticated by the firewall first.

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.

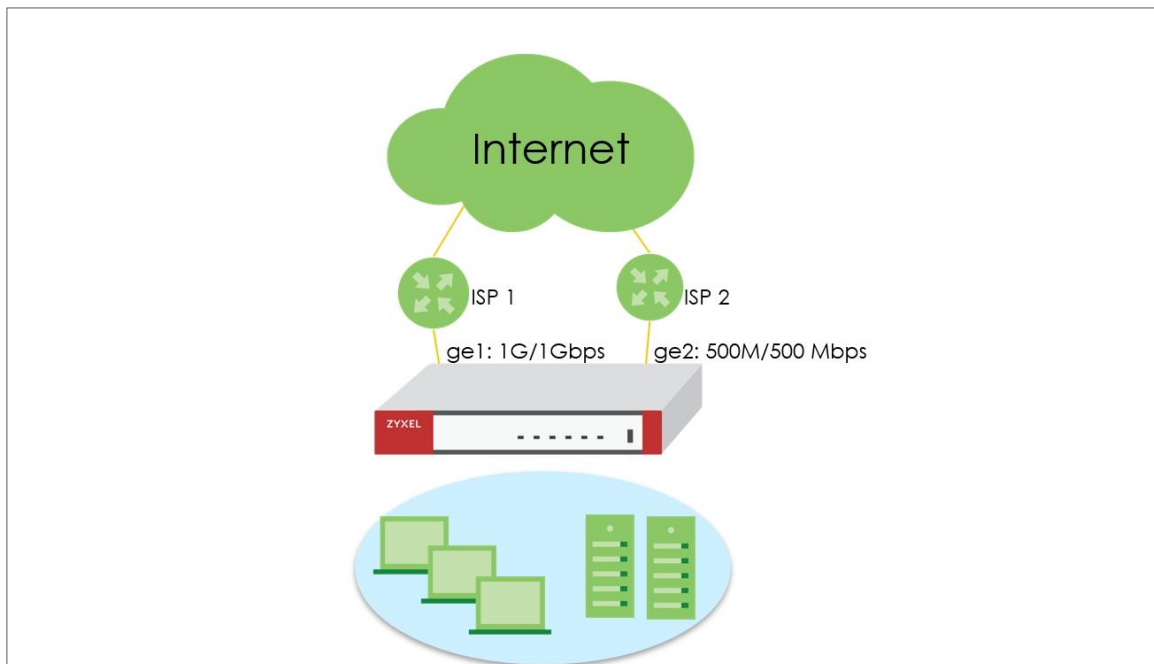


Go to Log & Report > Log/Events and select BWM to check the logs.

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 'Spillover' Trunk configuration with two member interfaces added. The 'Add' button is highlighted with a red box. The table below shows the configuration for the two member interfaces.

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
☐ LLF	llf	ge1, ge2
☐ 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.

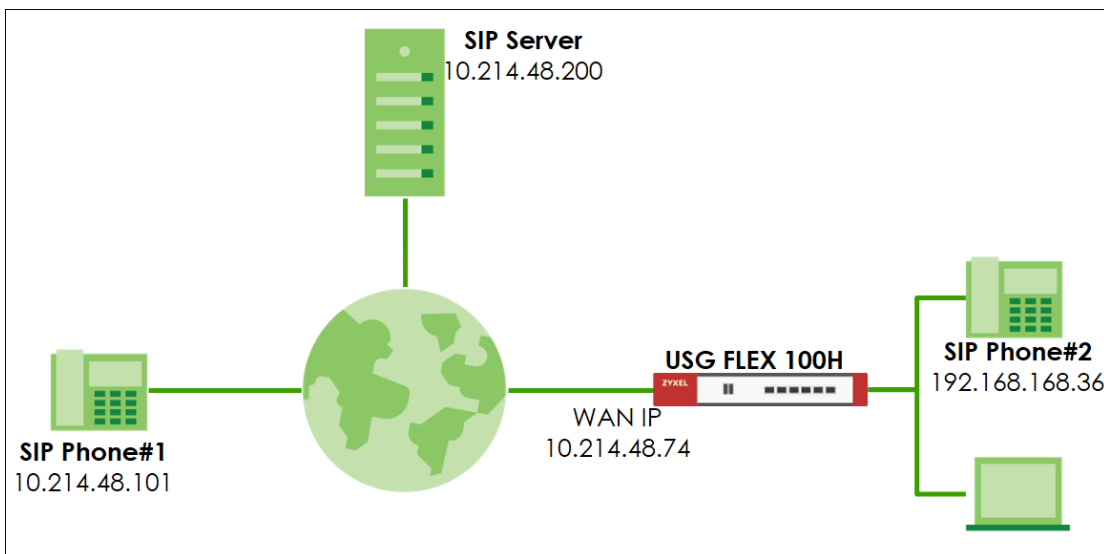
Least Load First

- 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 Pinhole Function Work on USG FLEX H?

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 Pinhole ⓘ

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 ☒

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)

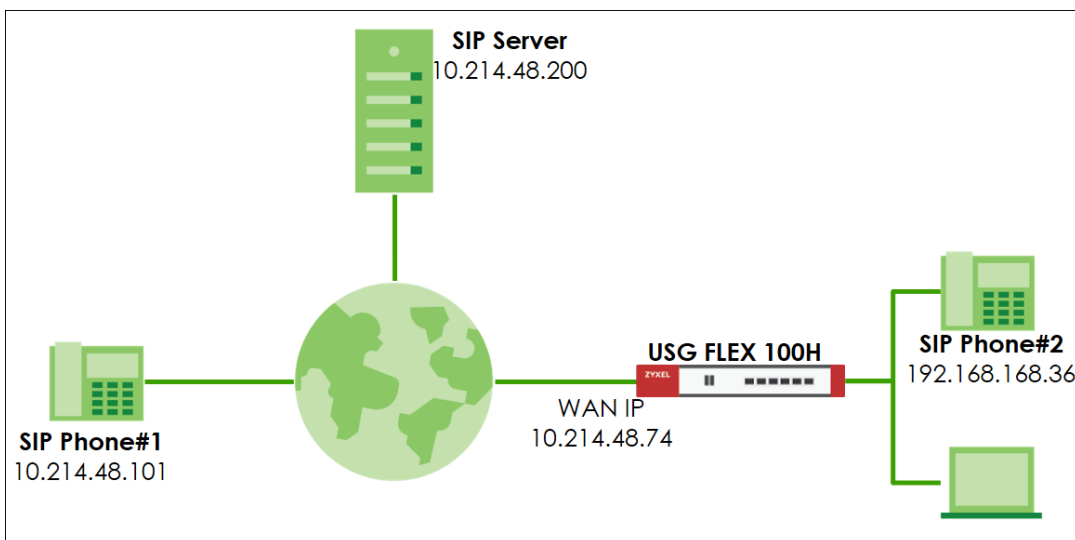
You can configure Media(RTP) and Signaling(SIP) timeout for your SIP phone, it could keep the sessions on firewall to prevent lost incoming phone call due to session expired.

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 Pinhole ⓘ

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 contracks | match "<IP address>"

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

```

usgflex100h> show contracks | 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
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
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>

```

RTP session

SIP session

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

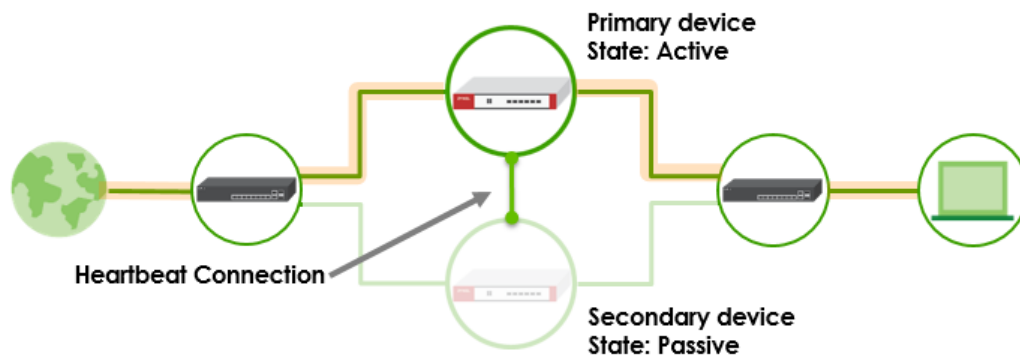
```
usgflex100h> show conntracks | match "192.168.168.36"
udp      17 2999 src=192.168.168.36 dst=10.214.48.200 sport=10002 dport=10254 packets=9513 bytes=1902600
src=10.214.48.200 dst=10.214.48.74 sport=10254 dport=10002 packets=18665 bytes=3733000 [ASSURED] mark=0 helper=RTP use=1
udp      17 2995 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
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
```

RTP Session

SIP Session

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.

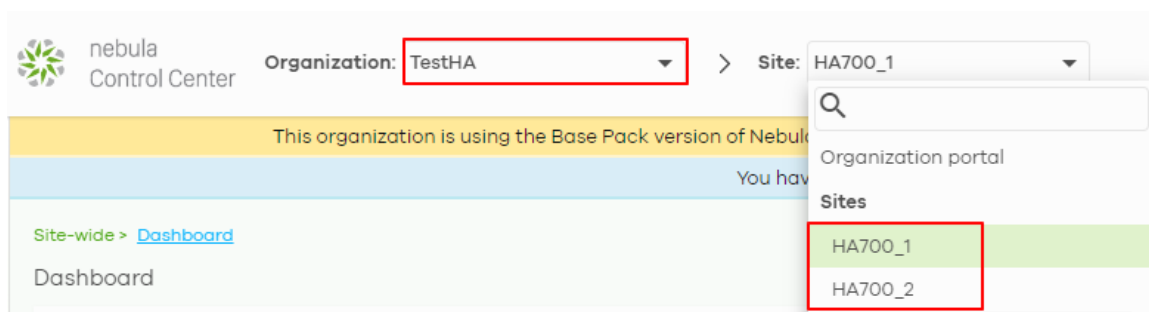


 Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.35).

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

+ Add ✎ Edit ✕ Remove 🔗 Reference 🟢 Active 🔴 Inactive 🟢 Connect 🔴 Disconnect Search insights 🔍 🔍 🔍								
☐ Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
☐ 🟢	ge1	WAN		10.214.48.99/255.255.255.0		Ethernet	p1	3
☐ 🟢	ge2	WAN		0.0.0.0/0.0.0.0		Ethernet	p2	1

Internal

+ Add ✎ Edit ✕ Remove 🔗 Reference 🟢 Active 🔴 Inactive Search insights 🔍 🔍 🔍								
☐ Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
☐ 🟢	ge3	LAN		192.168.168.1/255.255.255.0		Ethernet	p3,p4,p5,p6	2
☐ 🟢	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	☒	
Management Configuration		
Initial Role	☒ Primary (License Controller)	
HA MAC address	☐ Physical MAC address ☒ Virtual MAC address	
	☐ Secondary	
Active Node Management IP	10.10.10.1	
Passive Node Management IP	10.10.10.2	
Management IP Subnet Mask	255.255.255.0	
Monitor Interface		
Member	ge3	
Failover on Monitored Interface Link Down	☒	
Failover on Monitored Connectivity Check Failure	☐	

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)	
	HA MAC address ☐ Physical MAC address ☒ Virtual MAC address	
	☒ Secondary	
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

Enabled

Pairing Status

Paired

Synchronization Status

Last Full Sync Status

Success

Last Full Sync Time

2024-12-25 14:09:39

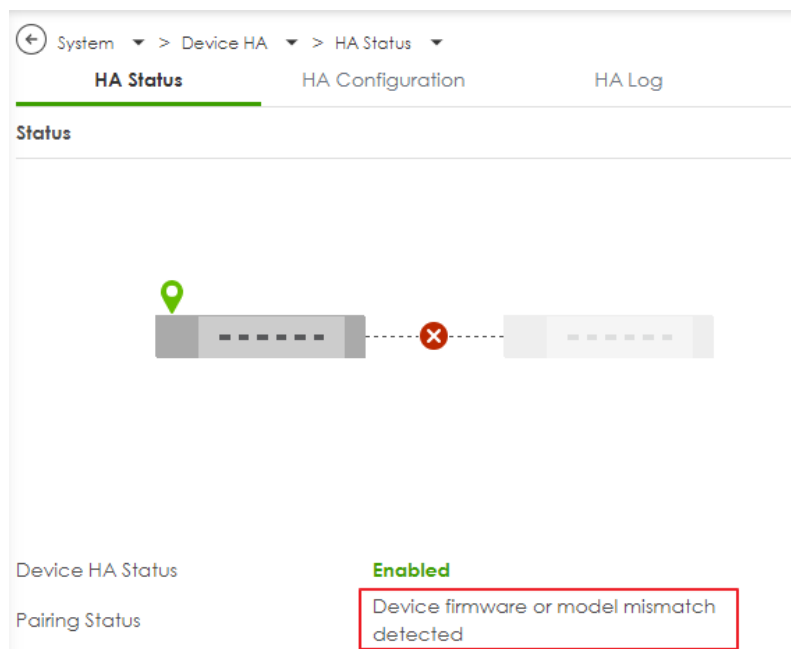
You can also enter the command on the primary device to check HA status.

usgflex200h> show state vrf main device-ha status

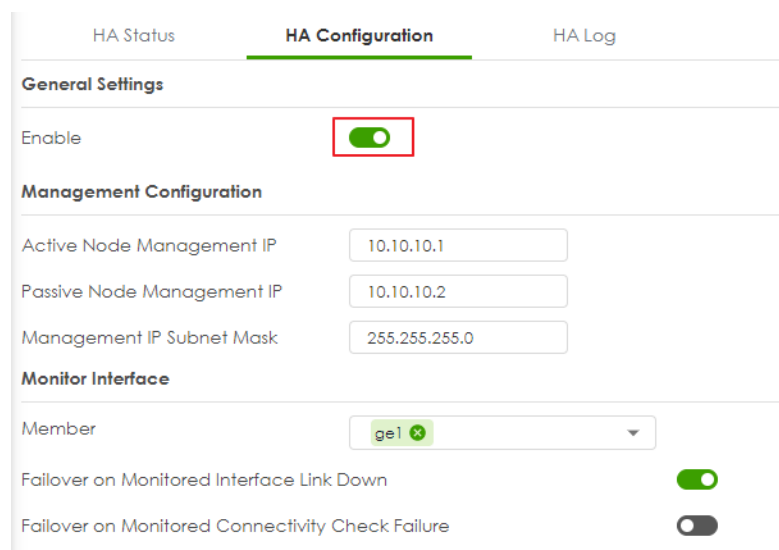
Synchronization can take up to 5 minutes or so. Once it has finished synchronizing, you can verify if the settings are synchronized by accessing the passive device through Passive Node Management IP. Once pairing is complete, the secondary device's license will automatically be transferred to the primary 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 Paring 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.



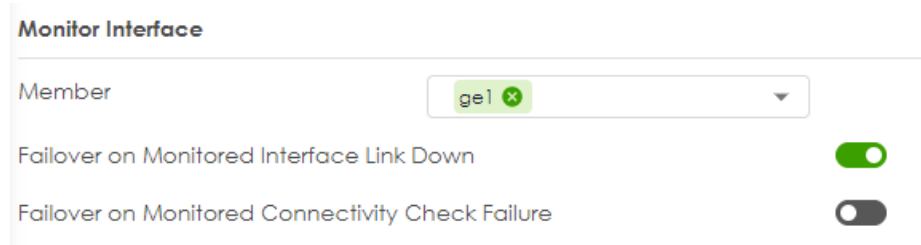
Note: All configuration changes must be made on the active device. Do NOT manually configure the passive device.

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.



The screenshot shows a configuration page titled "Monitor Interface". It contains a "Member" dropdown menu with "ge1" selected and a green "x" icon. Below the dropdown are two toggle switches: "Failover on Monitored Interface Link Down" which is turned on (green), and "Failover on Monitored Connectivity Check Failure" which is turned off (grey).

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.

Not secure https://10.10.10.1/apps/system/deviceha

ZYXEL USG FLEX 200H **Active Node**

System > Device HA > HA Log

HA Log

View Logs

Local	Peer
2024-12-25 14:57:38 Enter Active state.	2024-12-25 14:57:38 Enter Passive state.
2024-12-25 14:57:38 Change to active state : monitor interface link down	2024-12-25 14:57:38 Change to passive state : monitor interface link down
2024-12-25 14:10:53 Synchronize complete.	2024-12-25 14:57:38 Monitor interface ge1 link down detected.
2024-12-25 14:10:53 Synchronize success.	2024-12-25 14:08:57 Enter Active state.
2024-12-25 14:09:39 Start to synchronize with active device.	
2024-12-25 14:08:21 Enter Passive state.	

Refresh

- 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.

System Information 	
Host Name	usgflex200h0325
Serial Number	S212
MAC Address	<u>D8:EC:E5:</u> 1D ~ <u>D8:EC:E5:</u> :24
Firmware	V1.32(ABWV.0)b3 2025-03-19 14:18:15
Uptime	23:52:38
System Time	2025-03-27 16:41:38
Boot Status	OK
Nebula Status	Connected

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	☒ Use Default MAC Address <u>d6:ec:e5:</u> 1d ☐ Overwrite Default MAC Address auto1

Interface Properties

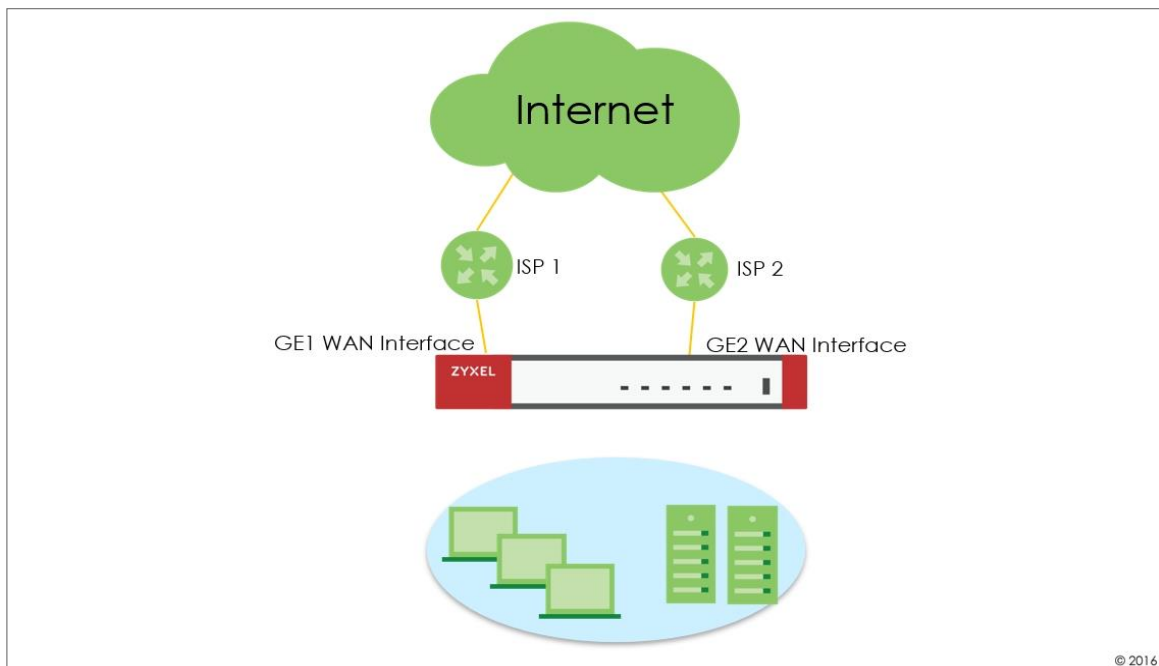
Role	internal
Interface Type	Ethernet
Interface Name	ge3
Port	p3 (ge3) ✕ p4 (ge3) ✕ p5 (ge3) ✕ p6 (ge3) ✕
Zone	LAN
MAC Address	☒ Use Default MAC Address <u>d6:ec:e5:</u> 1f ☐ Overwrite Default MAC Address auto3

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

☐	Status ▾	Name ▾	Destination ▾	Next Hop ▾	Description ▾	Metric ▾
☐		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









☐	Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits
☐		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, len
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, len
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, len
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, len
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, len
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, len
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, len
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, len
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, len
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, len
```

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:

 Note:

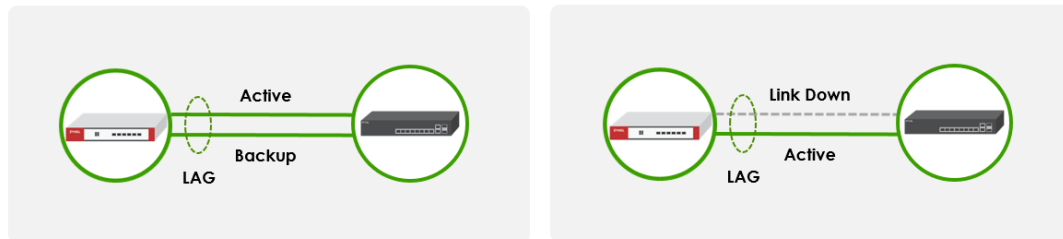
- LAG support interface Role: **External, Internal** and **General**
- When the interface role is external, the LAG IP address does not support PPPoE or PPPoE with a static IP

3. Select the LAG mode

Name	LAG-ge-5-6	
Zone	LAN	
MAC Address	☒ Use Default MAC Address ☐ Overwrite Default MAC Address	
Description		
Address Assignment	☐ Unassigned ☒ Use Fixed IP Address IP/Network Mask 172.198.1.1/24	
Secondary IP	+ Add  Remove ☐ IP/Netmask  No data	
Members 	ge5 ge6	
Mode	static active-backup lacp (802.3ad)	
Mii Monitoring Interval	(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

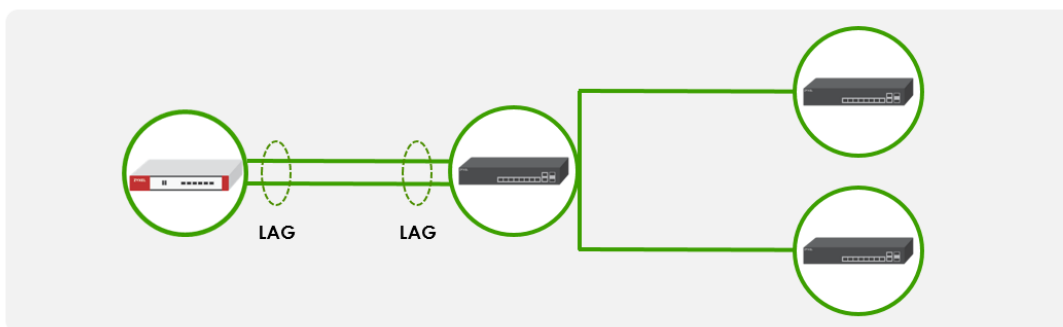
Primary: Allows you to specify which member interface should be preferred as the active link

Members i	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.

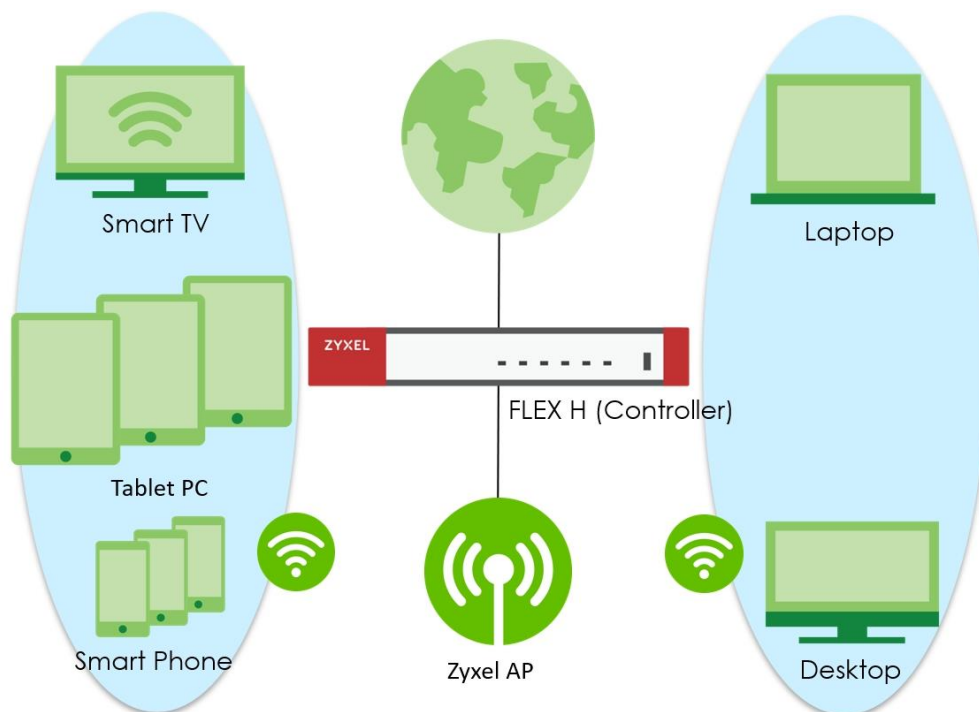
Members 	ge5  ge6 	
Mode	static ▼	
Mii Monitoring Interval	100	(1-1000)ms
Transmit Hash Policy	src-dst-ip-mac ▼	

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.

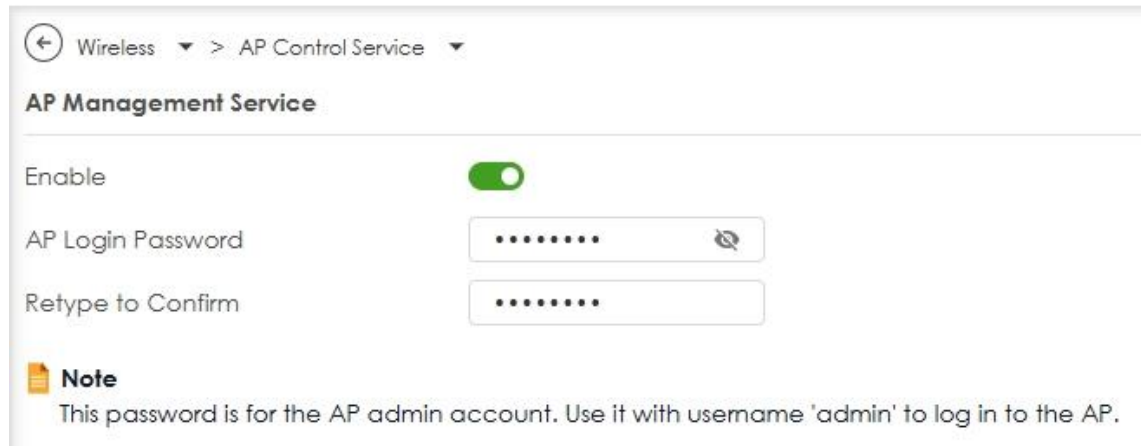


 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).

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

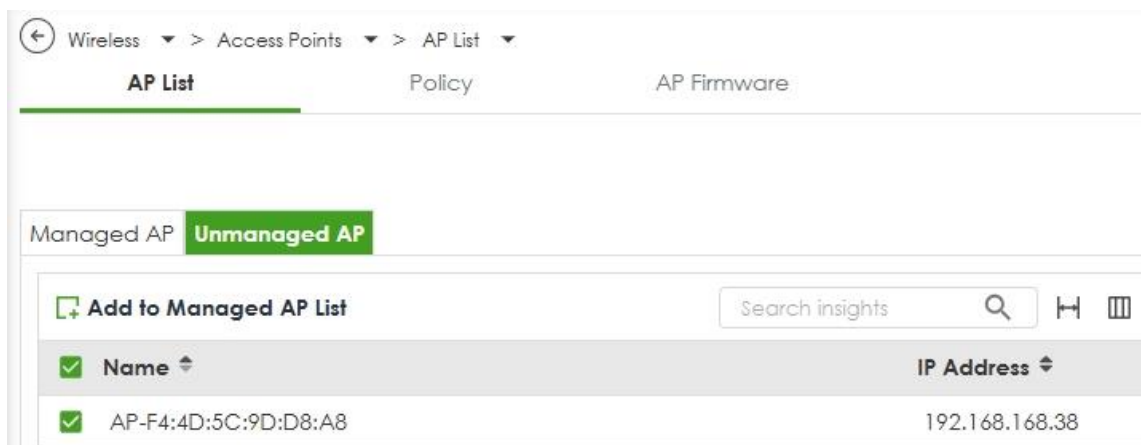
Retype to Confirm

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

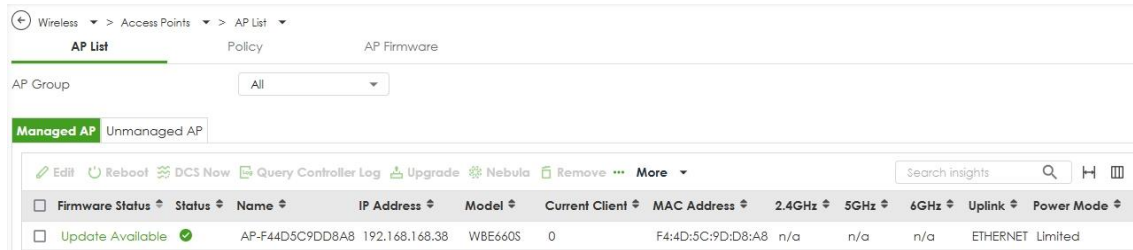
Managed AP **Unmanaged AP**

[Add to Managed AP List](#)

Name	IP Address
☒ 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



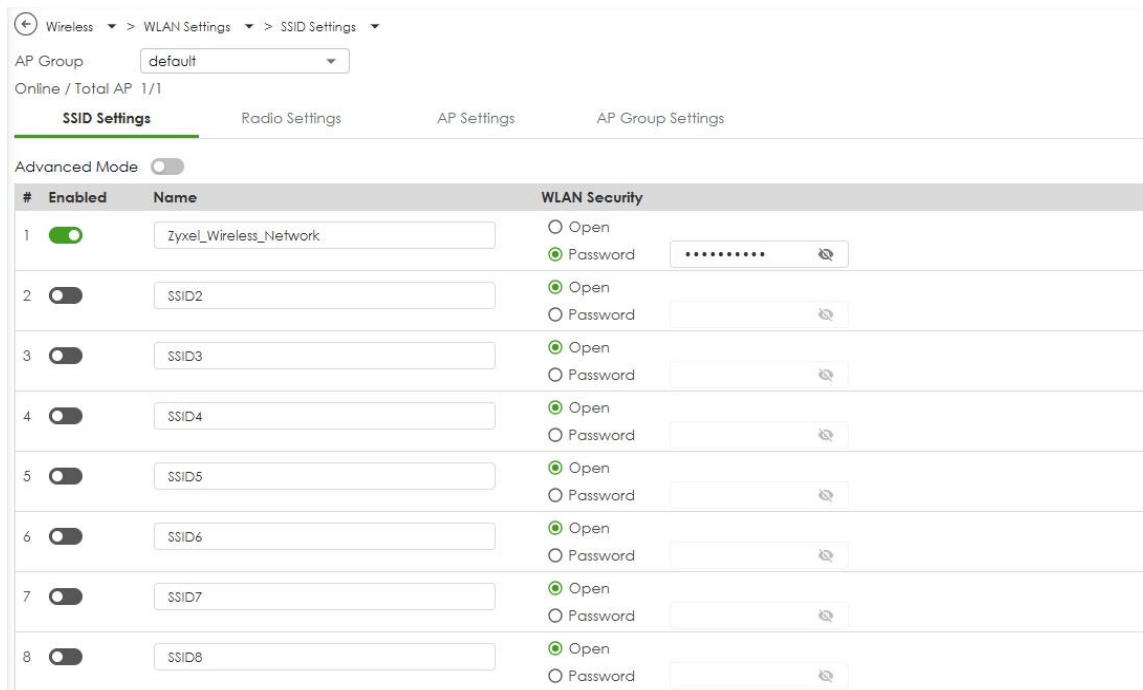
The screenshot shows the 'Managed AP' tab in the 'AP List' section. It includes a table with columns for Firmware Status, Status, Name, IP Address, Model, Current Client, MAC Address, 2.4GHz, 5GHz, 6GHz, Uplink, and Power Mode. A single entry is visible with status 'Update Available' and a green checkmark.

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



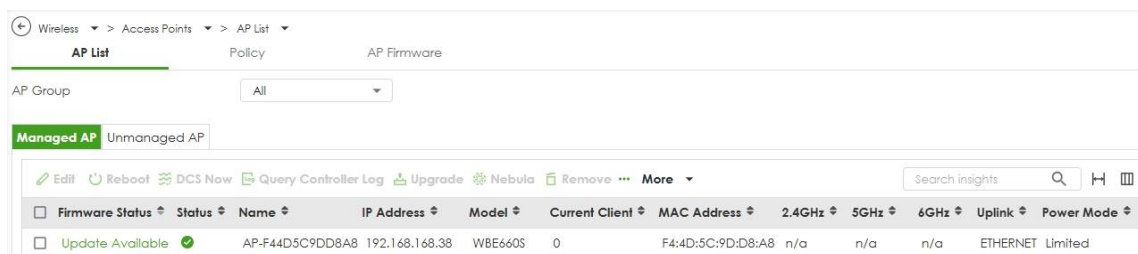
The screenshot shows the 'SSID Settings' page with a table for configuring SSIDs. It includes columns for #, Enabled, Name, and WLAN Security. The first SSID is 'ZyXel_Wireless_Network' and is enabled. The other SSIDs are labeled 'SSID2' through 'SSID8' and are disabled.

#	Enabled	Name	WLAN Security
1	☒	ZyXel_Wireless_Network	☐ Open ☒ Password
2	☐	SSID2	☒ Open ☐ Password
3	☐	SSID3	☒ Open ☐ Password
4	☐	SSID4	☒ Open ☐ Password
5	☐	SSID5	☒ Open ☐ Password
6	☐	SSID6	☒ Open ☐ Password
7	☐	SSID7	☒ Open ☐ Password
8	☐	SSID8	☒ Open ☐ Password

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



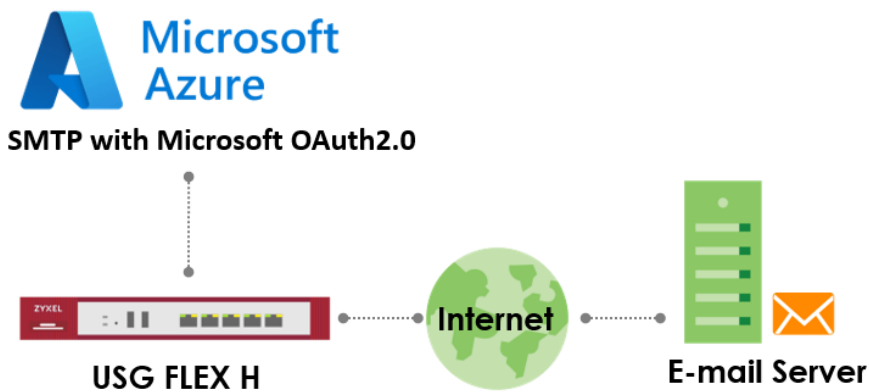
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2025-03-26 17:17:25	Wlan Station Info	STA connected, MAC:E0:D0:45:6B:3F:69, AP:AP-F44D5C9DD8A8, interface:wlan-2-1, SSID: ZyXel_Wireless_Network, Signal: -20dBm	0.0.0.0	0.0.0.0	0	

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	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: 27cba1b2-4a02-463a-969b-893384237a82	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: 52960d2c-971d-409b-a6d3-5d714087f423	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: d44c31fd-3801-477a-9337-475a436895a8	Managed application in L...	: SMTP
Supported account types	: My organization only		

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-af5f-7e6d5c4b3a21

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 have been granted to other applications. [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 Networks

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 Server

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 have been granted to other applications. [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 Networks

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, 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

To view and manage consented permissions for individual users, go to the [Users](#) blade.

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 the state of the application.
User.Read	Delegated	Sign in users.

To view and manage consented permissions for individual users, go to the [Users](#) page.

Request API permissions

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

SMTP

SMTP (1)

SMTP.Send
Send emails from mailboxes using SMTP AUTH.

[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 ↑

[Add a user](#) [Multi-factor authentication](#)

Account Devices Licenses and apps **Mail** OneDrive

Mailbox storage

Learn more about mailbox storage quotas

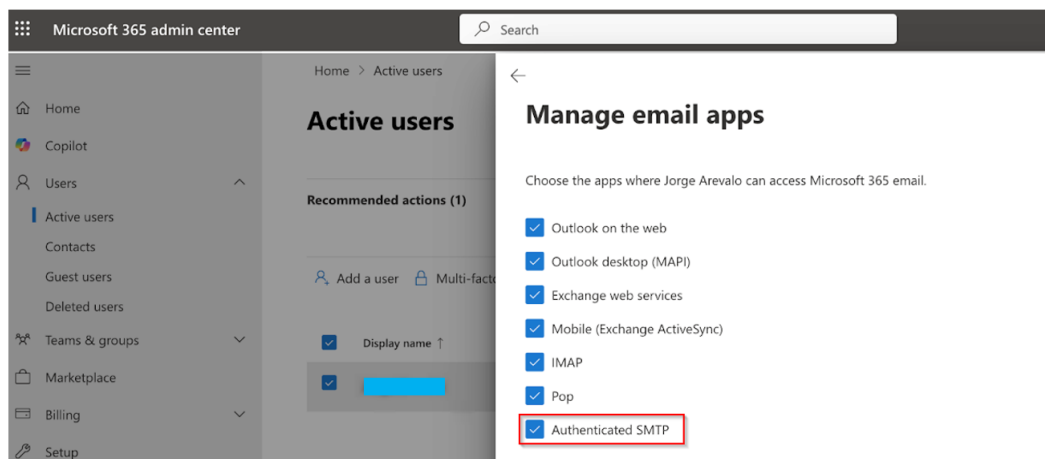
Mailbox permissions

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.

The screenshot shows the 'Mail Server' configuration page in the Zyxel management interface. The 'General Settings' section is active. The 'Mail Server' field is set to 'smtp.office365.com' (Outgoing SMTP Server Name or IP Address). The 'Port' is '587' (1-65535). 'TLS Security' is enabled. 'STARTTLS' is also enabled. 'Authenticate Server' is disabled. The 'Authentication Method' is set to 'Microsoft OAuth2.0'. A red box highlights the 'Sender Email Address' field, which contains 'jeff.lin@zyxel.com.tw'. Below it, the 'Client ID' is '27cba1b2-fad2-4c0a-9ee9-d9f3d4423ba8', the 'Client Secret' is masked with dots, and the 'Tenant ID' is 'd44c31fd-3401-417a-f157-d70e4ba78ba6'. The 'Token Status' is 'No token available – click "Get New Token"'. There are two buttons: 'Get New Token' and 'Refresh Token Status'. Below the 'Default Sender and Recipient' section, there is a 'Recipient' field with 'Email Address' and a 'Send Test Email' button.

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-f0e7-8f3d9423ba82

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-f0e7-8f3d9423ba82

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

Append system name
Append date time

Email from

Recipients

Send Report Now

Reset counters after sending report successfully.

Report Items

System Resource Usage

CPU Usage
Memory Usage

Traffic Statistics

Application Usage
Interface Usage
Port Usage
Session Usage

Security Services

Anti-Malware
Content Filtering
IPS
Reputation Filter
Sandbox

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.0j4) 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:

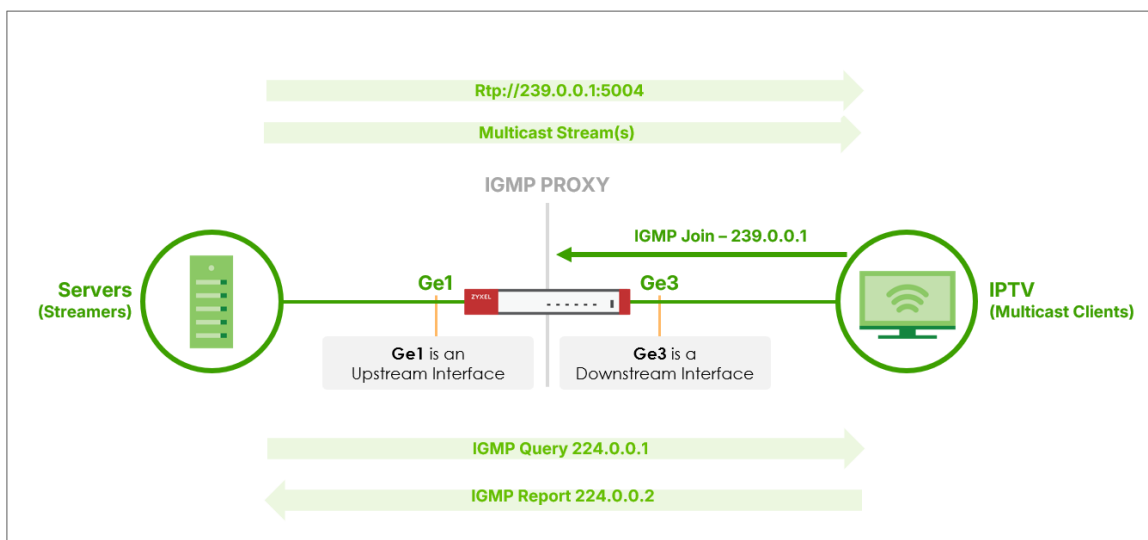
- o Verify all steps were completed correctly
- o Check Microsoft Entra ID audit logs for authentication errors
- o Contact your system administrator for Azure access issues
- o Refer to Microsoft's official OAuth 2.0 documentation

For technical support with your gateway device, contact our support team with your configuration details (never share client secrets).

How to Configure IGMP Proxy

In modern enterprise network environments, applications such as video streaming, IPTV, video conferencing, and multimedia broadcasting have become essential components of daily operations. This type of traffic, based on multicast technology, offers greater bandwidth efficiency compared to traditional unicast transmission. However, without proper management and control, multicast traffic can impose unnecessary load on the network, potentially affecting overall performance and user experience.

The Internet Group Management Protocol (IGMP) is a core mechanism of multicast technology, responsible for managing multicast group memberships between hosts and upstream routing devices. With IGMP, network devices can effectively determine which endpoints need to receive specific multicast streams, ensuring that the corresponding traffic is forwarded only to the necessary segments of the network. When properly configured, IGMP can significantly reduce bandwidth consumption in large-scale network environments, prevent unnecessary broadcasting, and help maintain the stability of multicast-based services.

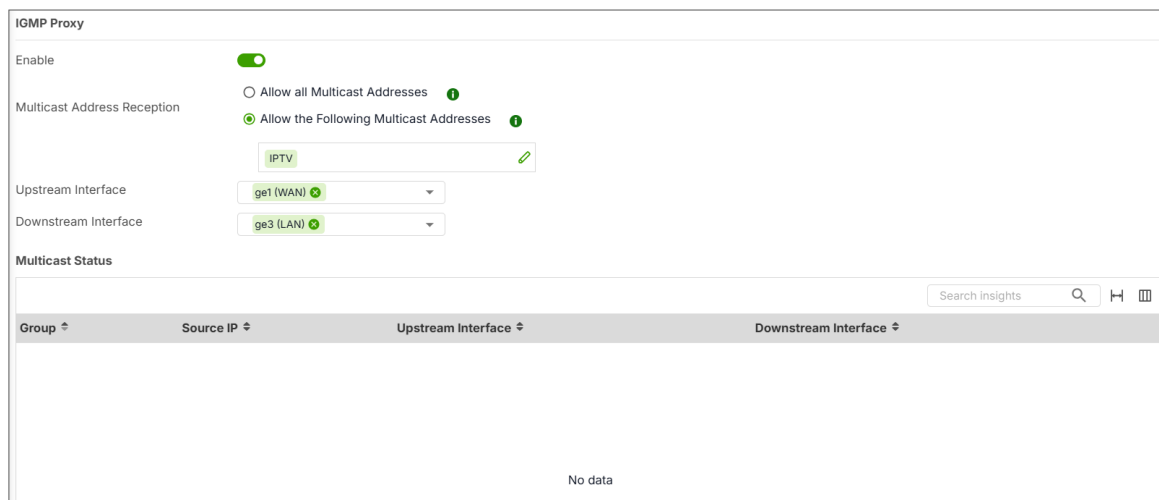


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.36).

Enable the IGMP Proxy for Downstream and Upstream Interface

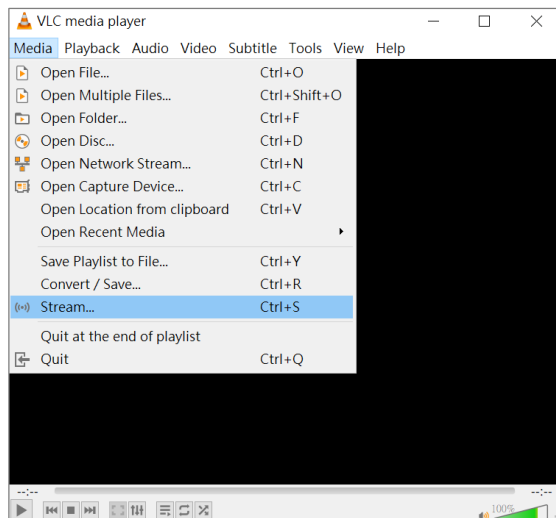
Go to "Network > Multicast" and enable IGMP Proxy. Select "Allow the Following Multicast Addresses". Create an address object for the IPTV client, and select this client.

Set the Upstream Interface to ge1 (the WAN interface), and the Downstream Interface to ge3 (the LAN interface). In this guide, we restrict multicast traffic to the IPTV client only, in order to minimize the impact on overall network performance.

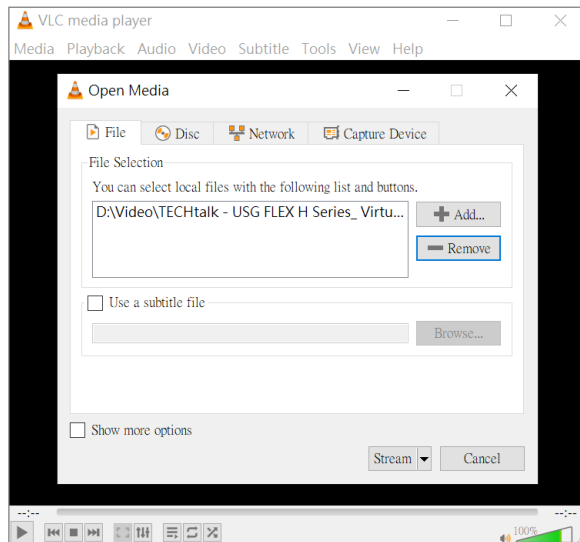


Set Up Streamer Server Using VLC software

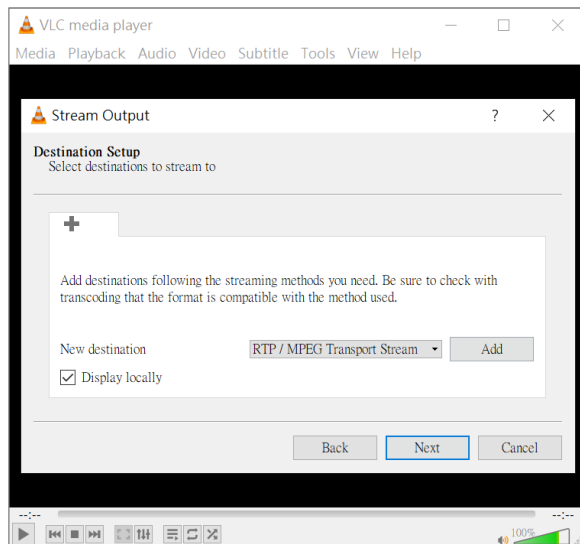
Open Medial Player, and Select "Stream"



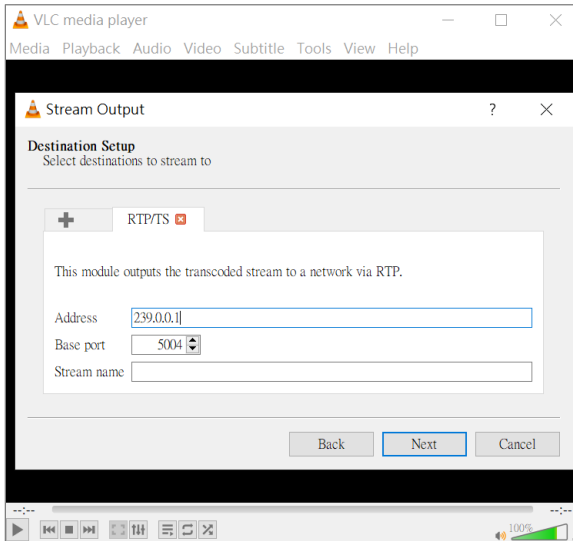
Add a video file and click on "Stream" button.



In Destination Setup section, select stream methods, then add new destination.

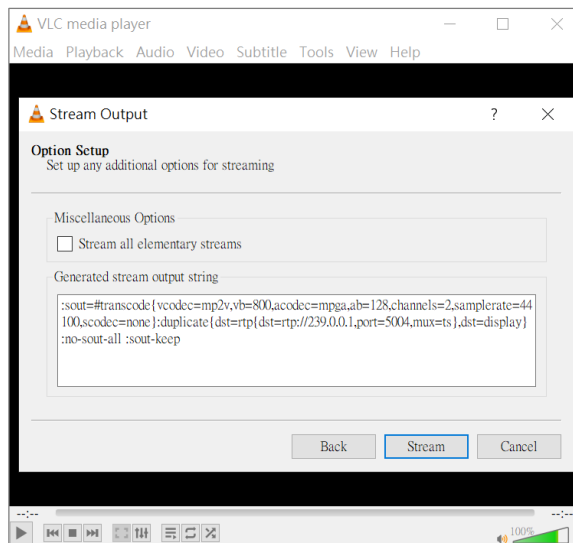


Configure IP address and port number of IGMP group.



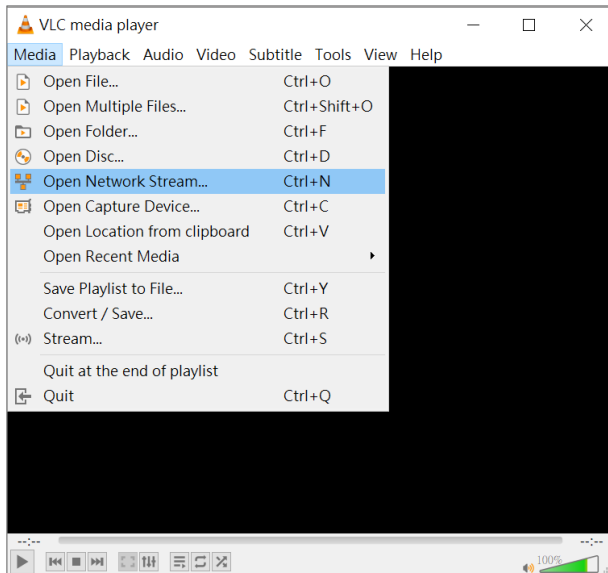
Click Next to complete the setup process

After clicking on "Stream", VLC will start outputting the video.

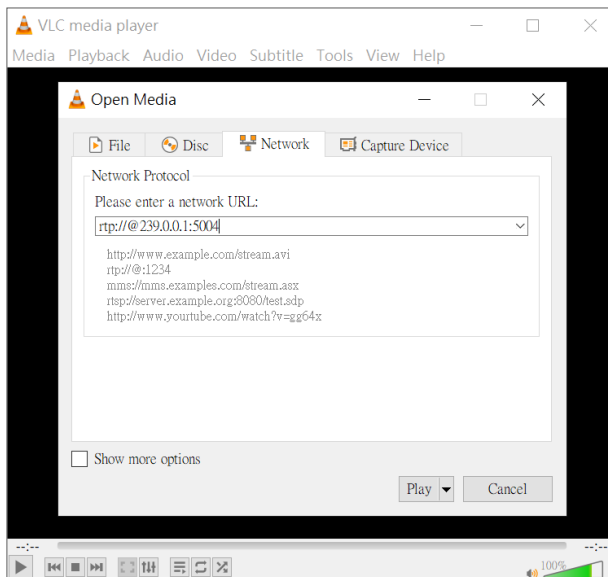


Set Up Player Client Using VLC software

Open Media Player, and select "Open Network Stream".



Fill in the IP address of IGMP group with port number, then press "Play".



We can now see the stream playing on the client.



Test the Result

After IPTV client join the multicast group, we can monitor the status on Multicast table.

IGMP Proxy

Enable

Multicast Address Reception

Allow all Multicast Addresses

Allow the Following Multicast Addresses

IPTV

Upstream Interface

ge1 (WAN)

Downstream Interface

ge3 (LAN)

Multicast Status

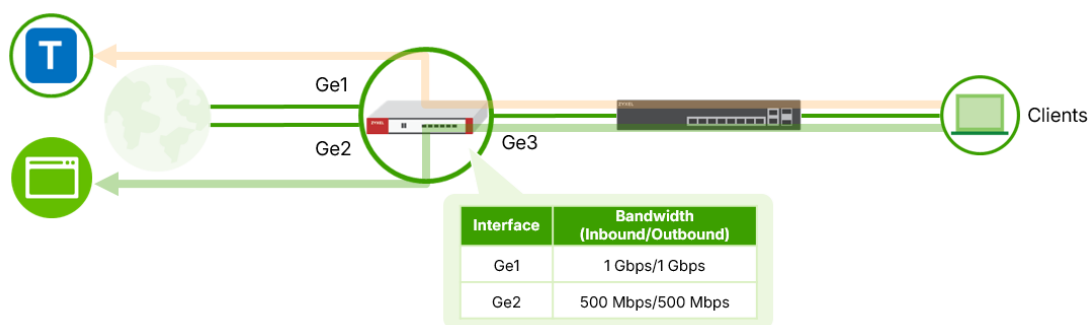
Search insights

Group	Source IP	Upstream Interface	Downstream Interface
239.0.0.1	172.24.125.45	ge1	ge3
239.255.255.250	172.24.125.45	ge1	ge3
239.255.255.250	192.168.168.34	ge1	ge3

How to Configure Application-Based Policy Route

USG FLEX H series supports configuring Application-Based Policy Routing. You can use the application as the matching criterion in a policy route to control traffic forwarding behavior based on the detected application, allowing traffic to be routed through a specific WAN interface according to application type. There is a total of 28 categories (at the time of writing) supported in the application service type.

Here is an example where Internet users want to access the Teams application behind the USG FLEX H, and the traffic is routed through a specific WAN interface based on application-based policy routing.



In the USG Flex H, go to Network > Routing > Policy Route > Add a Policy Route rule. Configure a Name for you to identify the Policy Router rule, such as "Teams_ge1". Set up the Criteria for the user, incoming interface, source/destination address, and select the Service Type as Application.

← Network > Routing > Policy Route

Configuration

Enable ☒

Name

Description

Criteria

User

Incoming

Please select one member

Source Address

Destination Address

DSCP Code

Schedule

Service Type ☐ Service Object ☒ Application

Application

❗ This field is required.

Source Port

Click the Application drop-down list to display the available application options, and tick the desired application.

Service Type ☐ Service Object ☒ Application

Application

Source Port

Next Hop

Type

DSCP Marking

DSCP Marking

Address Translation

SNAT Address

Advanced Settings ▾

Search

- ☐ iCloud
- ☐ Instagram
- ☐ iQIYI
- ☐ iTunes
- ☐ Netflix
- ☐ Microsoft OneDrive
- ☐ Spotify
- ☒ Microsoft teams
- ☒ Microsoft teams
- ☒ Teamspeak v2
- ☒ TeamSpeak v3
- ☐ Vimeo
- ☐ Xbox

Configure the ge1 interface as the Next-Hop, and select the SNAT address.

Service Type

☐ Service Object
 ☒ Application

Application

Microsoft teams, Teamspeak v2, TeamSpeak v3

Source Port

any

Next Hop

Type

Interface

Interface

ge1

DSCP Marking

DSCP Marking

preserve

Address Translation

SNAT Address

outgoing-interface

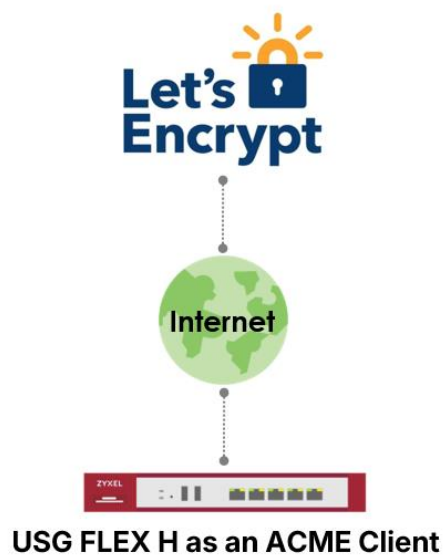
Test the result

Access the Teams application from a LAN host to verify that the traffic is routed to the interface. If the traffic hits the criteria and is being routed according to the rule, you will see the hit count of the policy route.

Policy Route													
Configuration													
+ Add ✎ Edit 🗑 Remove 🟢 Active 🔴 Inactive 🔄 Move to 🔄 Refresh Search insights													
Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits
☒	1	any	none	ge3	LANL_SUBNET	any	any	Microsoft teams, Teamspeak v2 + 1	any	ge1	preserve	outgoing-interface	59

How to Configure ACME client for Let's Encrypt

As an ACME (Automatic Certificate Management Environment) client, the USG FLEX H firewall can automatically renew certificates issued by Let's Encrypt on a regular basis. Users can use either the HTTP-01 or DNS-01 (Cloudflare) challenge method to validate domain ownership. This example demonstrates how the USG FLEX H firewall renews a certificate using Let's Encrypt.



Note: This feature is supported from firmware version uOS 1.39.

The USG FLEX H firewall supports both HTTP-01 and DNS-01 (Cloudflare) challenge methods. Users can choose either method to configure and renew a Let's Encrypt certificate.

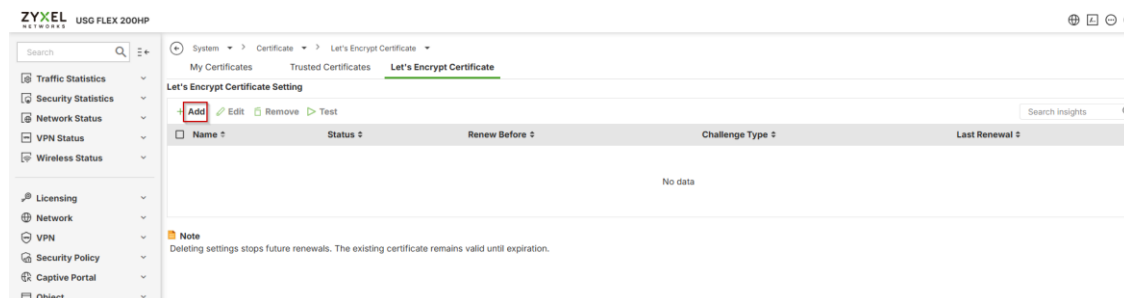
Method 1: HTTP-01 challenge method

HTTP-01 challenge method pre-requisites:

This WAN interface must be configured with a public IP address. The system will automatically open Port 80 temporarily during validation and close it automatically once completed. If the firewall is deployed behind an upstream NAT router, you must manually configure Port Forwarding (Port 80) on that router. DNS-01 is highly recommended for NAT environments.

Configure Let's Encrypt Certificate using HTTP-01 challenge method:

7. Navigate to System > Certificate > Let's Encrypt Certificate > Let's Encrypt Certificate Settings and click +Add to add a profile.



8. Enter the Domain Name, Email, and Renew Before Expiry fields, then save it.
 - Domain Name: A domain name that resolves to the firewall's WAN IP address.
 - Email: The domain name owner's email address.
 - Renew Before Expiry: The number of days before the certificate expires that it will be automatically renewed.
 - Challenge Type: Select HTTP-01.
 - P.S. To complete HTTP-01 validation, the device temporarily redirects WAN port 80 traffic for approximately 2–3 minutes (up to 5 minutes maximum). All required

firewall policy changes are applied and reverted automatically. To minimize potential service impact, perform validation during off-peak hours.

ZYXEL NETWORKS USG FLEX 200HP

System > Certificate > Let's Encrypt Certificate

Automatically provision and renew free SSL/TLS certificates with Let's Encrypt using the ACME protocol. This is the simplest way to secure your services with minimal maintenance. Learn more about [Let's Encrypt](#).

General Settings

Domain Name:

Email:

Renew Before Expiry: days (1-60)

Subject Alternative Name (SAN) ⚠ Changing SAN entries requires certificate re-issuance.

+ Add - Remove

☐ SAN

No data

Challenge Configuration

Challenge Type:

Renew Time:

⚠ To complete HTTP-01 validation, the device temporarily redirects WAN port 80 traffic for approximately 2-3 minutes (up to 5 minutes maximum). All required firewall policy changes are applied and reverted automatically. To minimize potential service impact, perform validation during off-peak hours.

⚠ When you click Apply, you're acknowledging and agreeing to the [Let's Encrypt subscriber agreement](#).

9. Select "Validate and Issue Now," then click "Continue."

Certificate Issuance Options

Choose how to validate and issue the Let's Encrypt certificate.

- ☒ Validate and Issue Now
- ☐ Validate Now, Issue at Renew Time
- ☐ Issue at Renew Time

⚠ During validation and certificate issuance, WAN port 80 traffic may be temporarily redirected for approximately 2-3 minutes (up to 5 minutes).

Cancel

Continue

10. Ensure that the Dry Run validation test is successful.

Dry Run- Validation Test

```

success
[2026-07-06 16:49:09] [INFO] [STEP-3] Checking authorization
status
[2026-07-06 16:49:18] [INFO] [STEP-3] Check authorization
success
[2026-07-06 16:49:24] [INFO] [STEP-4] certificate written
[2026-07-06 16:49:24] [INFO] [STEP-4] zyxelacme.duckdns.org:
dryrun verified successfully.
[2026-07-06 16:49:24] [INFO] [STEP-5] zyxelacme.duckdns.org:
triggering cleanup due to success.
[2026-07-06 16:49:24] [INFO] [STEP-5] Successfully remove
temporary firewall rule.
[2026-07-06 16:49:24] [INFO] [STATUS] zyxelacme.duckdns.org:
Script finished. Result: SUCCESS.
  
```

[Download Log](#) [Finish](#)

11. The configuration is created successfully. Verify that the status is "Valid".

System > Certificate > Let's Encrypt Certificate

My Certificates Trusted Certificates **Let's Encrypt Certificate**

Let's Encrypt Certificate Setting

+ Add Edit Remove Test

Name	Status	Renew Before	Challenge Type	Last Renewal
zyxelacme.duckdns.org	Valid	30	HTTP-01	2026-07-06 16:49

Note
Deleting settings stops future renewals. The existing certificate remains valid until expiration.

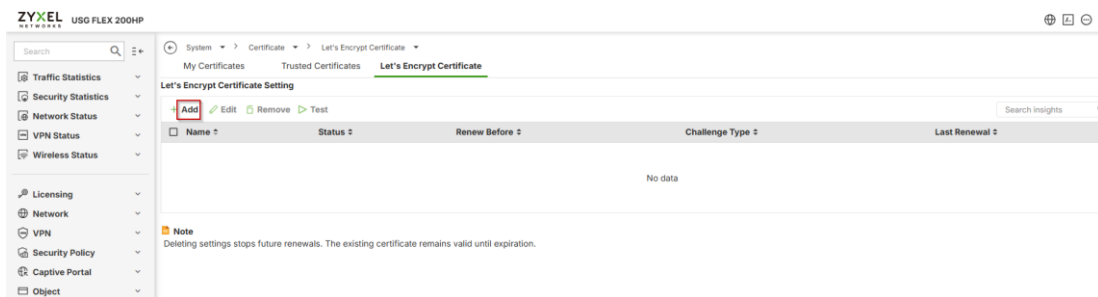
Method 2: DN-01 challenge method

DNS-01 challenge method pre-requisites:

This method currently supports only domains managed by Cloudflare. Please provide a Cloudflare API Token with DNS permission for your domain. This method does not require any inbound firewall ports and is ideal for devices deployed behind NAT.

Configure Let's Encrypt Certificate using DNS-01(Cloudflare) challenge method:

1. Navigate to System > Certificate > Let's Encrypt Certificate > Let's Encrypt Certificate Settings and click +Add to add a profile.



2. Enter the Domain Name, Email, and Renew Before Expiry fields, then save it.
 - Domain Name: A domain name that resolves to the firewall's WAN IP address.
 - Email: The domain name owner's email address.
 - Renew Before Expiry: The number of days before the certificate expires that it will be automatically renewed.
 - Challenge Type: Select DNS-01 (Cloudflare).
 - Cloudflare Zone ID : Paste the Zone ID from Cloudflare.
 - Cloudflare API Token : Paste the API token from Cloudflare.

ZYXEL USG FLEX 200HP

Search

- VPN Status
- Wireless Status
- Licensing
- Network
- VPN
- Security Policy
- Captive Portal
- Object
- Security Services
- User & Authentication
- Wireless
- System**
 - Settings
 - Device HA
 - DNS & DDNS
 - SNMP
 - Notification
 - Certificate
 - Advanced
 - External Integrations
 - Log & Report
 - Maintenance

System > Certificate > Let's Encrypt Certificate

Automatically provision and renew free SSL/TLS certificates with Let's Encrypt using the ACME protocol. This is the simplest way to secure your services with minimal maintenance. Learn more about [Let's Encrypt](#).

General Settings

Domain Name:

Email:

Renew Before Expiry: days (1-60)

Subject Alternative Name (SAN) ⚠ Changing SAN entries requires certificate re-issuance.

+ Add - Remove

☐ SAN

No data

Challenge Configuration

Challenge Type:

Cloudflare Zone ID:

Cloudflare API Token: [How to create a token?](#)

⚠ When you click Apply, you're acknowledging and agreeing to the [Let's Encrypt subscriber agreement](#).

3. The configuration is created successfully. Verify that the status is "Valid".

System > Certificate > Let's Encrypt Certificate

My Certificates Trusted Certificates Let's Encrypt Certificate

Let's Encrypt Certificate Setting

+ Add Edit Remove Test

Name	Status	Renew Before	Challenge	Last Renewal
☐ acmetests.com	Valid	30 Days	DNS-01 (Cloudflare)	2026-07-22 18:09

Note
Deleting settings stops future renewals. The existing certificate remains valid until expiration.

The Zone ID from Cloudflare

Quick search... Ctrl K

Back to Domains

Overview

- Recents
- AI Crawl Control
- Investigate
- Analytics
- DNS
- Email
- SSL/TLS
- Security

Client-side security

Ensure the safety and privacy of your visitors by monitoring third-party scripts, connections, and cookies loaded in web browsers.

Bot Fight Mode

Challenge known bots that may carry out attacks. Defend against threats like content scraping, click fraud, and credential stuffing by challenging simple bots with known traffic signatures.

Leaked credentials mitigation [Activate](#)

Turn on leaked credentials detection and deploy a rate limiting rule to meter the number of requests from IP addresses attempting to use leaked or stolen passwords for 10 seconds.

Support Resources

- [Documentation](#)
- [Community](#)

API

Zone ID: **8ed0da222a35ce9102b4f948b29...**

Account ID: 6a44d75d7f8794d573322f3a8...

[Get your API token](#)

[API documentation](#)

Create the API token from Cloudflare.

My Profile

Quick search... Ctrl K

- Settings
- Access Management
- API Tokens

[Back to view all tokens](#)

Create Token

Token name: [Edit zone DNS](#)

Permissions

Select edit or read permissions to apply to your accounts or websites for this token.

Zone DNS Edit

[+ Add more](#)

Zone Resources

Select zones to include or exclude.

Include Specific zone acmetests.com

[+ Add more](#)

The API token is created.

My Profile

Quick search... Ctrl K

- Settings
- Access Management
- API Tokens

Edit zone DNS API token was successfully created

Copy this token to access the Cloudflare API. For security this will not be shown again. [Learn more](#)

Test this token

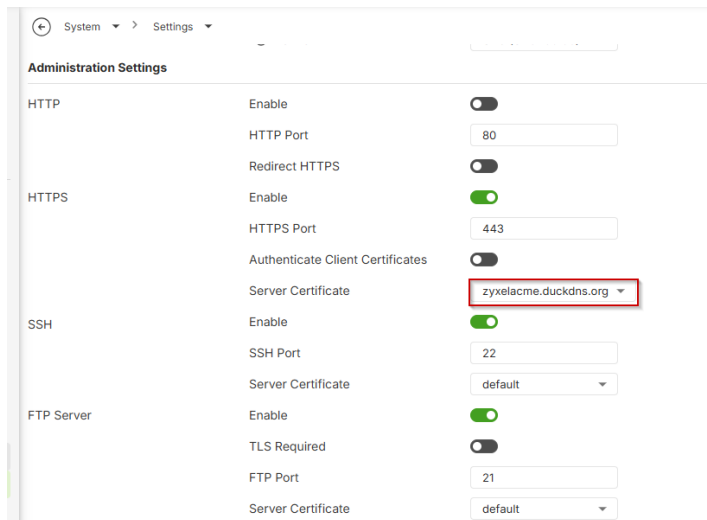
To confirm your token is working correctly, copy and paste the below CURL command in a terminal shell to test.

```
curl "https://api.cloudflare.com/client/v4/user/tokens/verify" \
-H "Authorization: Bearer cfFuT_uor0gKNSR71drc22W1dqf8IHRKUVk2qF5Uecc9679F8"
```

[View all API tokens](#)

Test the Result

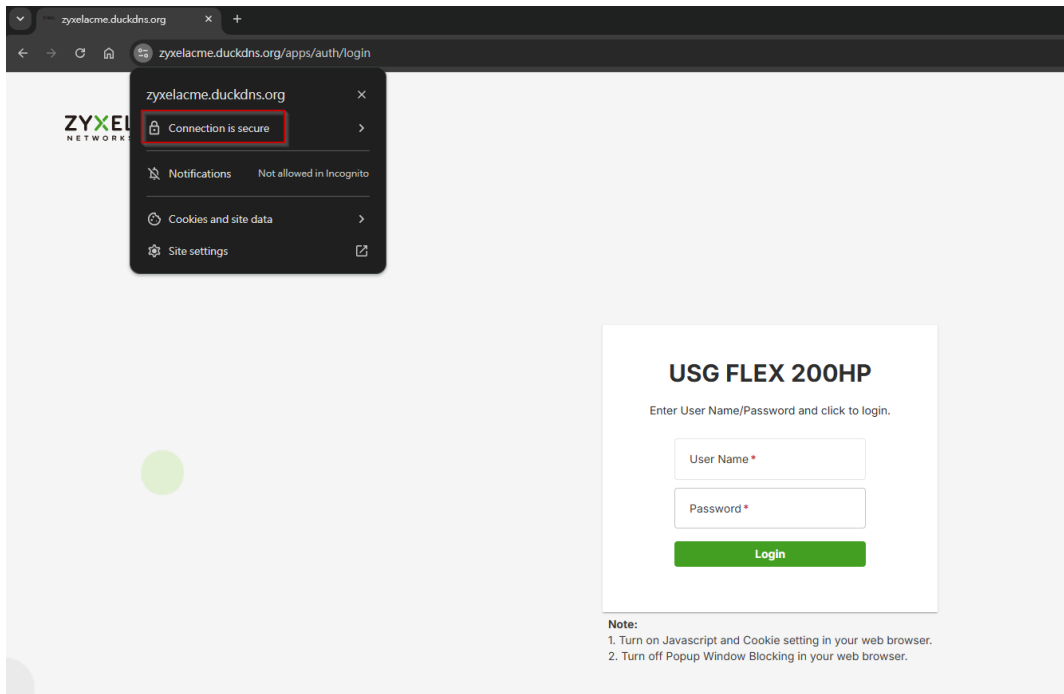
4. Navigate to System > Settings > Administration Settings > HTTPS > Server Certificate > Select the Let's Encrypt certificate.



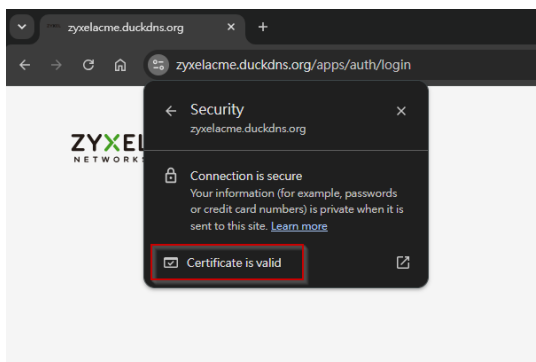
The screenshot shows the 'Administration Settings' page with a sidebar on the left containing 'System', 'Settings', and 'Administration Settings'. The main content area is titled 'Administration Settings' and contains a table of configuration options. The 'HTTPS' section is expanded, showing the following settings:

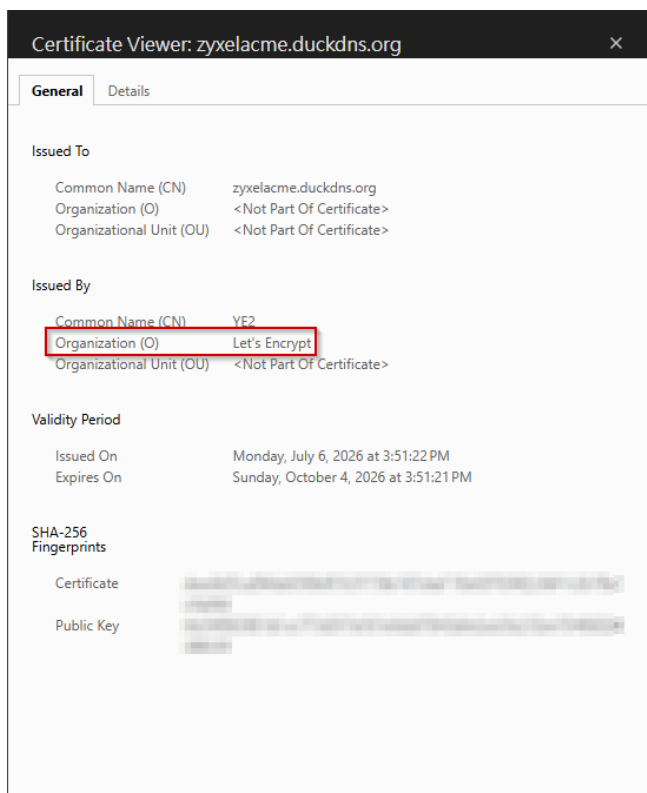
Category	Setting	Value
HTTP	Enable	☐
	HTTP Port	80
	Redirect HTTPS	☐
HTTPS	Enable	☒
	HTTPS Port	443
	Authenticate Client Certificates	☐
	Server Certificate	zyxelacme.duckdns.org
SSH	Enable	☒
	SSH Port	22
FTP Server	Server Certificate	default
	Enable	☒
	TLS Required	☐
	FTP Port	21
	Server Certificate	default

5. Enter https://<the device's domain name> in the browser to access the login GUI portal. Ensure that the connection is secure, as shown in the following screenshot captured from Chrome.



- Click the "Certificate is valid" option in Chrome and verify that the certificate is issued by Let's Encrypt.





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.

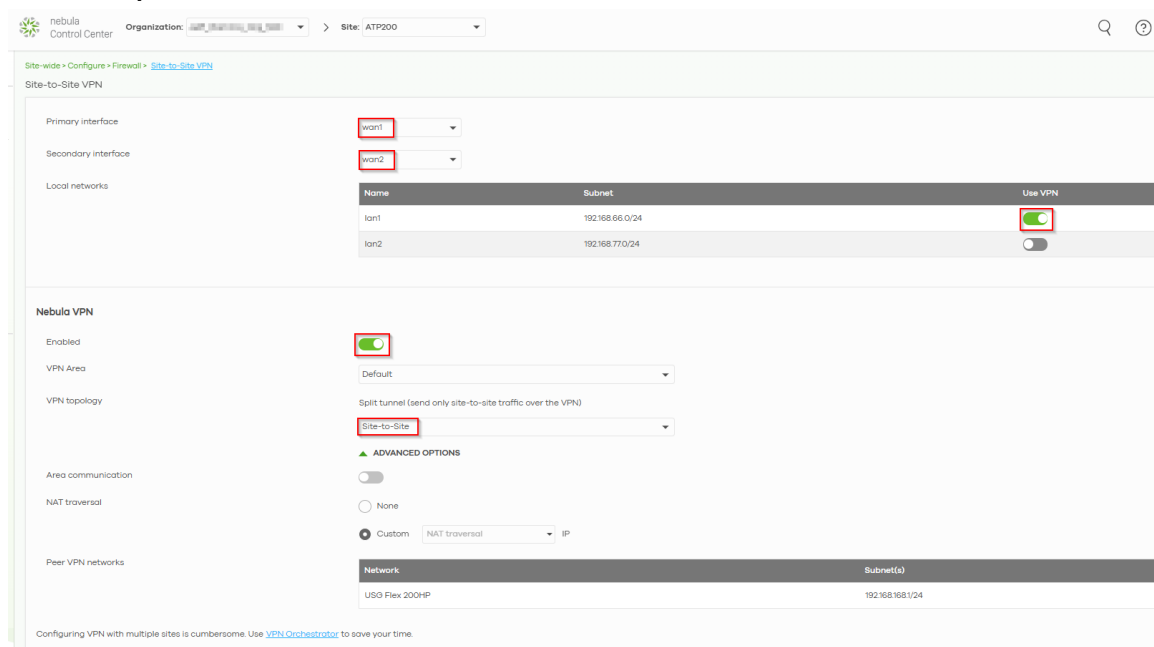


 **Note:** Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

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



Organization: [Organization Name] > 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	☒
lan2	192.168.77.0/24	☐

Nebula VPN

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 IP

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	☒
ge4	192.168.169/24	☐

Nebula VPN

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 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_BCP11802	111.243.24.24	5182L372000	59.115.115.115	0.0.0.0/0 <-> 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: [Nebula Control Center](#) > 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	☒
ge4	192.168.169.1/24	☐

Nebula VPN

Enabled: ☒

VPN Area:

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

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	☒
lan2	192.168.77.0/24	☐

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

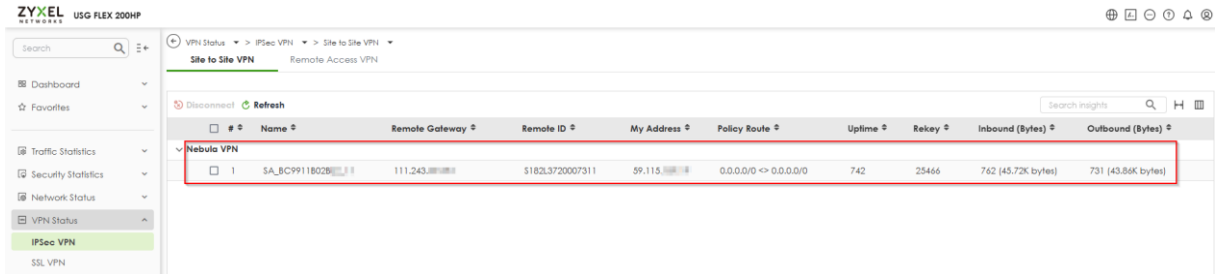
Connection status

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									
1	SA_BCP99118028	111.243.100.100	51823720007311	59.115.100.100	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.

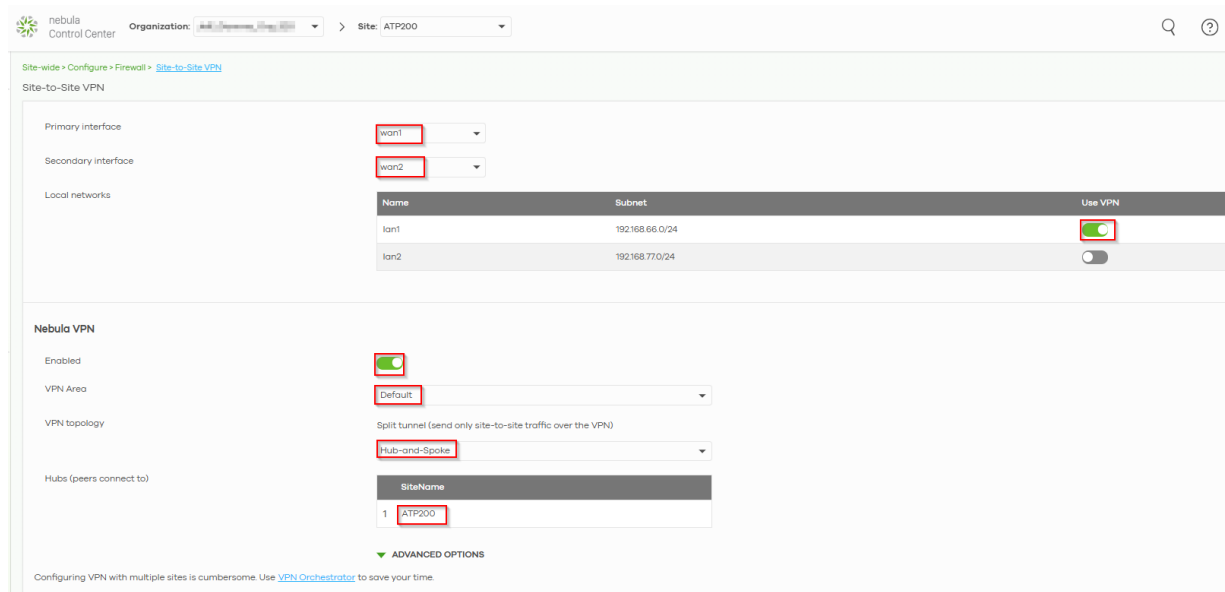


 **Note:** Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

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



Organization: Default 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	☒
lan2	192.168.770/24	☐

Nebula VPN

Enabled: ☒

VPN Area: Default

VPN topology: 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

nebulu Control Center Organization: [jerry@zyxel.com](#) 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	192.168.168/24	☒
ge4	192.168.169/24	☐

Nebula VPN

Enabled: ☒

VPN Area:

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hubs (peers connect to)

SiteName
1 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.

nebulu Control Center Organization: [jerry@zyxel.com](#) 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		192.168.168/24	connected	26.71 KB	34.84 KB	869	2025-01-07 17:46:52

nebulu Control Center Organization: [jerry@zyxel.com](#) 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

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last HeartBeat
ATP200		192.168.66/24	connected	93.05 KB	69.77 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.

ZYXELUSG FLEX 200HP

Search

Dashboard

Favorites

Traffic Statistics

Security Statistics

Network Status

VPN Status

IPSec VPN

SSL VPN

VPN Status > IPSec VPN > Site to Site VPN

Site to Site VPNRemote Access VPN

DisconnectRefresh

Search insights

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
Nebula VPN									
1	SA_BC991180288...	111.243.2...	\$182L372000...	1.161.1.8...	0.0.0.0/0 <- 0.0.0.0/0	140	27197	139 (8.34K bytes)	143 (8.58K bytes)

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 ✕ *

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 assige 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.

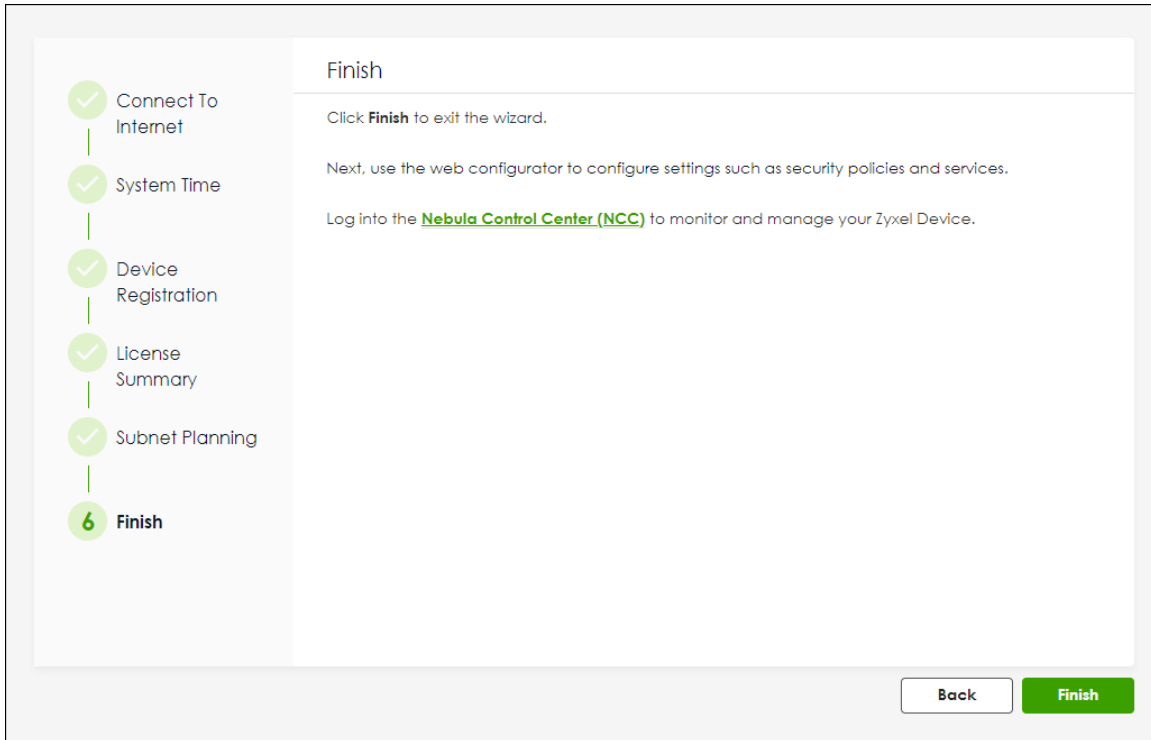
☒ No, I prefer to keep using default subnets of ge3/ge4.

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.

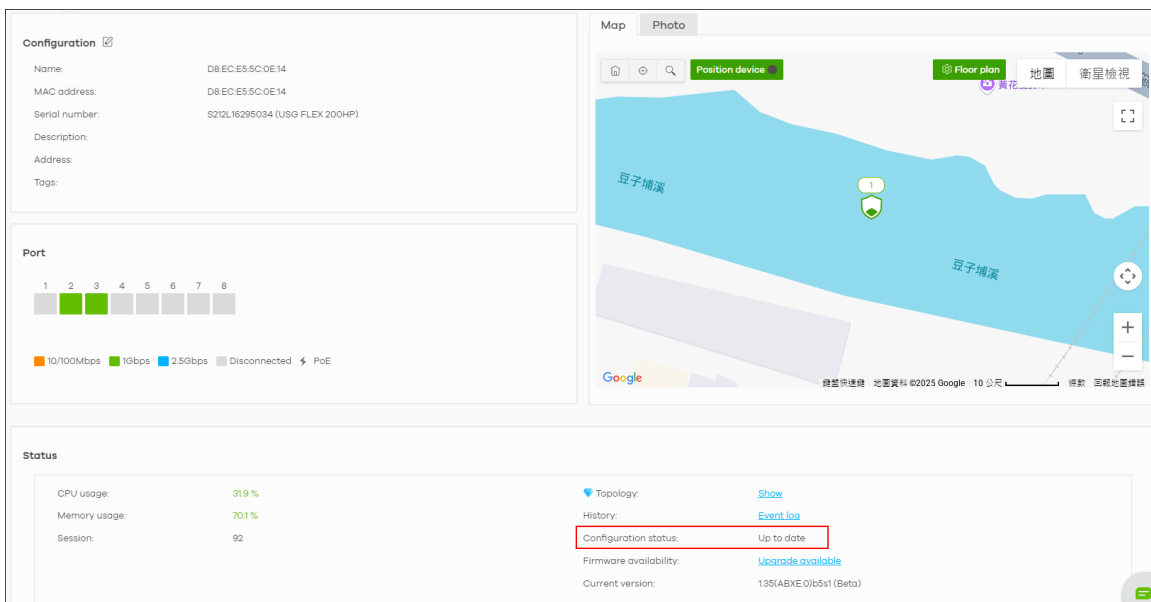
Back

Next

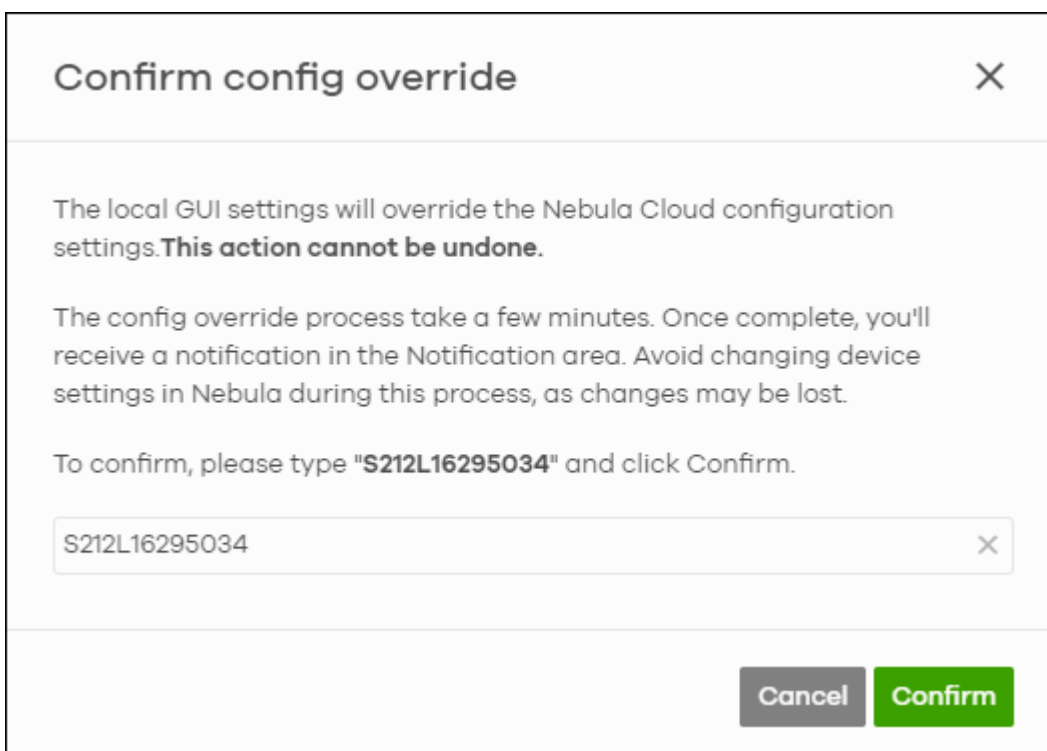
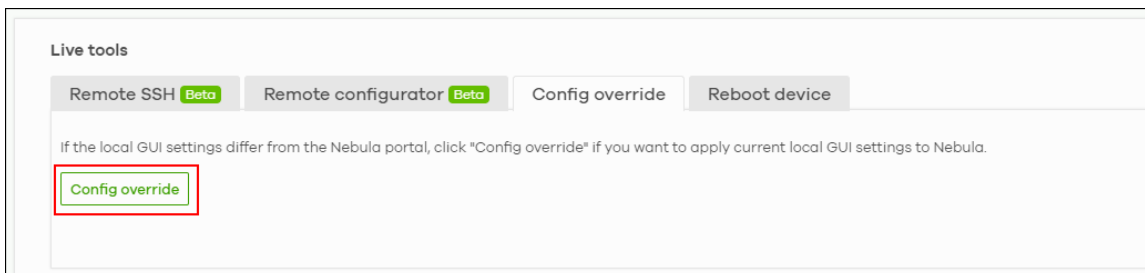
In Step 6, Click **Finish** to close the wizard from Web GUI.



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	S212L16295034	D8:EC:E5:5C:0E:14	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.

✓ Connect To Internet

✓ System Time

3 Device Registration

4 License Summary

5 Finish

Device Registration

Congratulations!

You have successfully completed the registration process. Click "Next" to finalize the installation wizard.

Back

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.

✓ Connect To Internet

✓ System Time

✓ Device Registration

✓ License Summary

5 Finish

Finish

Applying Cloud Configuration...

This process may take about 3-5 minutes.

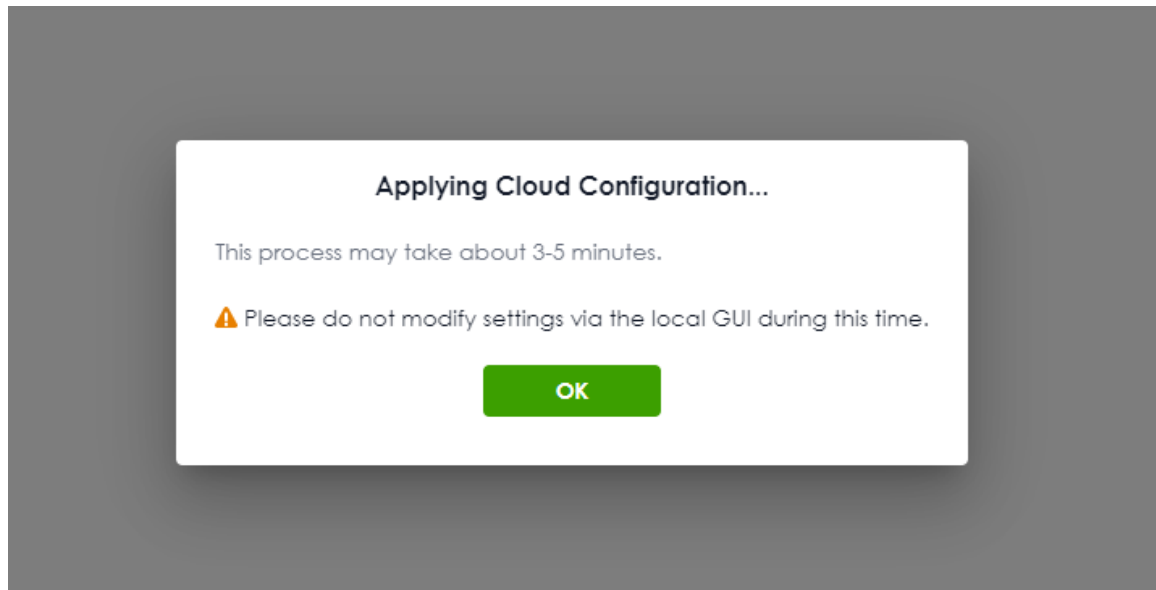
⚠

Please do not modify settings via the local GUI during this time.

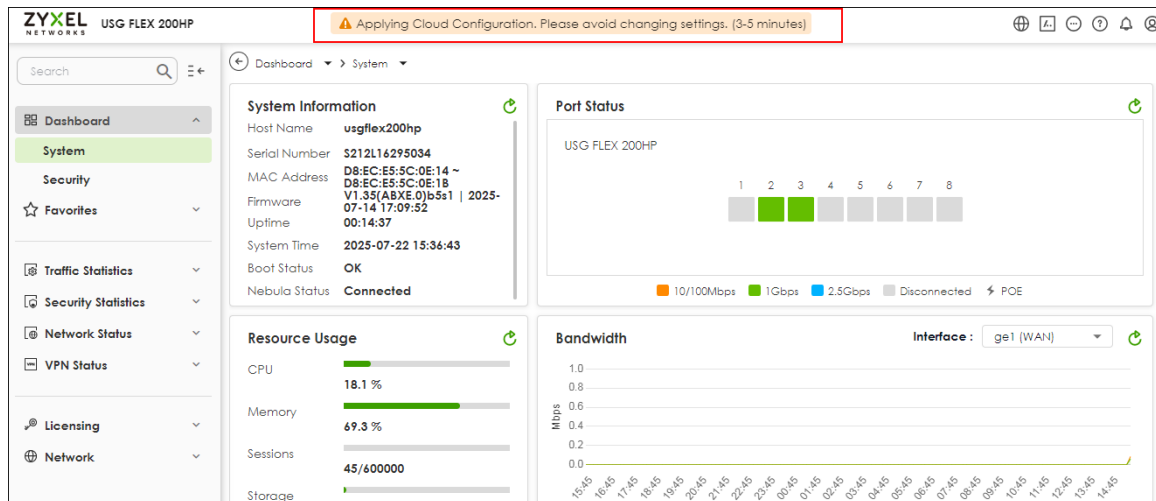
You can monitor the status and manage your Zyxel device in the [Nebula Control Center \(NCC\)](#).

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.



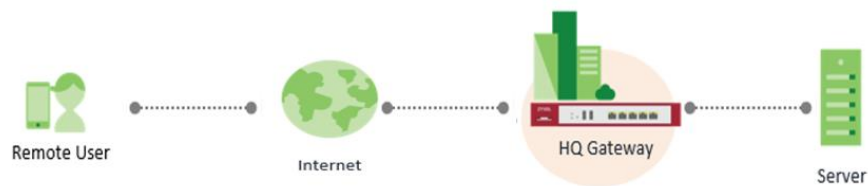
You can also monitor the firewall's status on the Nebula site and ensure the **Configuration Status** becomes Up to date.

The screenshot displays the Zyxel Nebula management interface for a specific firewall device. The interface is divided into several sections:

- Configuration:**
 - Name: D8EC55C0E14
 - MAC address: D8EC55C0E14
 - Serial number: S212L16295034 (USG FLEX 200HP)
 - Description:
 - Address:
 - Tags:
- Port:**
 - A row of 8 port status indicators. Port 2 is highlighted in green, indicating it is active.
 - 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)

How to Configure Remote Access VPN with Nebula Cloud Authentication?

This guide provides step-by-step instructions to set up Remote Access VPN on Nebula for Zyxel USG FLEX H series devices using remote access VPN, with the Window native client and Apple device(macOS, iOS, iPadOS) client.



Before You Begin

1. Create a Nebula User for VPN Authentication

Navigate to **Site-wide > Configure > Firewall > Remote access VPN** Create a nebula user account for remote access authentication on the User tab.

- Press the "+Add" button and then on the dialog enter Email, username and password.
- Make sure the VPN Access is enabled in the user settings and the authorized site.
- Save the settings.

VPN server address

Type

Nebula assigned domain name

Sign-on with

Nebula cloud authentication

+ Add account

Create user

Account type:

USER

Email:

yourmail@address.com

*

Username:

Zyxel_User

Description:

Password:

1234

*

Generate

DPPSK:

Generate

802.1X:

☐ Allow to use WPA-Enterprise to access network

VPN Access:

☒ Allow to use Remote VPN access

Authorized:

Yes

Expires:

☒ Does not expire

☐ Expires in:

*

minutes

Login by:

Email

VLAN assignment:

Preview

Two-Factor Auth(2FA):

☒ Bypass two-factor authentication.

Email to user:

☒ Email account information to user.

Close

Print

Create user

2. Enable the IPSec VPN settings on Nebula

Navigate to **Site-wide > Configure > Firewall > Remote access VPN**

Create a IPSec VPN Server settings.

1. Select a Binding address (The Nebula assigned domain will use this IP address). If not prefer WAN can be use Auto.
2. Enabled the IPSec VPN Server.
3. Select VPN server address type as "Nebula assigned domain name".
4. Sign-on with selected "Nebula cloud authentication" (The user authentication account can be also added on this page.
 - * Under The ADVANCED OPTIONS, you could base on the requirement to customized the settings.
5. Choose the **tunnel type** based on your network policy:
 - **Internet and Local Networks (Full Tunnel)**: All traffic goes through VPN
 - **Local Networks Only (Split Tunnel)**: Only specified subnet(s) go through VPN
6. The default address pool for IKEv2 remote access VPN is **192.168.50.0/24**

Note: Cloud auth. account only support "any" users.

Intent

Site-wide

Dashboard

Topology

Devices

Map & floor plans

Clients

Applications usage

Summary report

Monitor

Configure

Configure

Access points

Switches

Firewall

Port & Interface

Routing

NAT

Site-to-Site VPN

Remote access VPN

Security policy

Security service

Object

Firewall settings

Nebula assigned domain name

nebula-68c8f3e8.d2ns-nbl.com

Binding address

ge1_PPP

Auto

Custom IP

External

ge1

ge1_PPP

ge2

IPSec VPN Server

VPN server address

Type

IPSec VPN Server

IPSec VPN Server

VPN server address

Type

Sign-on with

VPN configuration script download

Clients will use VPN to access

ADVANCED OPTIONS

☒ Internet and Local Networks (Full Tunnel)

Auto SNAT ☒ ⓘ

☐ Local Networks Only (Split Tunnel)

Local Network

Client Network

IP Address Pool ✕

DNS Server

Security Settings

Zone

Allowed User ⓘ ✕

Phase 1 Settings

SA Life time ✕ (180 - 3000000 Seconds)

Proposal

Encryption	Authentication
AES256	SHA256
+Add	

Diffie-Hellman group ⓘ ⓘ ⓘ ✕

Phase 2 Settings

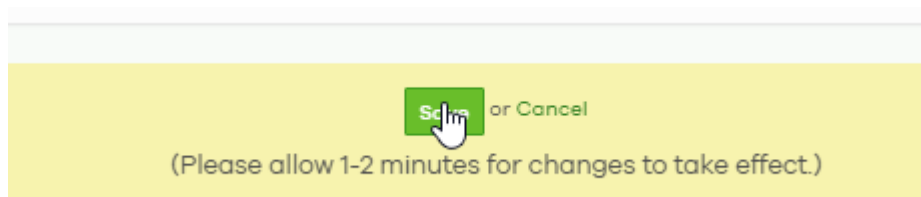
SA Life time ✕ (180 - 3000000 Seconds)

Proposal

Encryption	Authentication
AES256	SHA256
+Add	

Perfect forward secrecy (PFS) ⓘ ✕

Don't forget to click save before leaving the page.



Note: VPN configuration script download required to wait for synchronization



It may take 1-2 minutes to synchronize.



Enable SSL VPN on Nebula

Navigate to **Site-wide > Configure > Firewall > Remote access VPN**

1. Enabled the SSL VPN Server
2. Select VPN server address type as "Nebula assigned domain name"
3. Configure the server Port (Default port: **10443**).
4. Sign-on with selected "Nebula cloud authentication" (The user authentication account can be also added on this page.

Under the ADVANCED OPTIONS, you could base on the requirement to customized the settings.

5. Choose the **tunnel type** based on your network policy:

Internet and Local Networks (Full Tunnel): All traffic goes through VPN

Local Networks Only (Split Tunnel): Only specified subnet(s) go through VPN

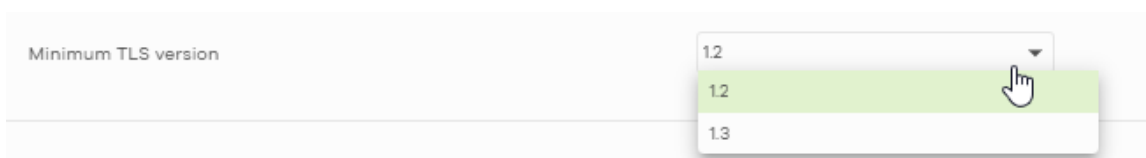
6. The default address pool for SSL VPN is **192.168.51.0/24**

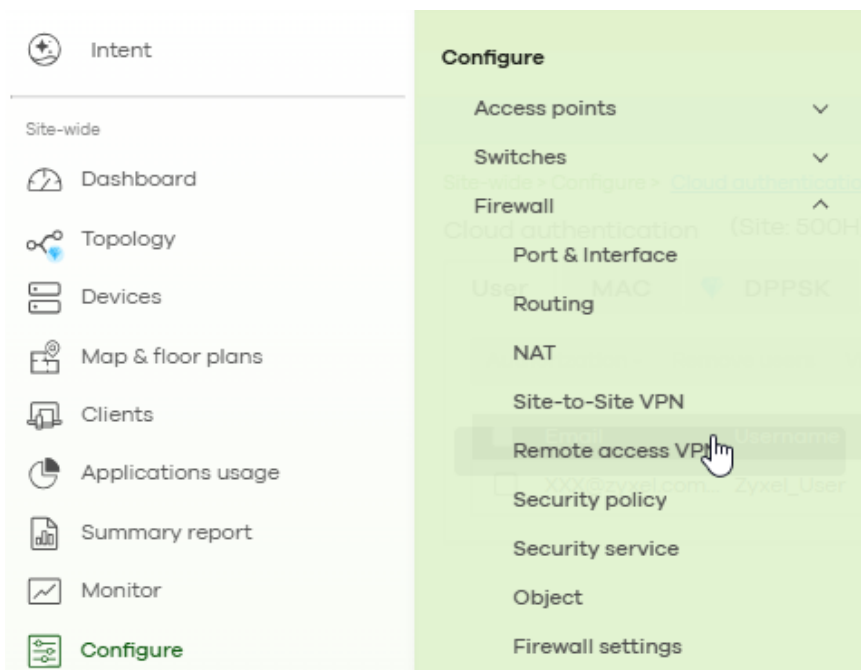
7. Assign allowed users for SSL VPN access

Note: Cloud auth. only support "any" user

* When the minimum TLS version is set to 1.2, clients can connect using TLS 1.2 or 1.3.

When the minimum TLS version is set to 1.3, only TLS 1.3 connections are allowed.





SSL VPN Server

VPN server address

Type

Nebula assigned domain name

Server Port

10443

Sign-on with

Nebula cloud authentication

+ Add account

SSL VPN configuration download

Download

ADVANCED OPTIONS

Internet and Local Networks (Full Tunnel)

Auto SNAT

Local Networks Only (Split Tunnel)

Clients will use VPN to access

Client Network

IP Address Pool

192.168.51.0/24

DNS Server

ZyWALL

Security Settings

Zone

SSL_VPN

Allowed User

any

Minimum TLS version

1.2

Get the SecuExtender VPN Client software

Windows

macOS

Configure IPSec VPN on the Laptop/Mobile

1. Navigate to **Site-wide > Configure > Firewall > Remote access VPN**
2. Click VPN configuration script download
3. After download the file you will see four scripts file in different type of OS model

VPN configuration script download

Download

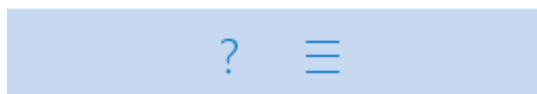
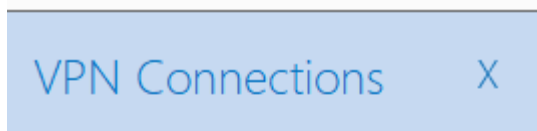
RemoteAccess_IPSecVPN_USG FLEX 500H.zip	2025-12-04 11:03 AM	WinRAR ZIP 壓縮檔	17 KB
---	---------------------	----------------	-------

After download, will require to unzip the file

Android(strongSwan)	2025-12-01 7:01 PM	File folder
Apple	2025-12-01 7:01 PM	File folder
Windows	2025-12-01 7:01 PM	File folder
ZyxelSecuExtender	2025-12-01 7:01 PM	File folder

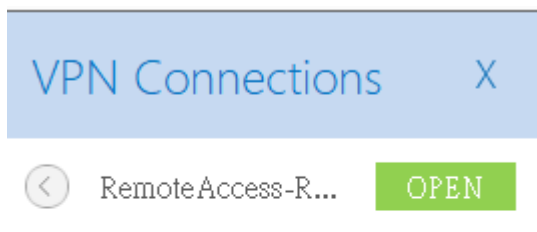
Set Up Remote Access on SecuExtender VPN Client (Windows)

1. Launch the client

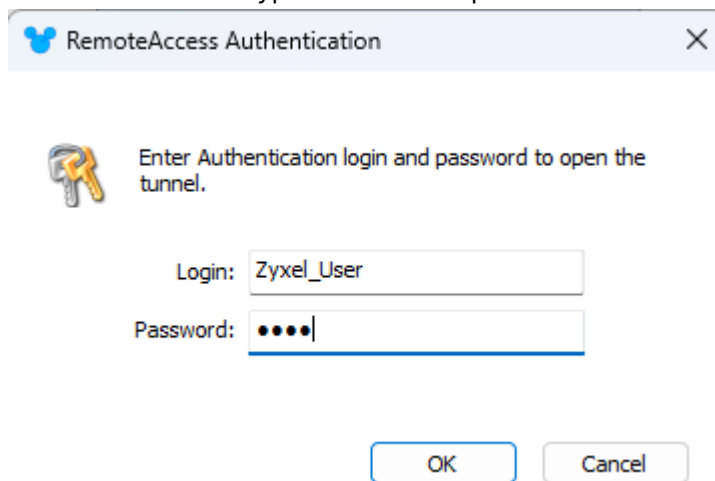


2. Double click the script file

RemoteAccess_SecuExtender_IPSecVPN.t...	2025-12-03 8:19 PM	TheGreenBow VP...	5 KB
---	--------------------	-------------------	------



3. Click OPEN and type account and password set on Nebula authentication

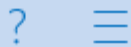


VPN Connections X



RemoteAccess-R...

CLOSE



```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::9b75:9035:5ef6:9150%23  
IPv4 Address. . . . . : 192.168.50.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.50.2
```

```
C:\Users\ [REDACTED] >ping 192.168.168.1
```

```
Pinging 192.168.168.1 with 32 bytes of data:  
Reply from 192.168.168.1: bytes=32 time=17ms TTL=64  
Reply from 192.168.168.1: bytes=32 time=8ms TTL=64  
Reply from 192.168.168.1: bytes=32 time=3ms TTL=64
```


Set Up IKEv2 VPN On Windows (Native IKEv2 Client)

1. Installed the script

Note: The certificate and bat file should be on same folder.

 Readme.txt	2025-12-04 3:03 AM	TXT File	1 KB
 RemoteAccess_Windows_IPSecVPN.bat	2025-12-04 3:03 AM	Windows Batch File	4 KB
 RemoteAccess_Windows_IPSecVPN.crt	2025-12-04 3:03 AM	CRT File	1 KB
 RemoteAccess_Windows_IPSecVPN.bat	2025-12-04 3:03 AM	Windows Batch File	4 KB

```

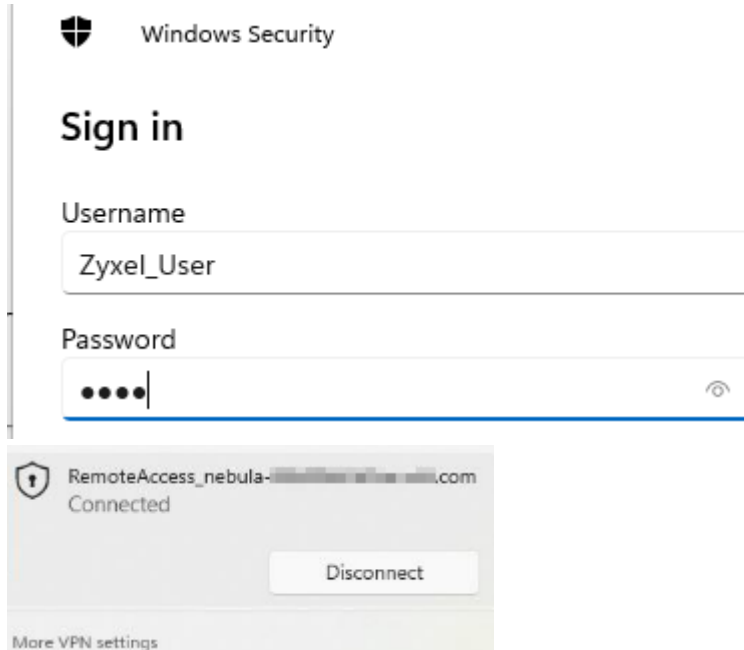
Requesting administrative privileges to install the IKEv2 VPN CA certificate...
"Install the IKEv2 VPN CA certificate..."
Create the RemoteAccess_10.10.10.10/24 VPN connection

DestinationPrefix : 10.10.10.10/24
InterfaceIndex    :
InterfaceAlias    : RemoteAccess_10.10.10.10/24 VPN connection
AddressFamily     : IPv4
NextHop           : 0.0.0.0
Publish           : 0
RouteMetric       : 1
PolicyStore       :

Press any key to continue . . . |

```

2. Connect to the VPN and enter the user name and password



```
PPP adapter RemoteAccess_nebula-... com:
```

```
Connection-specific DNS Suffix  : 
IPv4 Address. . . . . : 192.168.50.1
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0
```

```
C:\Users\... ping 192.168.168.1
```

```
Pinging 192.168.168.1 with 32 bytes of data:
Reply from 192.168.168.1: bytes=32 time=3ms TTL=64
Reply from 192.168.168.1: bytes=32 time=12ms TTL=64
```

Set Up IKEv2 VPN on iOS

1. Send the scripts below to the iOS/macOS/iPadOS device. => macOS need manual change the auth type

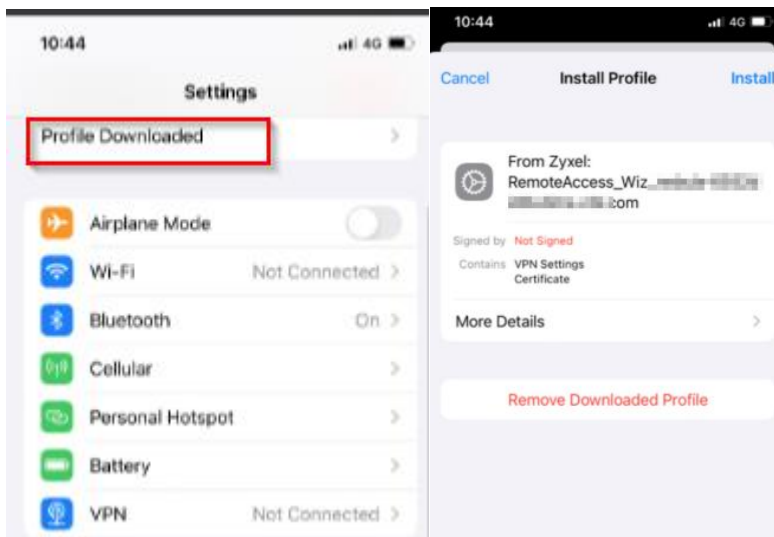
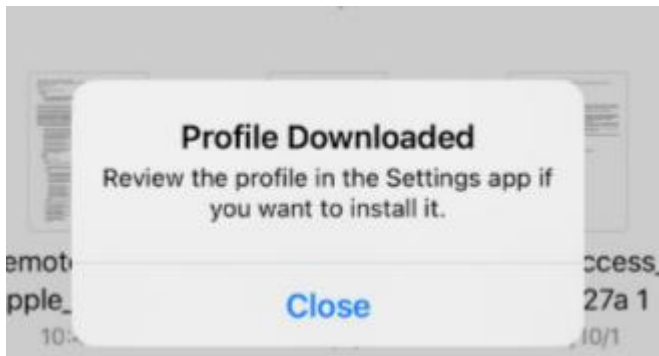
RemoteAccess_Apple_IPSecVPN.mobileconfig

2025-12-04 2:26 AM

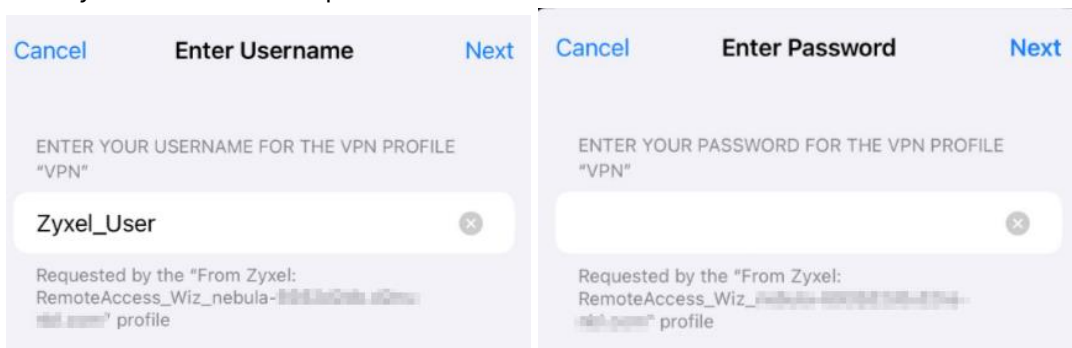
MOBILECONFIG File

6 KB

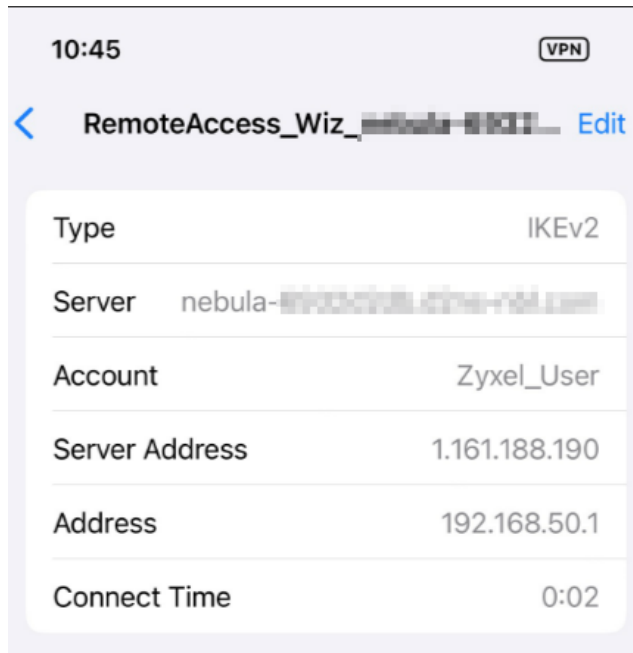
2. Go to **Settings > Profile Downloaded**, then **Install**
(Mac device: System Settings > Network / VPN)



3. Enter your username and password.

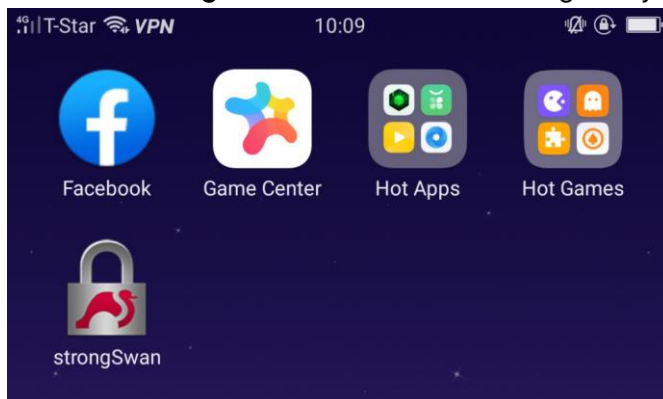


4. Connect to the VPN from the **Settings** > **VPN** menu.

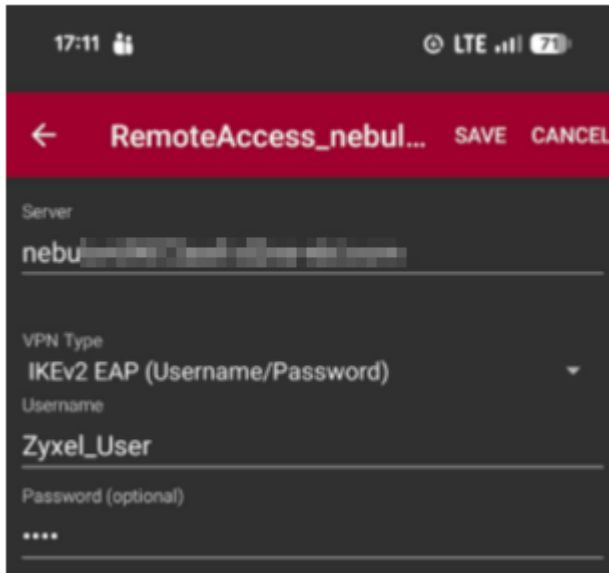


Set Up IKEv2 VPN on Android (strongSwan App)

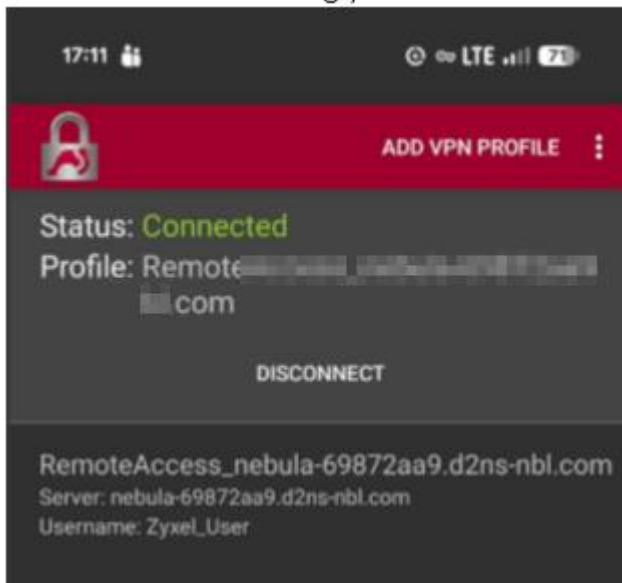
1. Install the **strongSwan VPN Client** from Google Play Store



2. Send the config script to the Android device.
3. Import the profile into strongSwan



4. Connect to the VPN using your credentials



Configure SSL VPN on the Laptop/Mobile

1. Navigate to **Site-wide > Configure > Firewall > Remote access VPN**
2. Click VPN configuration script download

SSL VPN Server

VPN server address

Type

Nebula assigned domain name

Server Port

10443

Sign-on with

Nebula cloud authentication

+ Add account

SSL VPN configuration download

Download

▲ ADVANCED OPTIONS

Internet and Local Networks (Full Tunnel)

Auto SNAT

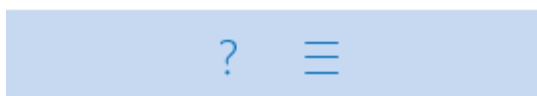
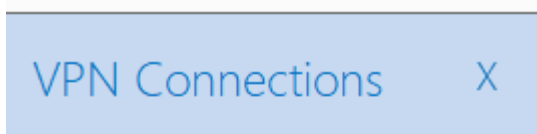
Local Networks Only (Split Tunnel)

3. After download the file you will see two scripts file

 ZyxeISecuExtender	2025-12-04 3:29 PM	File folder	
 RemoteAccess_SSLVPN.ovpn	2025-12-04 7:28 AM	OVPN Profile	5 KB

Set Up Remote Access on SecuExtender VPN Client(Windows)

1. Launch the client



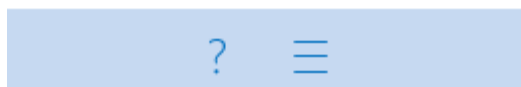
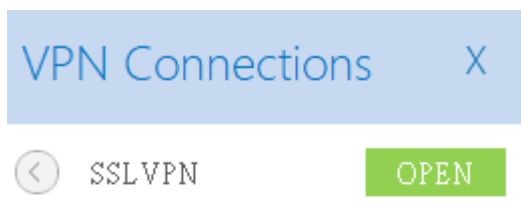
2. Double click the script file

 RemoteAccess_SecuExtender_SS...tgb

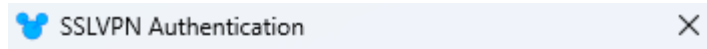
2025-12-04 7:28 AM

TheGreenBow VP...

6 KB



3. Click OPEN and type account and password set on Nebula authentication



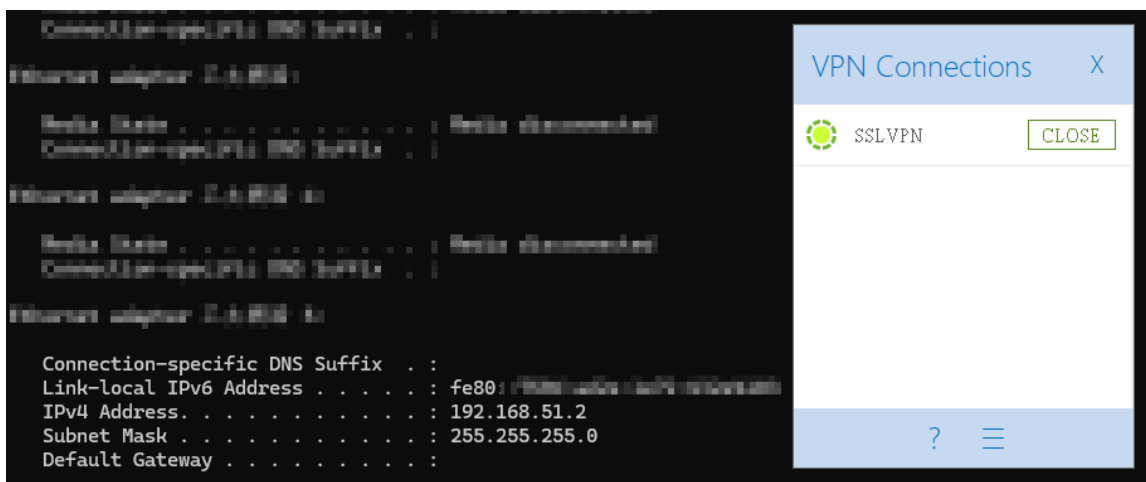
Enter Authentication login and password to open the tunnel.

Login:

Password:

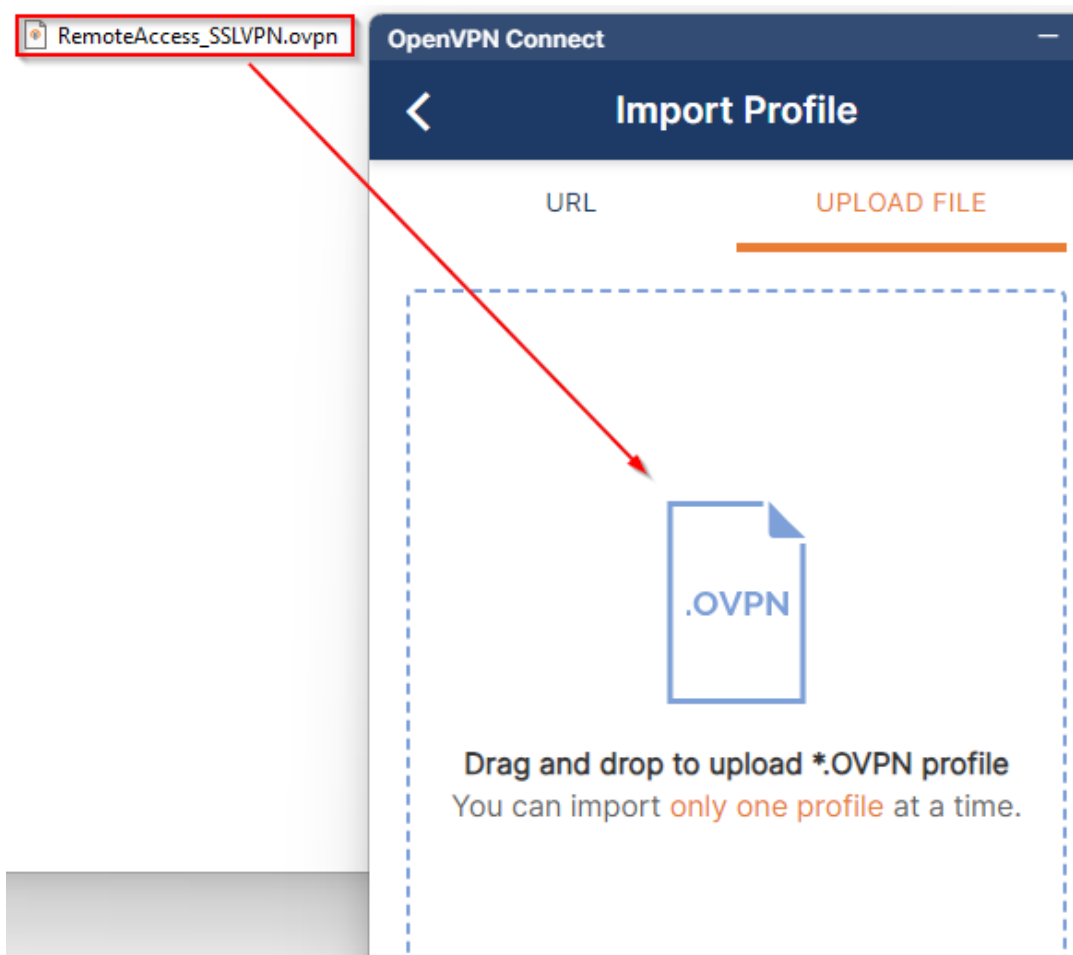
OK

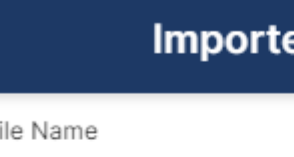
Cancel

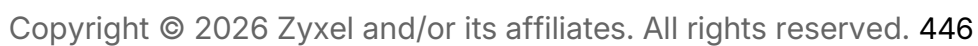


Set Up Remote Access on SecuExtender VPN Client(Windows)

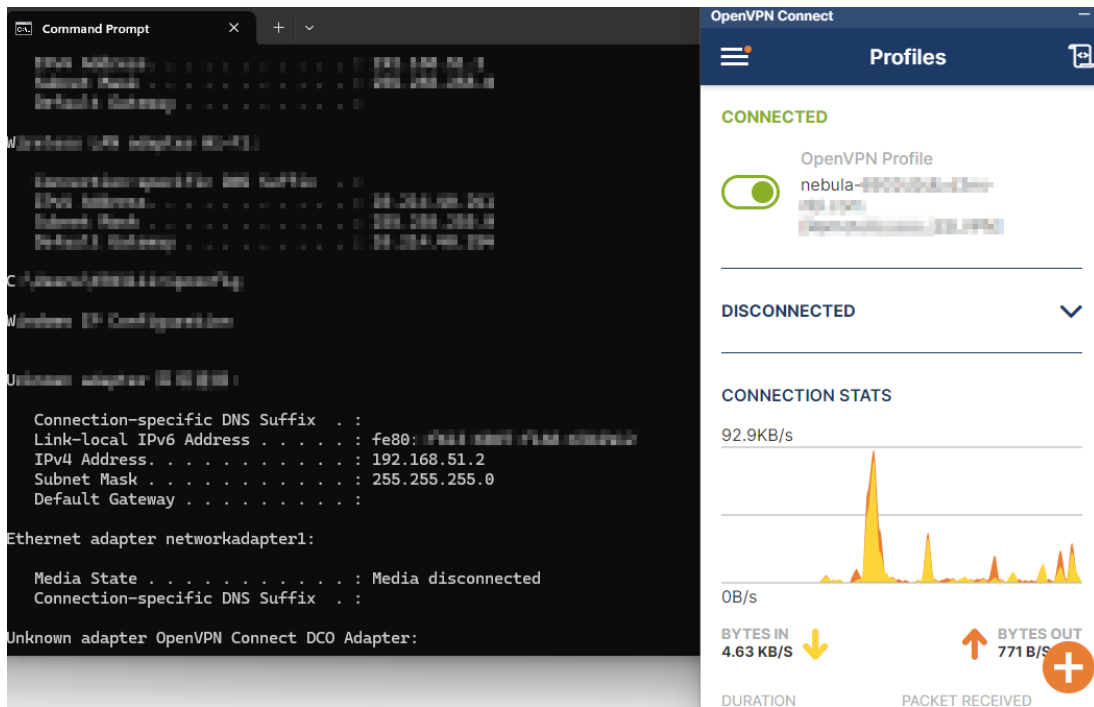
1. Launch the open VPN client and drag the upload ovpn profile to the application



- 
- OpenVPN Connect
- Imported Profile
- Profile Name
- nebula- [REDACTED]
- Server Hostname
- nebula- [REDACTED]
- Username
- Zyxel_User
- ☐ Save password

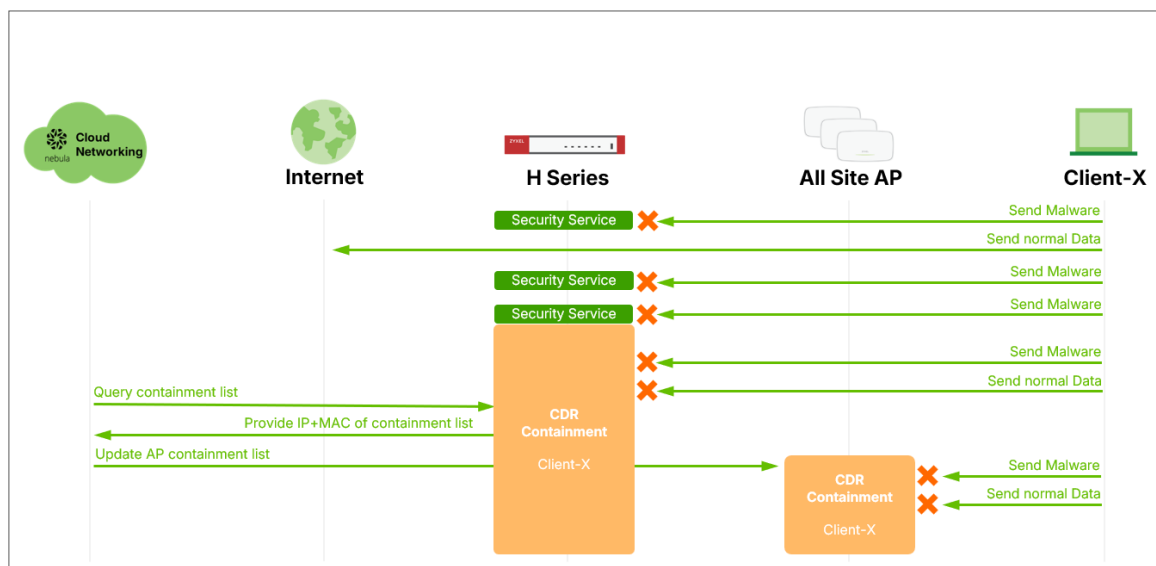


3. The connection should work



How to Configure CDR on Nebula

Collaborative Detection & Response (CDR) allows you to detect wired and WiFi clients that are sending malicious traffic in your network and then block or quarantine traffic coming from them. In this way, malicious traffic is not spread throughout the network. Secure policies can block malicious traffic for specific traffic flows, but CDR can block malicious traffic from the sender. Malicious traffic is identified using a combination of Web Filtering, Anti-Malware and IPS (IDP) signatures.



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 700H (Firmware Version: uOS V1.38).

Set Up the CDR on Nebula

Navigate to Site-wide > Configure > Collaborative Detection & Response. Turn on this feature and configure policies for each Security service: Malware, IDP, and web threats. Configure the occurrence, time window (minutes), and containment settings.

We have 3 actions for containment:

Alert: Send alert mail to recipient

Block: Block traffic from client on Nebula AP and Firewall and show notification page

Quarantine: Client from Nebula AP will stick to quarantine VLAN.

In this guide, we set the containment to block.

Category	Event type	Occurrence	Time window (min)	Containment
Malware	Malware detected	100 × *	30 × *	Block ▼
IDP	Vulnerability exploit detected	100 × *	30 × *	Block ▼
Web Threats	Connections to malicious web sites detected	30 × *	30 × *	Block ▼

The notification message can be edited if you need to modify the default message.

Or you want to redirect to an external URL.

We leave it as the default message. and redirect to local block page.

Notification message

There are malicious network activities found on your device. Please contact network administrator. ×

Redirect external URL

☐ URL:

To use custom captive portal page, please download the zip file and edit them.

[Download](#) the customized captive portal page example.

Set the Containment duration to 60 minutes. Once the client triggers CDR, the host will be blocked for 60 minutes.

Containment duration

60 ×

Another optional setting for wireless clients, if you want to block client association, is to enable "Block wireless client".

Block

Block wireless client ⓘ ☐

After completing the above settings, the client will be blocked when the host triggers a security service event within the given time window. We can add IP/MAC addresses to Exempt list, and they will never be added to the containment list. However, traffic matching a source IP in this list can still be blocked by security services.

Exempt list

IP or MAC

Set Up the containment to Alert

Assume you just want to set containment for alert emails only; you can select Alert in Containment.

Category	Event type	Occurrence	Time window (min)	Containment
Malware	Malware detected	100 × *	30 × *	Alert ▼
IDP	Vulnerability exploit detected	100 × *	30 × *	Alert ▼
Web Threats	Connections to malicious web sites detected	10 × *	30 × *	Alert ▼

Configure recipient at Site-wide > Configure > Alert settings

Security alerts

CDR containment ⓘ

Email ▼

to receive containment alerts

Hide additional recipients

xxxx@zyxel.com.tw

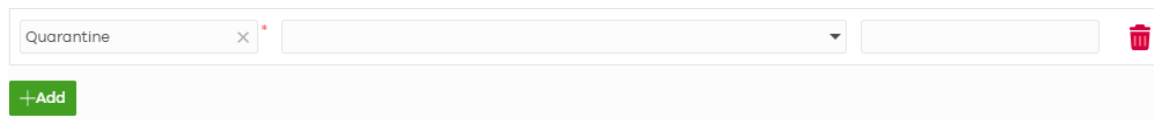
×

Set Up the containment to Quarantine

If you want to isolate a wireless client to a Quarantine VLAN after disassociation, you can select Quarantine in Containment. To avoid compromised clients continuing to damage network security, you will need to create a specific VLAN and a specific zone for the quarantine.

Create a zone by navigating to Site-wide > Configure > Firewall > Object.

Click the "Add" button and enter the zone name.

The screenshot shows a web interface for adding a new zone. At the top, there is a text input field containing the word "Quarantine" with a small 'x' icon to its right. To the right of this field is a dropdown menu and a red trash can icon. Below these elements is a green button with a white plus sign and the text "+Add".

Create a VLAN interface at Site-wide > Configure > Firewall > Port & Interface.

Click the "Add" button to open the Internal Interface configuration window.

Configure it as follows:

Interface name = quarantine

Type = VLAN

Member type = Port

Member = p4

Zone = Quarantine

VLAN ID = 101

Address assignment = Static

IPv4 address/Network Mask = 192.168.101.1/24

Internal interface configuration

Enable

Interface properties

Interface name

quarantine

Description

Type

VLAN

Member type

Port

Members

p4

Zone

Quarantine

VLAN ID

101

(1 - 4094)

Priority (8021P)

(0 - 7)

Address assignment

Static

IPv4 address/Network Mask

192.168.101.1/24

Secondary IP

Cancel

Ok

In the DHCP server section, enable it, then configure the starting IP address and the pool size.

DHCP server

Enable

☒

Mode

DHCP server

Start IP

192.168.101.33

Pool size
200

First DNS server

ZyWALL

Second DNS server

None

Third DNS server

None

Default gateway

Interface IP

Lease time

2

days

hours

minutes

Static DHCP table

Hostname	IP address	MAC address	Description
+Add			

Set the containments to Quarantine at Site-wide > Configure > Collaborative Detection & Response.

Category	Event type	Occurrence	Time window (min)	Containment
Malware	Malware detected	100	30	Alert
IDP	Vulnerability exploit detected	100	30	Alert
Web Threats	Connections to malicious web sites detected	3	10	Quarantine

Fill in the VLAN ID to assign a quarantine VLAN.

Quarantine

Quarantine VLAN ID

101

[What is this?](#)

For wired client, the firewall uses Captive Portal technology to drop client traffic and redirect HTTP/HTTPS traffic to a block page. This is identical to the Block action.

For wireless client, Wireless clients are dynamically assigned to a Quarantine VLAN after disassociation. Wireless clients are redirected to a block page on the AP.

Please note that for containment actions, only alerts will send email notifications. "Block" will only block client traffic and will not send an alert email, while "Quarantine" only applies to APs.



Note: This feature requires a license. Gold security pack is needed to enable this feature, and each Security service must be enabled because CDR relies on Security service (Anti-Malware, Intrusion Prevention System (IPS), Web Threats) to trigger CDR

Verification

If clients access a malicious site, they will be redirected to a blocked page.

Limited Network Access !

There are malicious network activities found on your device. Please contact network administrator.

Detail information:
 Category: Web Threats
 Security event: Connections to malicious web sites detected
 Event counts: 30 in 30 minutes
 Containment: Block
 Client information:
 IP address: 10.214.36.43
 MAC address: 30:65:ec:49:85:ea
 User: -

Please contact network administrator and close this window.

Powered by **ZYXEL**

Navigate to Log & Report > Log/Events > System, and we can see the blocked log as shown below.

Log & Report

Log / Events

System

System

APC

AP

Category

CDR

Clear Log

Export

Refresh

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port
1589	2026-04-30 15:57:59	CDR	client:10.214.36.43 user:- from:vlan30 security event: Web Threats threshold:30 containment:Block	0.0.0.0	0.0.0.0	0

Navigate to Site-wide > Monitor > Containment List, and the client will appear in the containment list. Click the Release button to manually release clients from the containment list.

Site-wide > Monitor > [Containment list](#)

Containment list

Q, IP address, MAC address

Time	IP address	MAC address	User	Event type	Containment	Time remaining (mins.)	Connect to
2026-04-30 16:13:32 (UTC +8...)	10.214.36.43	30:65:EC:49:85:EA	-	Connections to malicious w...	Block	57	Primary700H

Release/Add to Exempt List

☒ IP address
☐ MAC address

[Release](#) [Add to Exempt List](#)

If you select the containment to alert, you will receive mail content as below.

Collaborative Detect & Response found malicious activities of 1 client(s)

Dear administrator,

Organization : ZyXel_CSO

Site : [REDACTED]

Event Time	Category	Event type	Event count	Client information
2026-04-30 16:28:21	Web Threats	Connections to malicious web sites detected	30 in 30 minutes	IP Address: 10.214.36.43 MAC Address: 30:65:EC:49:85:EA User: -

This is an automatically generated email, please do not reply.

Sincerely,
The ZyXel Nebula Team

For the quarantine scenario, when a station triggers web threats, it will be redirected to a blocked page first.

Limited Network Access !

There are malicious network activities found on your device. Please contact network administrator.

Detail information:
Category: Web Threats
Security event: Connections to malicious web sites detected
Event counts: 3 in 10 minutes
Containment: Quarantine
Client information:
IP address: 192.168.168.38
MAC address: 54:8d:5a:4[REDACTED]
User: -

Please contact network administrator and close this window.

Powered by **ZYXEL**

After a few minutes, it will be redirected to a quarantine VLAN, and the following page will be displayed.

Limited Network Access !

There are malicious network activities found on your device. Please contact network administrator.

Detail information:
Category: Web Threats
Security event: Connections to malicious web sites detected
Event counts: 3 in 10 minutes
Containment: Quarantine
Client information:
IP address: 192.168.101.34
MAC address: 54:8d:5a: [REDACTED]
User:

Close

Powered by **ZYXEL**

Please contact network administrator and close this window.

Powered by **ZYXEL**

And CDR log can be seen under Site-wide > Monitor > firewall > event log.

Site-wide > Monitor > Firewall > [Event log](#)

Event log

Keyword: Category: CDR 2026-05-07 1h UTC+8

< Newer Older > 1 matches in 45 Event logs Export

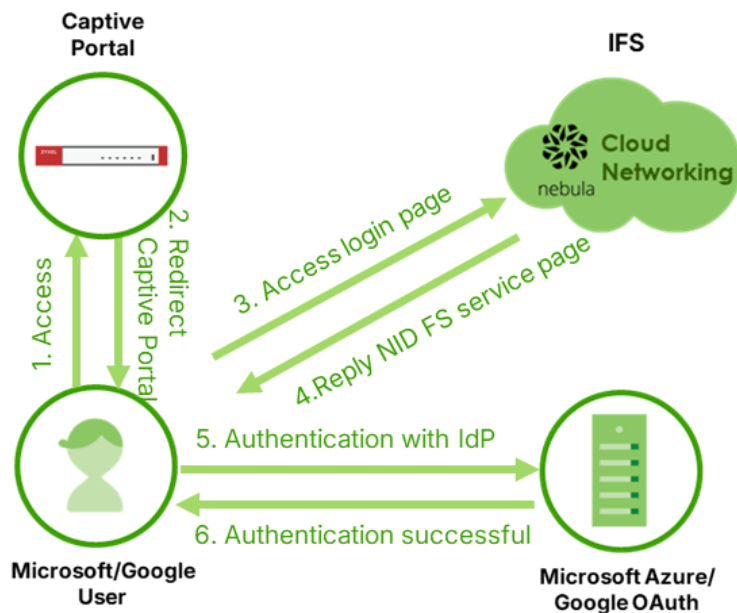
Time	Category	Source IP	Source port	Destination IP	Destination p...	Detail
2026-05-07 16:38:18	CDR					client:192.168.168.38 user:- from:ge3 security event:Web Threats threshold:2 containment:Quarantine

 **Note:** The firewall containment list references the client's source IP. New devices might obtain an IP address that is still in the containment list if the DHCP lease of a contained client expires before the containment period ends. It is strongly recommended to configure the DHCP server leasing time greater than 2 times of containment period

Nebula identity federation service (NID FS) support Captive Portal

Architecture Comparison:

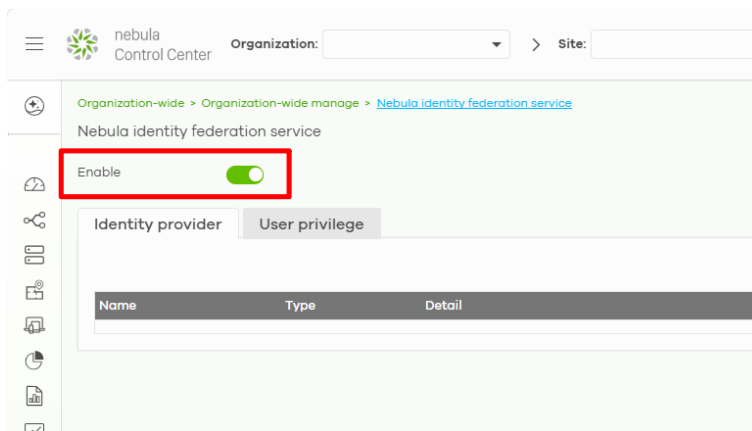
In Firmware v1.39, the USG FLEX H series introduces Nebula Identity Federation Service (NID FS) to provide flexible and centralized third-party identity authentication for Captive Portal.



Prerequisites

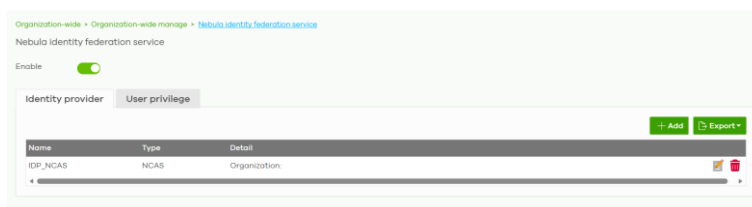
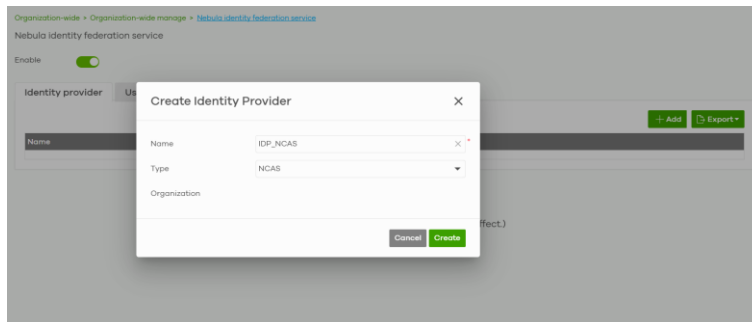
Before using NID FS for Captive Portal authentication, ensure the following licensing and Nebula Control Center (NCC) settings are completed:

- Licensing Requirement: All same Org devices must have a valid Nebula Professional Pack or Gold Pack license.
- Enable NID FS. (Organization-wide > Organization-wide manage > Nebula identity federation service)

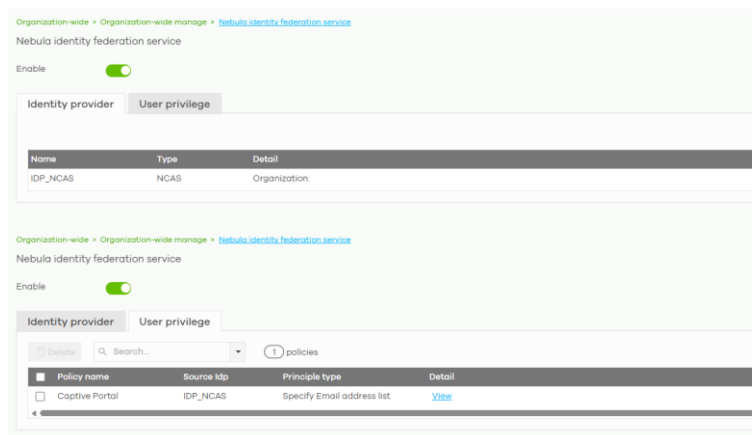


- Configure IdP in Nebula: click the Add button > Enter custom name > Select type (NCAS) > Click the Create button. Supported IDP types include (Microsoft Entra ID, Google OAuth, NCAS)





- User Privilege: Configure User Privileges and selected the IdP in Nebula NID FS.

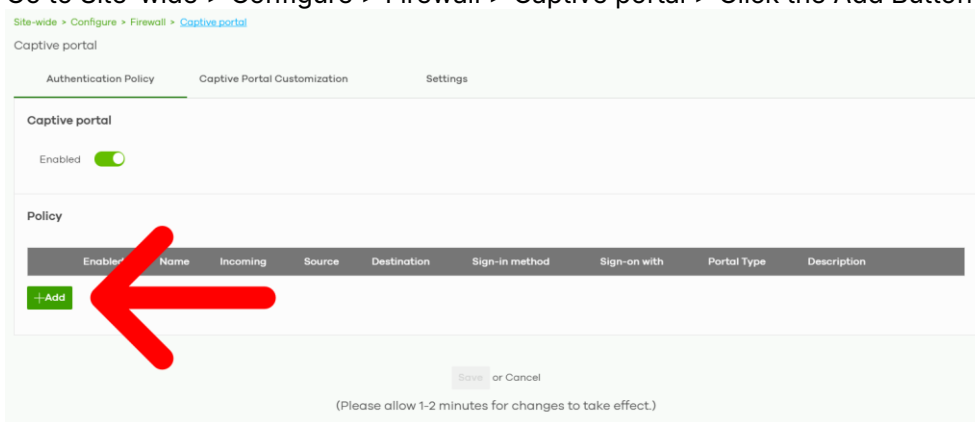


Captive Portal Configuration

Administrators can configure the Captive Portal sign-in method to NID FS either via Nebula Cloud Control Center or local Firewall Web GUI.

Step-by-Step Configuration (Nebula Cloud)

1. Go to Site-wide > Configure > Firewall > Captive portal > Click the Add Button



Site-wide > Configure > Firewall > Captive portal

Captive portal

Authentication Policy Captive Portal Customization Settings

Captive portal

Enabled ☒

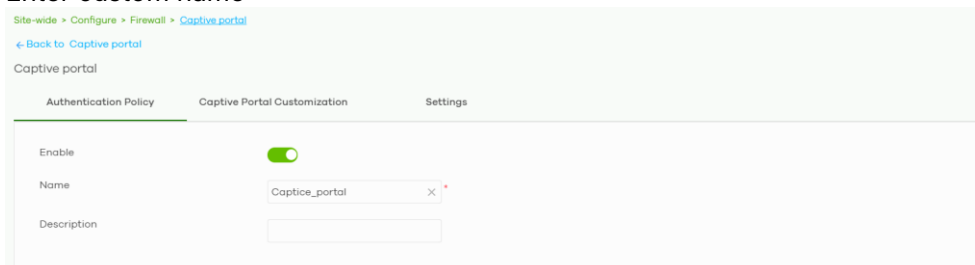
Policy

Enabled	Name	Incoming	Source	Destination	Sign-in method	Sign-on with	Portal Type	Description
+Add								

[Save](#) or [Cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

2. Enter custom name



Site-wide > Configure > Firewall > Captive portal

[Back to Captive portal](#)

Captive portal

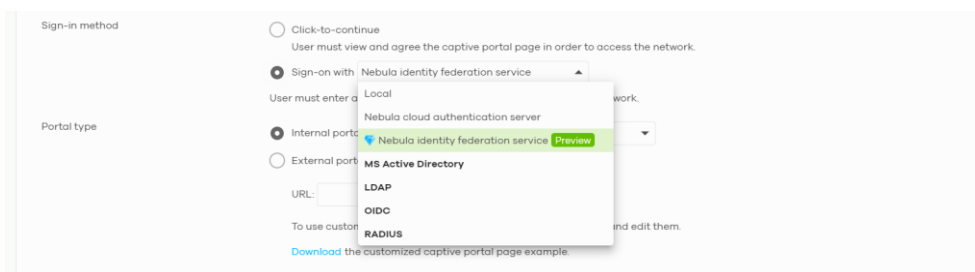
Authentication Policy Captive Portal Customization Settings

Enable ☒

Name

Description

3. Criteria > Sign-in method > Sign-on with > choose "Nebula identity federation service" and press save button.



Sign-in method

☐ Click-to-continue
User must view and agree the captive portal page in order to access the network.

☒ Sign-on with **Nebula identity federation service**

User must enter a work.

☒ Internal port **Nebula identity federation service** [Preview](#)

☐ External port **MS Active Directory**

URL:

To use custom and edit them.

[Download](#) the customized captive portal page example.

4. Click the SAVE button

Download the customized captive portal page example.

Policy advance setting

After the captive portal page where the user should go

☒ Stay on Captive portal authenticated successfully page

☐ Stay on login session page

☐ To promotion URL:

Redirect TCP port 443 traffic to login page ☐

Idle timeout ☐

Log ☐

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

Step-by-Step Configuration (Local Web GUI)

1. Captive Portal > Authentication Policy > Policy. Add or Edit policy

Search

Network Status

VPN Status

Wireless Status

Licensing

Network

VPN

Security Policy

Captive Portal

Authentication Policy

Object

Security Services

User & Authentication

Captive Portal > Authentication Policy > Policy

Policy Settings

General Settings

Enable ☒

+ Add Edit Remove Active Inactive Move to

Status	Priority	Name	Incoming	Source	Destination
☒	1	Captive_portal	ge3	any	any

2. Sign-in Method section > select "Sign-on with Nebula identity federation service".

Captive Portal > Authentication Policy

Object

No data

Sign-in Method

☐ Click-to-continue
Users must view and agree the captive portal page in order to access the network

☒ Sign-on With

Nebula identity federation service

Local
Nebula cloud authentication server
Nebula identity federation service
Default

Portal Type

☒ Internal

☐ External

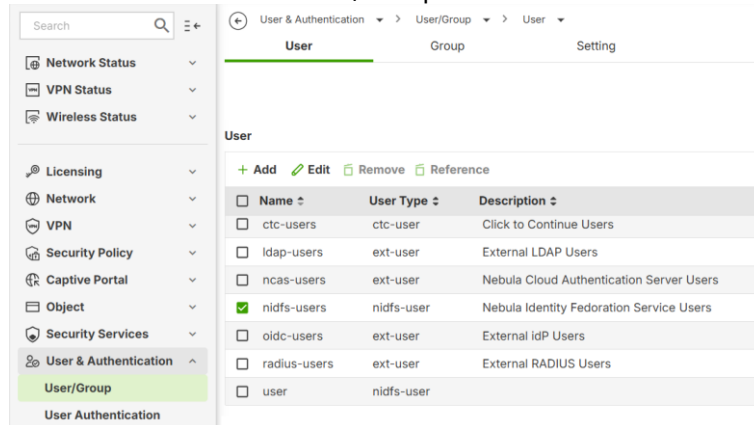
URL

Advanced Settings

NID FS User Objects & Claim-Based Policy Control:

Default User Profile Management:

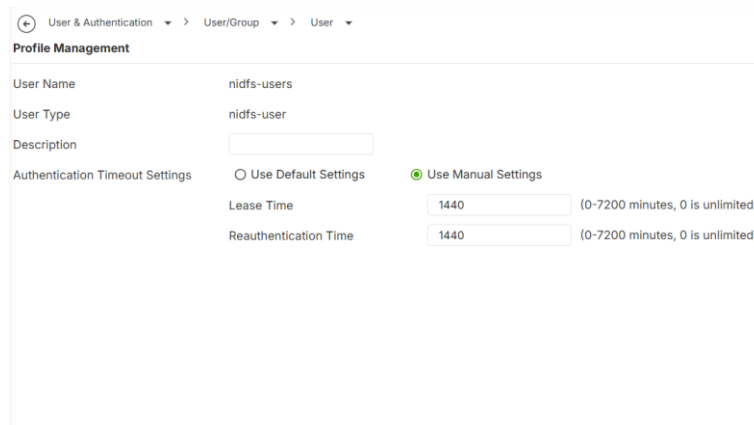
1. User & Authentication > User/Group > User > nids-users



The screenshot shows the ZyXel management interface. On the left is a sidebar menu with categories like Network Status, VPN Status, Wireless Status, Licensing, Network, VPN, Security Policy, Captive Portal, Object, and Security Services. The 'User & Authentication' section is expanded, showing 'User/Group' and 'User Authentication'. The main area displays a breadcrumb trail: 'User & Authentication > User/Group > User'. Below this is a tabbed interface with 'User', 'Group', and 'Setting' tabs. The 'User' tab is active, showing a table of users. At the top of the table are buttons for '+ Add', 'Edit', 'Remove', and 'Reference'. The table has columns for 'Name', 'User Type', and 'Description'. The 'nids-users' entry is selected with a green checkmark.

Name	User Type	Description
ctc-users	ctc-user	Click to Continue Users
ldap-users	ext-user	External LDAP Users
ncas-users	ext-user	Nebula Cloud Authentication Server Users
☒ nids-users	nids-user	Nebula Identity Federation Service Users
oidc-users	ext-user	External idP Users
radius-users	ext-user	External RADIUS Users
user	nids-user	

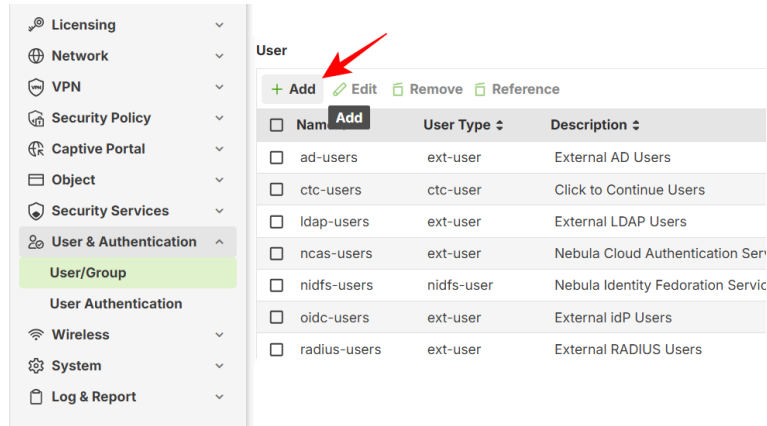
2. Click Edit on nids-users to adjust Lease Time (default: 1440 minutes) and Reauthentication Time (default: 1440 minutes)



The screenshot shows the 'Profile Management' page for the 'nids-users' profile. The breadcrumb trail is 'User & Authentication > User/Group > User'. The page title is 'Profile Management'. It shows the 'User Name' as 'nids-users' and 'User Type' as 'nids-user'. There is a text field for 'Description'. Under 'Authentication Timeout Settings', the 'Use Manual Settings' radio button is selected. Below this, there are two input fields: 'Lease Time' with a value of '1440' and 'Reauthentication Time' with a value of '1440'. Both fields have a note '(0-7200 minutes, 0 is unlimited)'.

3. Creating NID FS User Objects with Claim-Based Matching:

User & Authentication > User/Group > User > click +Add



Set User Type to "NID FS User" and select the target Identity Provider.

User & Authentication > User/Group > User

Profile Management

User Name: user

User Type: **NID FS User**

Identity Provider: **IDP_NCAS**

Matching Type: ☒ All Users ☐ Matching Rules

Description:

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

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Under Matching Type, select Matching Rules for IdP claim-based matching (e.g., mapping Entra ID group membership via groups claim)

Rule Constraint: Only 1 Claim Key can be configured (e.g., group), and up to 5 Claim Values can be added (e.g., sales).

[User & Authentication](#) > [User/Group](#) > [User](#)

Profile Management

User Name:

User Type:

Identity Provider:

Matching Type: ☐ All Users ☒ Matching Rules

Claim Key	Matching Values
☐ group	sales <input checked="" type="button" value="x"/> +

Description:

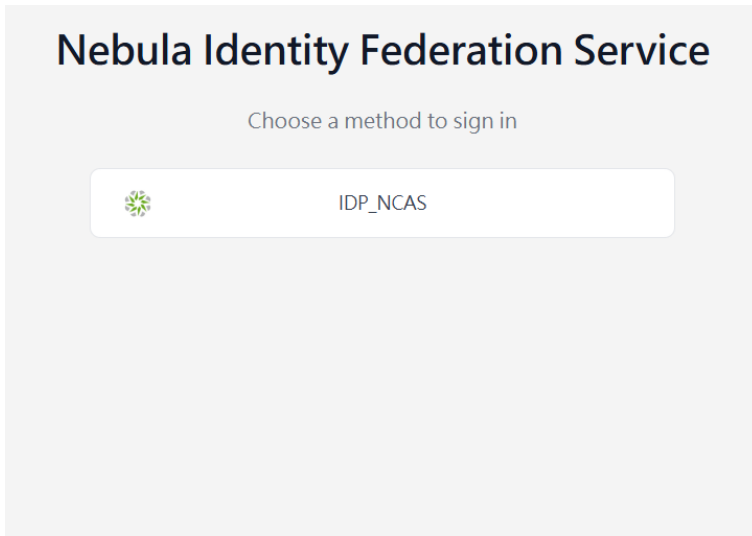
Authentication Timeout Settings: ☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

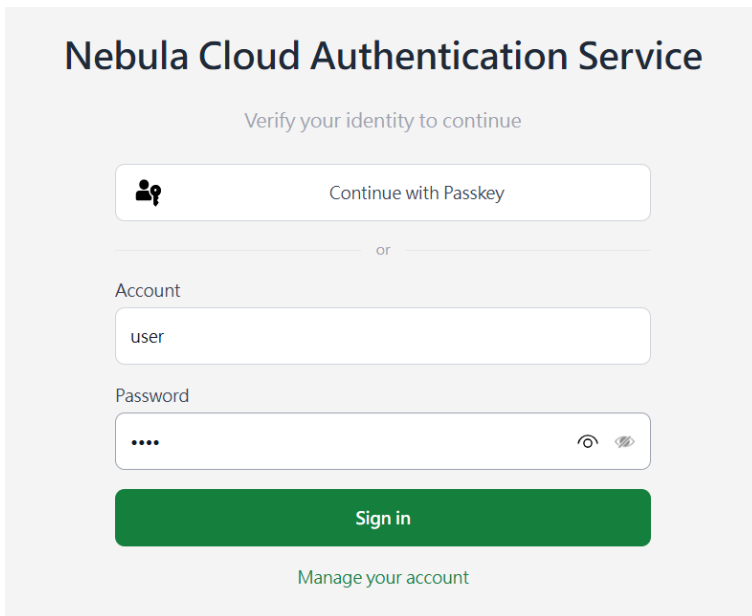
User Login Flow

1. User connected to device and matching the captive portal policy and then opens an HTTP/HTTPS web page in browser.
2. Browser will redirect to the NID FS login page.



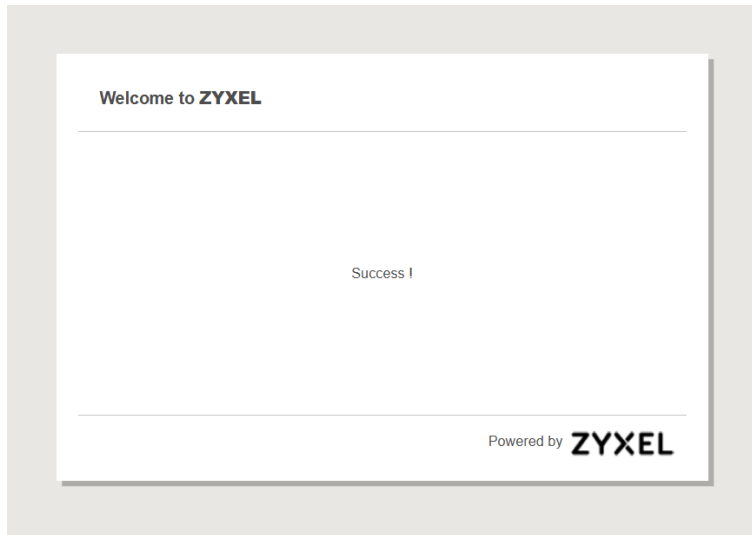
The image shows the 'Nebula Identity Federation Service' login page. At the top, it says 'Choose a method to sign in'. Below this, there is a single button with a green icon and the text 'IDP_NCAS'.

3. User selects the desired IdP
4. NID FS will redirect browser to IdP login endpoint.
5. User enters credentials on IdP login page.



The image shows the 'Nebula Cloud Authentication Service' login page. At the top, it says 'Verify your identity to continue'. Below this, there is a button with a person icon and the text 'Continue with Passkey'. Below this button, there is a horizontal line with the word 'or' in the center. Below the line, there are two input fields: 'Account' with the text 'user' and 'Password' with four dots. To the right of the password field are two icons: an eye and a hand. Below the input fields is a green button with the text 'Sign in'. At the bottom, there is a link that says 'Manage your account'.

6. When authentication is pass, you will see the authentication success page and opens network access.



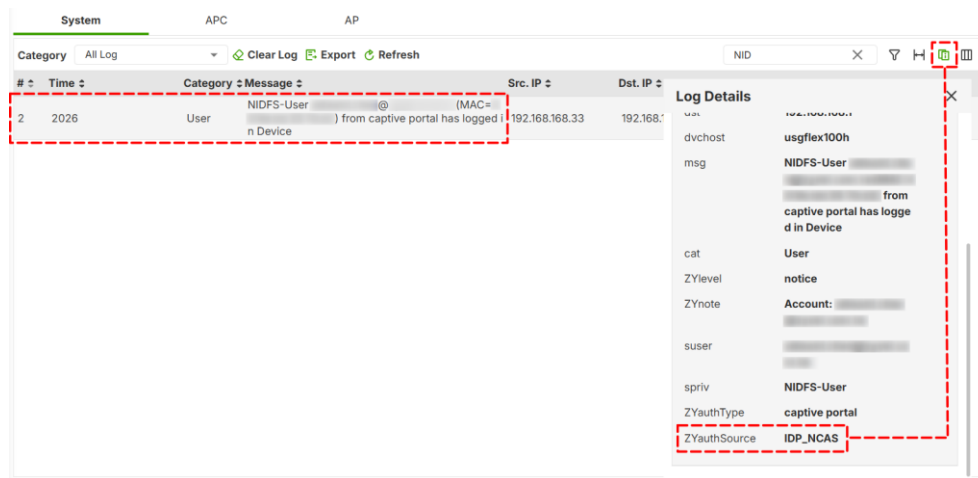
Verification & Log Inspection

Login User Status (Network Status > Login Users)

Login Users		Lockout IPs						
Force Log Out		Search insights						
#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
2	(Auth Source: IDP_NCAS)	nidsf-user	192.168.168.33	0:00:18	captive portal	0.0.0.0	23:59:42	nidsf-user(nidsf-users)

System Event Logs:

- Go to Log & Report > Log / Events > System
- The category type is User and the message will see the NIDFS user information example: NIDFS-User *****@example.com.tw(MAC=...) from captive portal has logged in Device.
- Expand Log Details / Extended Information

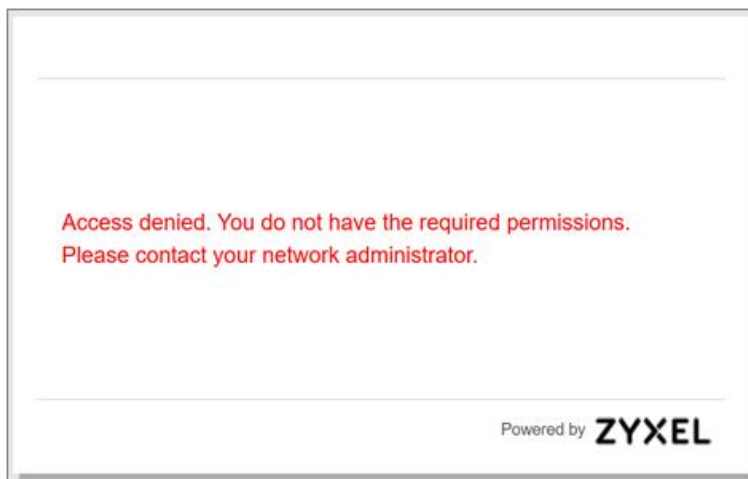


Error Handling & CLI Debug Commands

Common Error Pages:

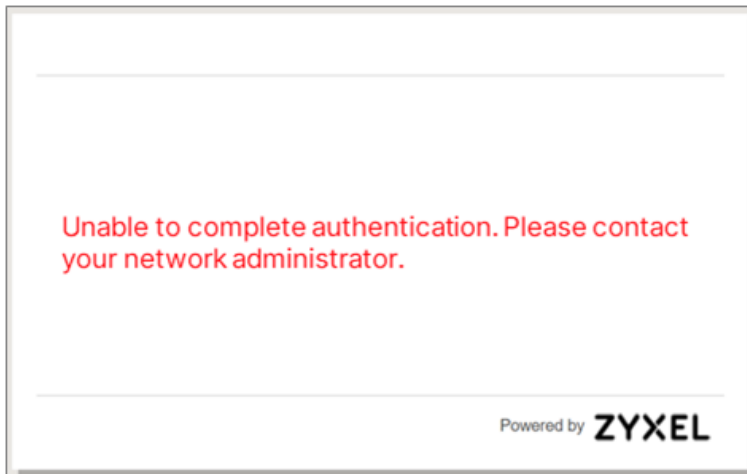
1. User Without Assigned Privileges

Cause: User authenticated successfully at IdP but failed privilege verification in Nebula NID FS User Privileges policies.



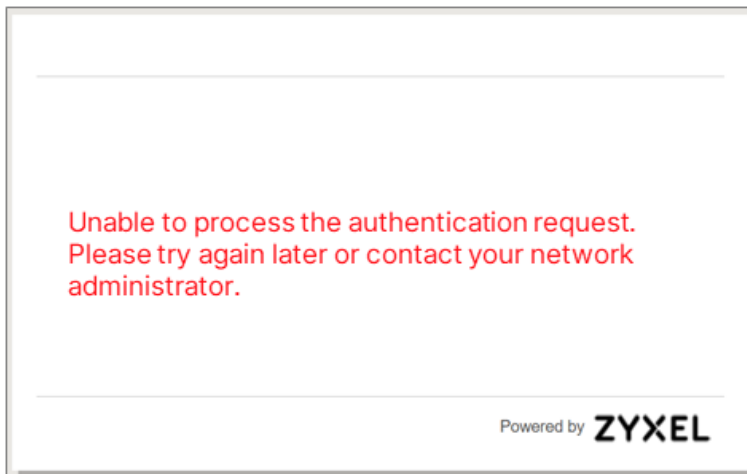
2. Nebula Pro Pack License Expired

Cause: Device lacks an active Nebula Professional Pack or Gold Pack license.



3. Token Validation Failed

Cause: Token validation failed or invalid response received.



CLI Debug Command

Before initiating end-user testing, run the following CLI command to verify that the firewall can properly generate OIDC authorization requests.

- Output includes test-uri with full parameter strings (client_id, redirect_uri, scope, state, nonce). Copy and paste the URI into a browser to test NID FS availability.

```
usgflex200h> cmd aaa validate-oidc-profile nids
```

```
validate-oidc-profile
```

```
data
```

```
test-uri
```

```
https://mainpaab40hv.ifs.timber.zndev.link/api/v1/oauth/authorize?client_id=*****  
*****&response_type=code&redirect_uri=*
```

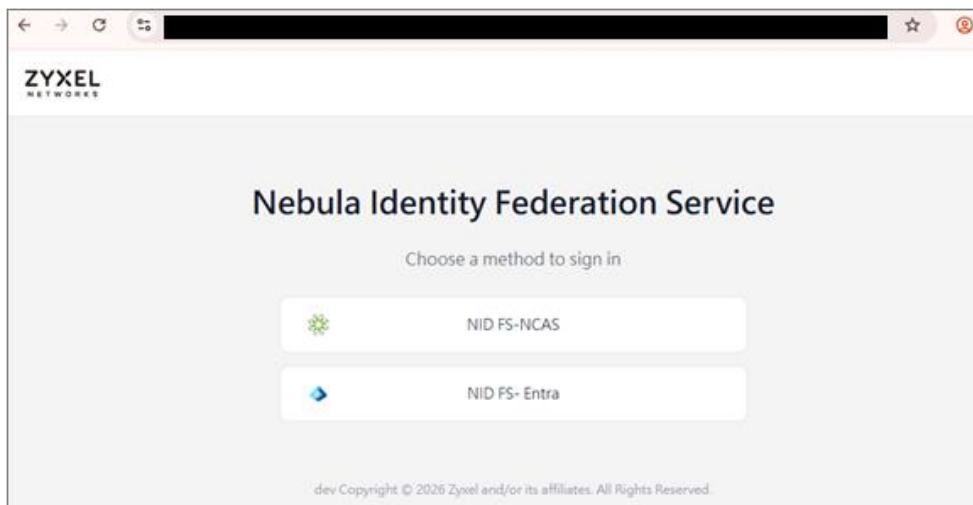
```
*****_
```

```
slogin.nebula.zyxel.com*****&response_mode=query&  
scope=*****&state=*****
```

```
*****&nonce=*****
```

```
**&prompt=login
```

```
..
```



NCAS Integration & Removal of Disconnection Behavior

- NCAS authentication is now natively integrated into the NID FS framework and follows OIDC flows.
- If only using NCAS authentication, administrators do not need to configure additional NID FS settings.
- Removed the NCAS Disconnection Behavior setting under Captive Portal > Authentication Policy > Advanced Settings. Current behavior is always block if can't reach the NCAS server

Mandatory Unique Authentication Policy Name

- A mandatory rule Name is now required when creating Captive Portal authentication policies for mapping with NID FS privileges.
- Naming Rule: Must start with a letter, maximum 31 characters, valid characters: [a-zA-Z_-][a-zA-Z0-9._-].
- Firmware Upgrade Migration: After upgrading from v1.38 to v1.39, existing Auth Policy IDs are automatically populated as rule names

Automated Certificates & Authentication Proxy

Captive Portal Certificate:

- When upgrade to the v1.39 the default redirect URL will changed using FQDN (ngw-login.nebula.zyxel.com) to prevent SSL warnings.
- When Server Certificate is set to Auto, the Redirect FQDN cannot be manually modified.

Authentication Proxy Settings:

- Path: User & Authentication > User Authentication > Advanced > Authentication Proxy.
- Enabled by default (HTTPS Port 1003) to handle authorization code exchange between Client and IdP.

Security Enhancement: User Lockout Behavior

Local / External User Authentication:

- Firewall locks client IP only when username/password retries exceed the maximum limit.

NID FS Authentication:

- Firewall immediately locks client IP when validation failures are triggered by an invalid authentication response or an invalid ID Token. This prevents malicious access attempts using forged tokens.

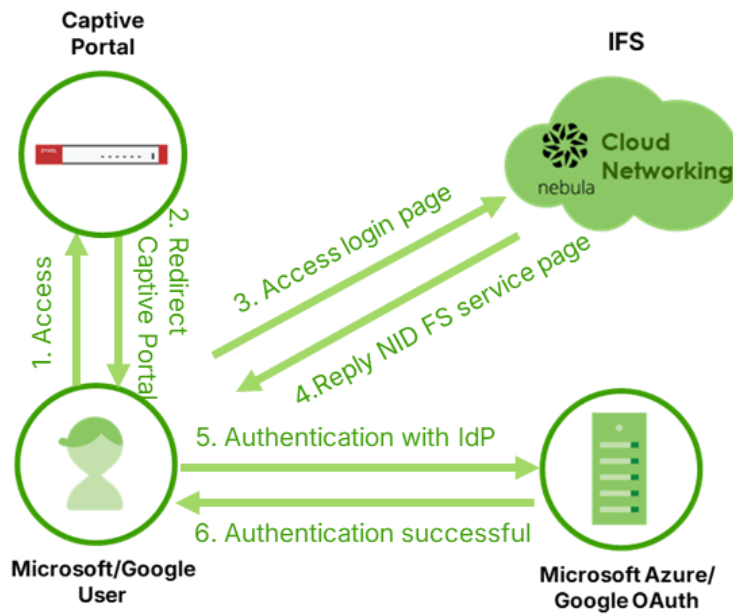
Portal Restrictions & External Portal Guidelines

- Custom internal portal themes are no longer supported for NCAS / NID FS because the login portal is hosted by NID FS.
- External portal pages must not collect user credentials directly. They must use a redirect page/button (e.g., "Click to Continue") to redirect users to NID FS. If before v1.39 has used the external portal, after upgrade to 1.39 must using the new external portal template.

Nebula identity federation service (NID FS) support SSL VPN

Architecture Comparison:

In Firmware v1.39, the USG FLEX H series introduces Nebula Identity Federation Service (NID FS) to provide flexible and centralized third-party identity authentication for SSL VPN.

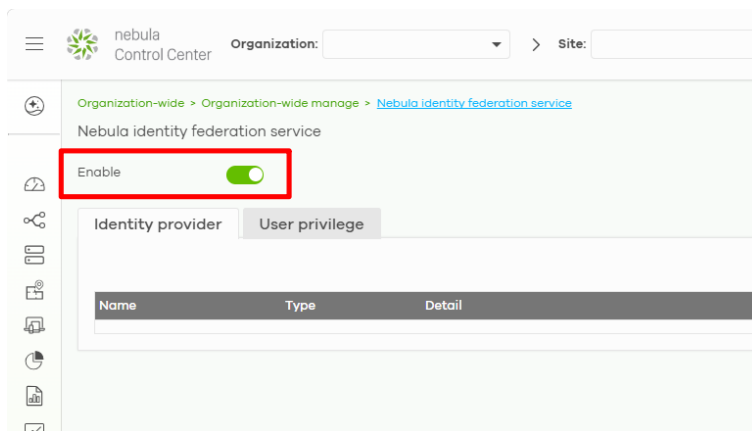


Note: SecuExtender VPN client does not support NID FS and NCAS Passkey

Prerequisites

Before using NID FS for Captive Portal authentication, ensure the following licensing and Nebula Control Center (NCC) settings are completed:

- Licensing Requirement: All same Org devices must have a valid Nebula Professional Pack or Gold Pack license.
- Enable NID FS. (Organization-wide > Organization-wide manage > Nebula identity federation service)



- Configure IdP in Nebula: click the Add button > Enter custom name > Select type(NCAS) > Click the Create button. Supported IDP types include (Microsoft Entra ID, Google OAuth, NCAS)



Organization-wide > Organization-wide manage > Nebula identity federation service

Nebula identity federation service

Enable ☒

Identity provider

Create Identity Provider

Name IDP_NCAS

Type NCAS

Organization

Cancel Create

Name	Type	Detail
IDP_NCAS	NCAS	Organization

- Create user privilege policy: Enter in Policy name and select the IdP you just created, and click Next.

Create user privilege policy

[Select user](#)

Select service

Summary

Policy name SSL_VPN

Source Idp IDP_NCAS

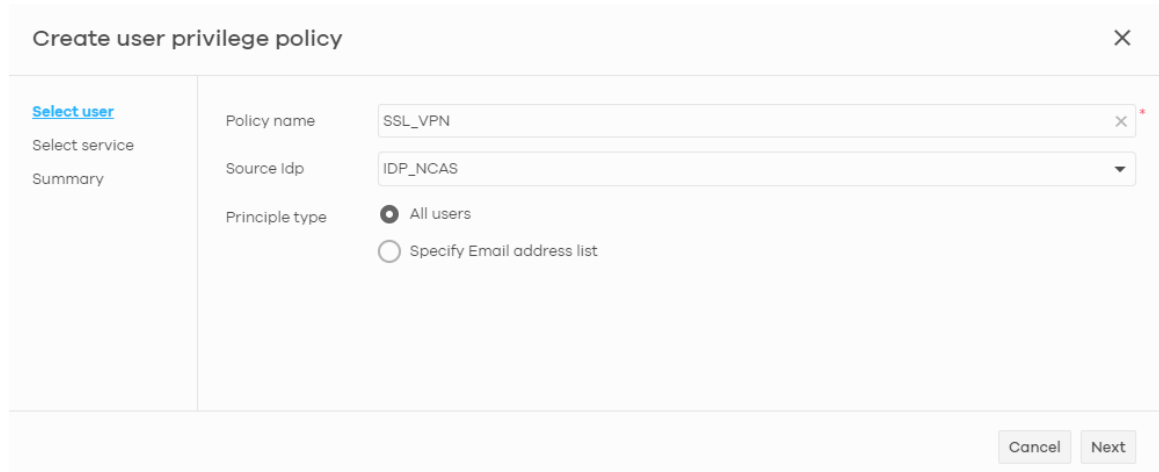
Principle type

☒ All users

☐ Specify Email address list

Cancel Next

- Create user privilege policy: Enter in Policy name and select the IdP you just created, and click Next.



Create user privilege policy [X]

[Select user](#)
Select service
Summary

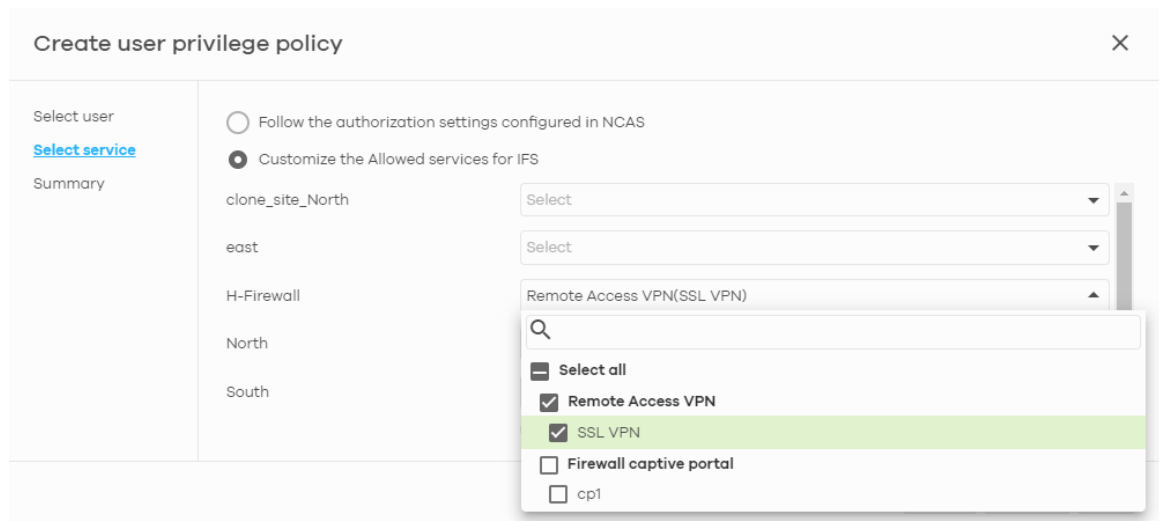
Policy name:

Source Idp:

Principle type: ☒ All users
☐ Specify Email address list

[Cancel] [Next]

- Select Customize the Allowed services for IFS, and select the site you configured and the service you need. (In this case, we select SSL VPN). And click Next.



Create user privilege policy [X]

Select user
[Select service](#)
Summary

☐ Follow the authorization settings configured in NCAS
☒ Customize the Allowed services for IFS

clone_site_North:

east:

H-Firewall:

North:

South:

Search:

☒ Select all
☒ Remote Access VPN
☒ SSL VPN
☐ Firewall captive portal
☐ cp1

- Check the summary and click Create.

Create user privilege policy

Select user

Select service

Summary

Policy name

Source Idp

Principle type

Allowed services

SSL_VPN

IDP_NCAS

All users

Site: H-Firewall

Service type	Service name
Remote Access VPN	SSL VPN

Cancel

Previous

Create

SSL VPN Configuration:

Administrators can configure the Remote SSL VPN to NID FS either via Nebula Cloud Control Center or local Firewall WebGUI.

Step-by-Step Configuration (Nebula Cloud)

1. Go to Site-wide > Configure > Firewall > Remote access VPN > Enable SSL VPN server, and configure the Type and Server port.

SSL VPN Server

VPN server address

Type

Server Port

Sign-on with

SSL VPN configuration download

Nebula assigned domain name

10443

Nebula identity federation service

Download

Download available after synchronization

ADVANCED OPTIONS

- Choose "Nebula identity federation service" as Sign-on with method.

The screenshot shows the 'SSL VPN Server' configuration page. The 'Sign-on with' dropdown menu is open, displaying a list of authentication methods. The 'Nebula identity federation service' option is highlighted with a red box and a green 'Preview' button next to it. Other options in the list include 'AD or RADIUS server', 'AD or RADIUS server, then local users', 'Local users', 'Local users, then AD or RADIUS server', 'OIDC server', and 'Nebula cloud authentication server'.

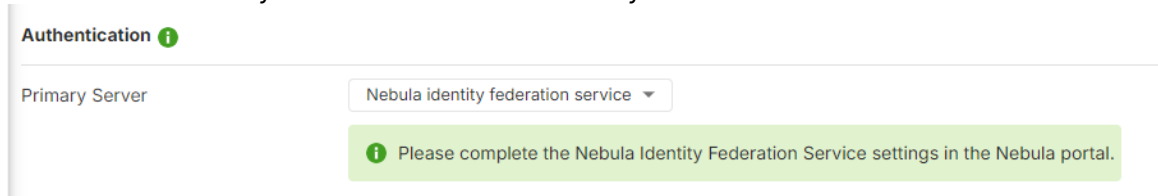
- Click the SAVE button.

Step-by-Step Configuration (Local Web GUI)

- VPN > SSL VPN > Enable the SSL VPN option, and configure the VPN server address and port.

The screenshot shows the 'VPN > SSL VPN' configuration page. The 'General Settings' section includes an 'Enable' toggle switch which is turned on. Below it is a link for 'SSL VPN Configuration Download' and a green 'Download' button. The 'VPN Server Address' section contains fields for 'Type' (set to 'Nebula Assigned Domain Name'), 'Domain Name', 'Binding Address' (set to 'auto'), 'Server Port' (set to '10443'), and 'Zone' (set to 'none').

2. Select "Nebula identity federation service as Primary Server at Authentication section.



Authentication ⓘ

Primary Server: Nebula identity federation service ▼

ⓘ Please complete the Nebula Identity Federation Service settings in the Nebula portal.

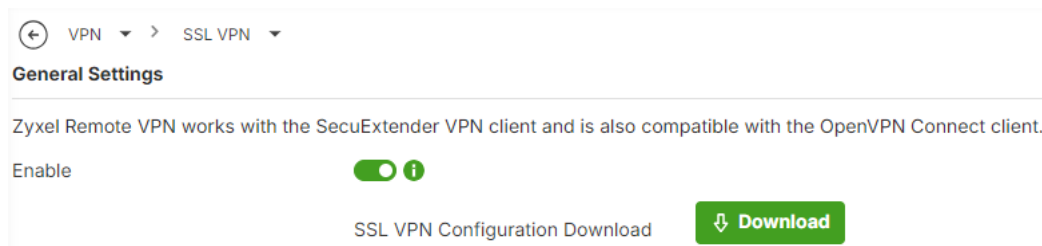
3. Continue to finish the SSL VPN setting for tunnel mode and client network, and click Apply

How to connect the SSL VPN via OpenVPN connect

You need to download OpenVPN connect application first.

1. Download the OpenVPN connect script.

Local Web GUI



VPN > SSL VPN

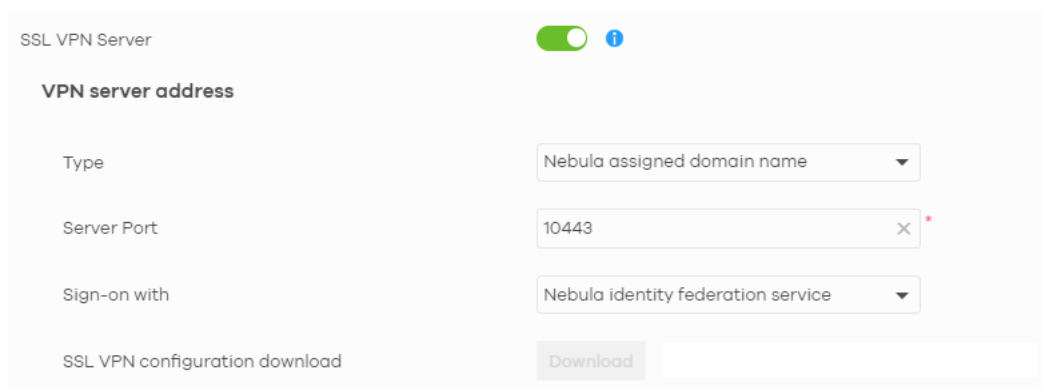
General Settings

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

Enable ☒ ⓘ

SSL VPN Configuration Download [Download](#)

Nebula GUI



SSL VPN Server ☒ ⓘ

VPN server address

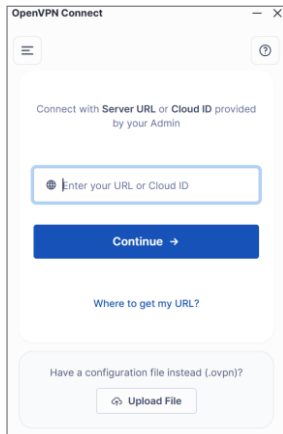
Type: Nebula assigned domain name ▼

Server Port: 10443 ✕

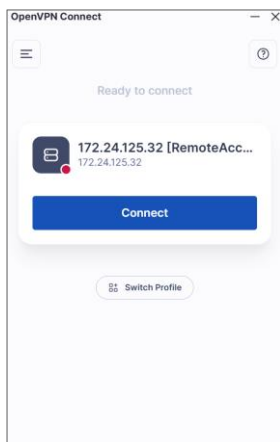
Sign-on with: Nebula identity federation service ▼

SSL VPN configuration download [Download](#)

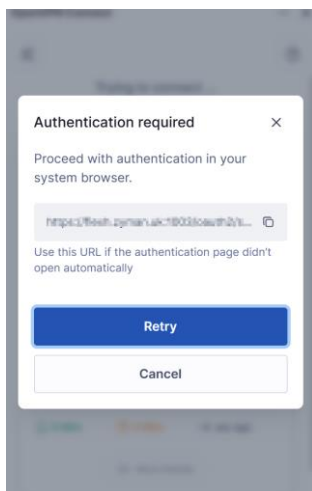
2. Click Upload File on OpenVPN connect



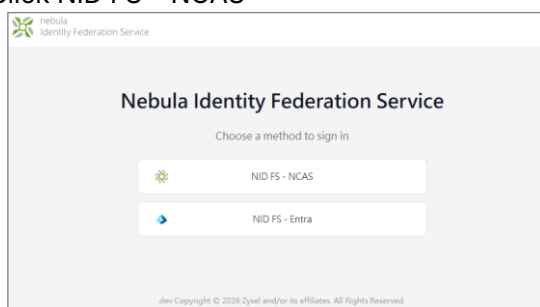
3. Select the uploaded profile and click Connect



4. After you seeing this message, the browser will automatically redirect to the login page.
If not, you can copy the URL and manually paste on the browser.

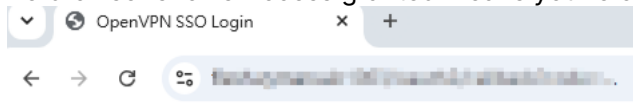


5. Click NID FS – NCAS



Enter in the credentials

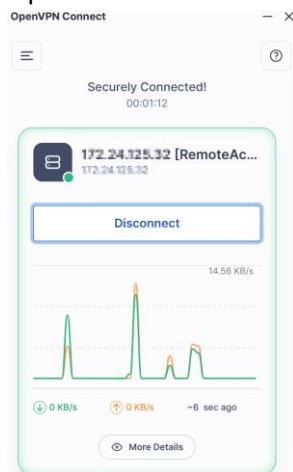
6. The browser shows Access granted means you're connected.



Access granted

You can close this window now.

OpenVPN connect shows Securely Connected!



Verification & Log Inspection

Login User Status (Network Status > Login Users)

Login Users									
Lockout IPs									
Force Log Out Search insights									
#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info	
1	admin	admin	console	22:07:00	console	0.0.0.0	22:44:44	admin(admin)	
2	admin	admin	172.24.125.68	0:46:05	http/https	0.0.0.0	23:59:59	admin(admin)	
3	*****@outlook.com (Auth Source: NID FS - Entra)	nidsf-user	172.24.125.68	0:00:07	sslvpn	192.168.51.2	23:59:53	nidsf-user(nidsf-users)	

System Event Logs:

Go to 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		
1	2026-07-1...	SSL VPN	SSL VPN client IP assigned 192.168.51.2 [profile0] idp=NID FS - Entra	172.24.125.68	0.0.0.0	0	account *****@outlook.com		
2	2026-07-1...	SSL VPN	SSL VPN Tunnel established idp=NID FS - Entra	172.24.125.68	0.0.0.0	0	account *****@outlook.com		
3	2026-07-1...	User	NIDFS-User *****@outlook.com(MAC=) from sslvpn has tunnel assigned Device (tunnel_ip=192.168.51.2)	172.24.125.68	0.0.0.0	0	Account: *****@outlook.com		
4	2026-07-1...	SSL VPN	Provision sslvpn user *****@outlook.com get sslvpn config success.	0.0.0.0	0.0.0.0	0			
5	2026-07-1...	User	NIDFS-User *****@outlook.com(MAC=) from sslvpn has logged in Device	172.24.125.68	0.0.0.0	0	Account: *****@outlook.com		
6	2026-07-1...	SSL VPN	TLS: Username/Password authentication deferred for username 'idp_auth' [CN SET]	0.0.0.0	0.0.0.0	0			
7	2026-07-1...	SSL VPN	VERIFY OK: depth=0, CN=SSLVPN_CLIENT_7049A21DB051	0.0.0.0	0.0.0.0	0			
8	2026-07-1...	SSL VPN	VERIFY OK: depth=1, CN=SSLVPN_CA_7049A21DB051	0.0.0.0	0.0.0.0	0			

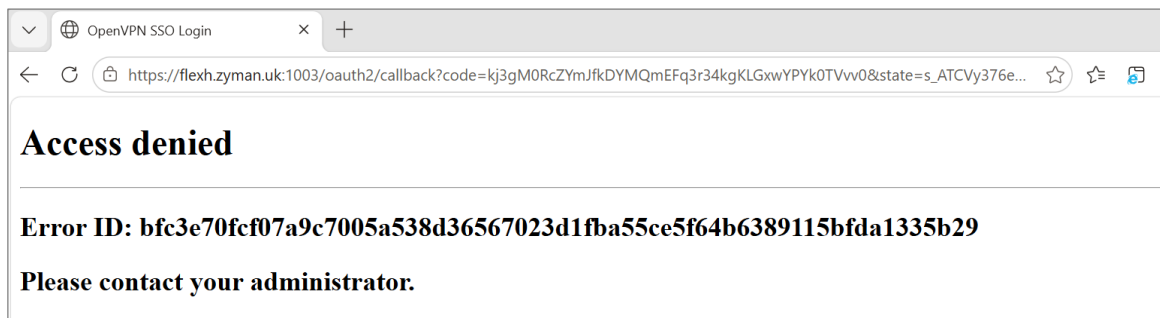
The category type is User and the message will see the NIDFS user information example:
NIDFS-User *****@example.com.tw(MAC=...) from sslvpn has logged in Device.

Error Handling

Common Error Pages:

1. User Access denied

Cause: The SSL VPN user does not have user privilege.



2. Nebula Pro Pack License Expired

Cause: Device lacks an active Nebula Professional Pack or Gold Pack license.

