

# 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 1.38

Apr. 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 ..... 55

How to Configure Route-Based VPN ..... 66

How to Use Tailscale..... 78

How to use Ext-group user to connect Remote Access VPN..... 89

How to Configure SSL VPN Access Profile ..... 92

**Chapter 2- Security Service** ..... 98

How to Block HTTPS Websites Using Content Filtering and SSL Inspection ..... 98

How to Configure Content Filter with HTTPs Domain Filter ..... 107

How to Block Facebook Using a Content Filter Block List ..... 112

How to block YouTube access by Schedule ..... 116

How to Control Access to Google Drive ..... 125

How to Block the Spotify Music Streaming Service ..... 133

How does Anti-Malware Work ..... 136

How to Detect and Prevent TCP Port Scanning with DoS Prevention ..... 139

How to block the client from accessing to certain country using Geo IP? ..... 143

How to Use Sandbox to Detect Unknown Malware? ..... 148

How to Configure Reputation Filter- IP Reputation..... 151

How to Configure Reputation Filter- URL Threat Filter..... 156

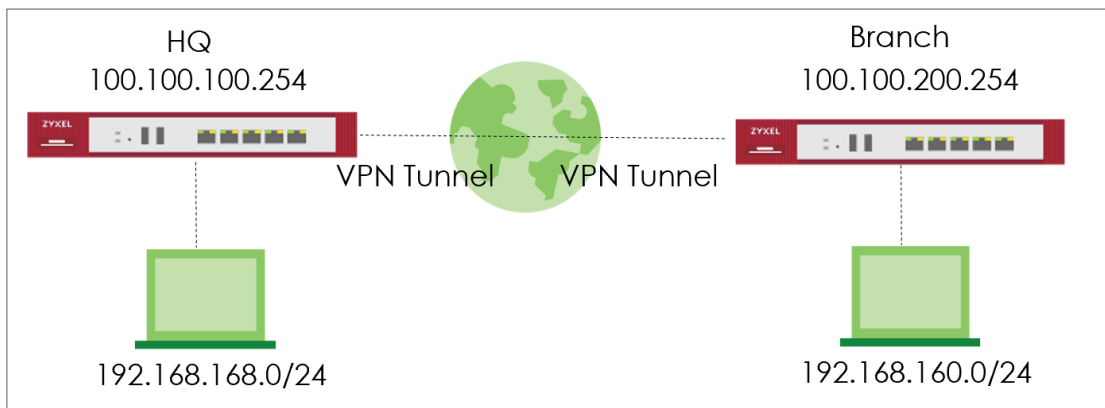
How to Configure Reputation Filter- DNS Threat Filter .....	160
How to Configure DNS Content Filter .....	164
External Block List for Reputation Filter .....	169
How to set up DNS SafeSearch? .....	174
<b>Chapter 3- Authentication</b> .....	182
How to Use Two Factor with Google Authenticator for Admin Access .....	182
How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN .....	189
How to set up AD authentication with Microsoft AD .....	199
How to Set Up Captive Portal?.....	204
Captive Portal authentication with Google.....	213
Captive Portal authentication with Microsoft Entra ID .....	233
SSLVPN authentication with Google .....	252
SSLVPN authentication with Microsoft Entra ID .....	264
Captive Portal authentication with Microsoft Entra ID Group .....	274
<b>Chapter 4- Maintenance</b> .....	280
How to Manage Configuration Files .....	280
How to Manage Firmware .....	284
How to set up configuration file backup rotation .....	286
<b>Chapter 5- Others</b> .....	290
How to Setup and Configure Daily Report .....	290
How to Setup and Send Logs to a Syslog Server .....	295
How to Setup and Send logs to the USB storage .....	298
How to Perform and Use the Packet Capture Feature .....	300
How to Allow Public Access to a Server Behind USG FLEX H.....	304
How to Configure DHCP Option 60 – Vendor Class Identifier .....	308
How to Configure Session Control .....	310

How to Configure Bandwidth Management for FTP Traffic .....	313
How to Configure WAN trunk for Spillover and Least Load First .....	318
How Does SIP Pinhole Function Work on USG FLEX H? .....	324
How to Deploy Device HA .....	329
How to check Packet Flow Explorer .....	342
How to set up a Link Aggregation Group (LAG) interface .....	348
How to Set Up AP Control Service for Zyxel APs .....	354
How to set up SMTP with Microsoft OAuth2.0? .....	359
How to Configure IGMP Proxy .....	372
How to Configure Application-Based Policy Route .....	378
<b>Chapter 6- Nebula</b> .....	<b>381</b>
How to Set Up Nebula site-to-site VPN on the USG FLEX H? .....	381
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)? .....	385
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)? .....	389
How to Onboard Firewall to Nebula within Initial Setup Wizard .....	393
How to Configure Remote Access VPN with Nebula Cloud Authentication? .....	406
How to Configure CDR on Nebula .....	428

## 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 navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area is titled 'VPN > Site to Site VPN' and has a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are: \*Name: HQtoBranch; IKE Version: IKEv2 (selected); Type: Site-to-Site (selected); Behind NAT: None (selected). Below the fields is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is connected to a 'Remote Site'. At the bottom 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	<input type="text" value="100.100.100.254"/>
Peer Gateway Address	Domain Name / IP	<input type="text" value="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

Remote Subnet

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

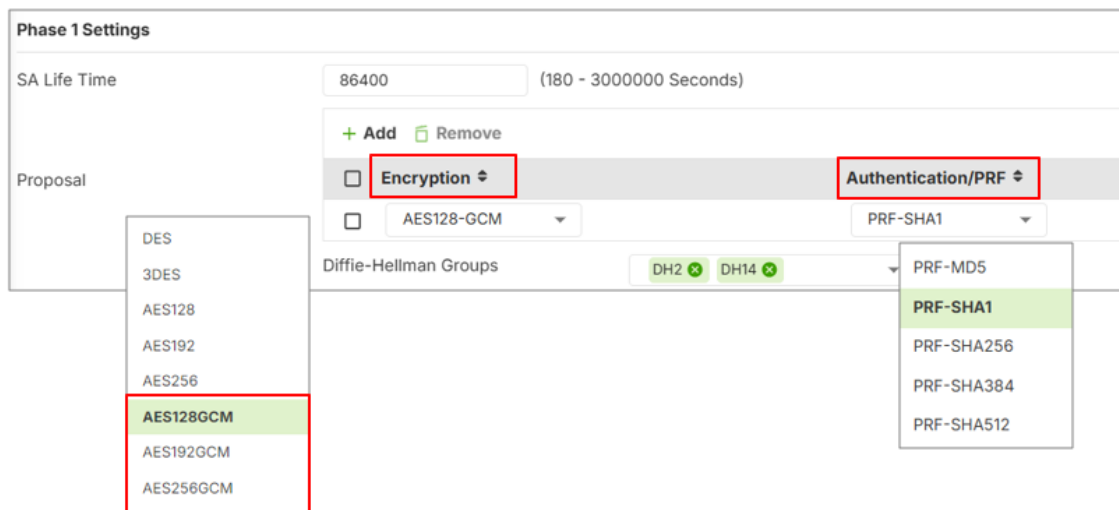
**Policy & Routing**

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.



**Phase 1 Settings**

SA Life Time: 86400 (180 - 3000000 Seconds)

Proposal:

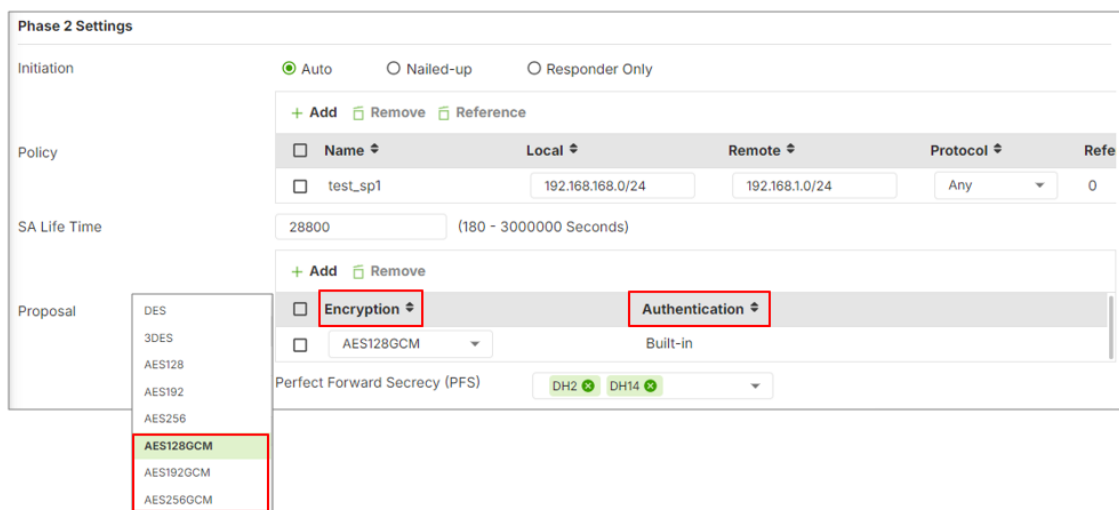
- Encryption: AES128-GCM
- Authentication/PRF: PRF-SHA1

Diffie-Hellman Groups: DH2, DH14

Encryption options: DES, 3DES, AES128, AES192, AES256, **AES128GCM**, AES192GCM, AES256GCM

PRF options: PRF-MD5, **PRF-SHA1**, PRF-SHA256, PRF-SHA384, PRF-SHA512

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



**Phase 2 Settings**

Initiation:  Auto  Nailed-up  Responder Only

Policy:

Name	Local	Remote	Protocol	Refe
test_sp1	192.168.168.0/24	192.168.1.0/24	Any	0

SA Life Time: 28800 (180 - 3000000 Seconds)

Proposal:

- Encryption: AES128GCM
- Authentication: Built-in

Perfect Forward Secrecy (PFS): DH2, DH14

Encryption options: DES, 3DES, AES128, AES192, AES256, **AES128GCM**, AES192GCM, AES256GCM

## 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 displays the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area shows the configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active, with the following settings: \*Name: BranchtoHQ, IKE Version: IKEv2, Type: Site-to-Site, and Behind NAT: None. A diagram below shows a Local Site connected to an Internet cloud, which is 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

Peer Gateway Address Domain Name / IP



Local Site  
100.100.200.254

Internet

Remote Site  
100.100.100.254

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

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

The screenshot shows a configuration wizard for Site to Site VPN. The breadcrumb path is VPN > Site to Site VPN. The wizard has five steps: 1. Scenario (checked), 2. Network (checked), 3. Authentication (active), 4. Policy & Routing, and 5. Summary. Under the Authentication step, there are two radio button options: 'Pre-Shared Key' (selected) and 'Certificate'. A text input field for the Pre-Shared Key is highlighted with a red box and contains seven dots. Below the input field is a dropdown menu with 'default' selected. At the bottom of the form, there are three buttons: 'Cancel', 'Back', and 'Next' (highlighted in green).

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

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

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. At the top, a progress bar indicates the current step is 4 of 5: Scenario (checked), Network (checked), Authentication (checked), Policy & Routing (active), and Summary (disabled). Below the progress bar, the 'Type' is set to 'Policy-Based' (selected with a radio button). The 'Local Subnet' is configured as '192.168.160.0/24' and the 'Remote Subnet' is '192.168.168.0/24', both fields are highlighted with red boxes. A network diagram below shows a 'Local Site' (100.100.200.254) connected to an 'Internet' cloud, which is then connected to a 'Remote Site' (100.100.100.254). The local site is associated with the subnet 192.168.160.0/24, and the remote site is associated with 192.168.168.0/24. At the bottom of the page, there are 'Cancel', 'Back', and 'Finish' buttons.

**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. On the left is the 'Network Connection Details' window for the Intel(R) Ethernet Connection. On the right is an Administrator Command Prompt window showing the execution of a ping command to 192.168.160.1.

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

The screenshot shows the 'VPN Status' interface with the 'IPsec VPN' section selected. A table lists the VPN connections, and a 'Connectivity Check' dialog box is open, showing a successful test result for the IP address 192.168.160.1.

#	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

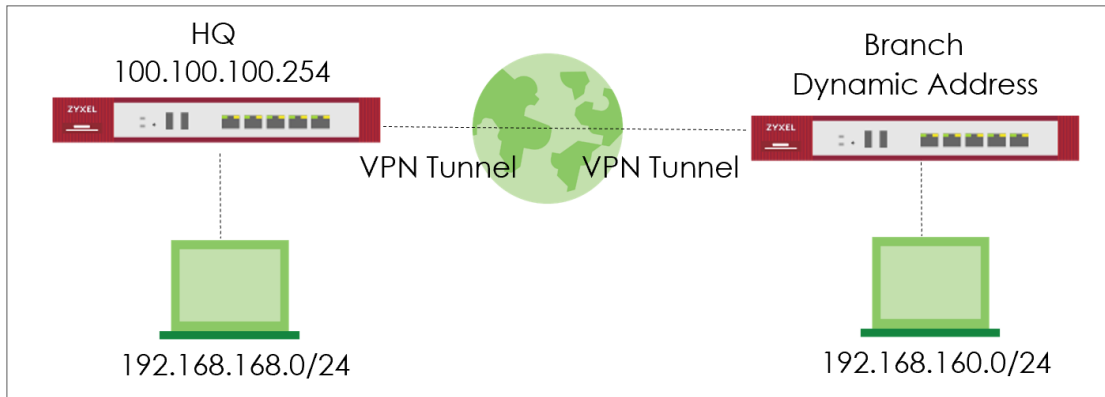
**Connectivity Check**

IP Address: 192.168.160.1

Result: ICMP Connectivity Check PASS on sec\_policy1\_HQtoBranch

## 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**.

The screenshot shows the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The 'VPN' section is expanded, and 'Site to Site VPN' is selected. The main area shows a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are:
 

- \*Name: HQtoBranch
- IKE Version:  IKEv1,  IKEv2
- Type:  Site-to-Site,  Custom

 At the bottom, there are 'Cancel' and 'Next' buttons.

### VPN > Site to Site VPN

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

The screenshot shows the ZyXel VPN configuration interface for the 'Network' and 'Authentication' steps. The configuration fields are:
 

- General Settings:**
  - Enable:
  - Name: HQtoBranch
  - IKE Version:  IKEv1,  IKEv2
  - Type:  Route-Based,  Policy-Based
- Network:**
  - My Address: Domain Name / IP: 100.100.100.254
  - Peer Gateway Address:  Domain Name / IP,  Dynamic Address
- Authentication:**
  - Authentication:  Pre-Shared Key,  Certificate
  - Pre-Shared Key: [Redacted]
  - Certificate: default

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](#)

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

Rows per page: 50 1 of 1 < 1 >

SA Life Time  (180 - 3000000 Seconds)

Proposal

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

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

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups

## 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**.

The screenshot shows the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The 'VPN' section is expanded, and 'Site to Site VPN' is selected. The main area shows a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are: \*Name: BranchtoHQ; IKE Version: IKEv2 (selected); Type: Custom (selected). There are 'Cancel' and 'Next' buttons at the bottom.

### VPN > Site to Site VPN

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

The screenshot shows the ZyXel VPN configuration interface for the 'Network' and 'Authentication' steps. The 'General Settings' section has 'Enable' turned on, 'Name' as BranchtoHQ, 'IKE Version' as IKEv2, and 'Type' as Policy-Based. The 'Network' section has 'My Address' set to 0.0.0.0 and 'Peer Gateway Address' set to 100.100.100.254. The 'Authentication' section has 'Pre-Shared Key' selected with a masked key field. There are 'Cancel' and 'Next' buttons at the bottom.

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

Phase 2 Settings

Initiation  Auto  Nailed-up  Responder Only

Policy

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

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

Rows per page: 50 1 of 1 < 1 >

SA Life Time  (180 - 3000000 Seconds)

Proposal

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

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

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups

## Test IPsec VPN Tunnel

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

**Network Connection Details**

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

**Administrator: Command Prompt**

```

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

C:\WINDOWS\system32>ping 192.168.160.1

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

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

C:\WINDOWS\system32>
    
```

### VPN Status > IPsec VPN

Verify the IPsec VPN status and do the Connectivity Check

**VPN Status > IPsec VPN > Site to Site VPN**

Site to Site VPN | Remote Access VPN

Disconnect Refresh **Connectivity Check**

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

**Connectivity Check**

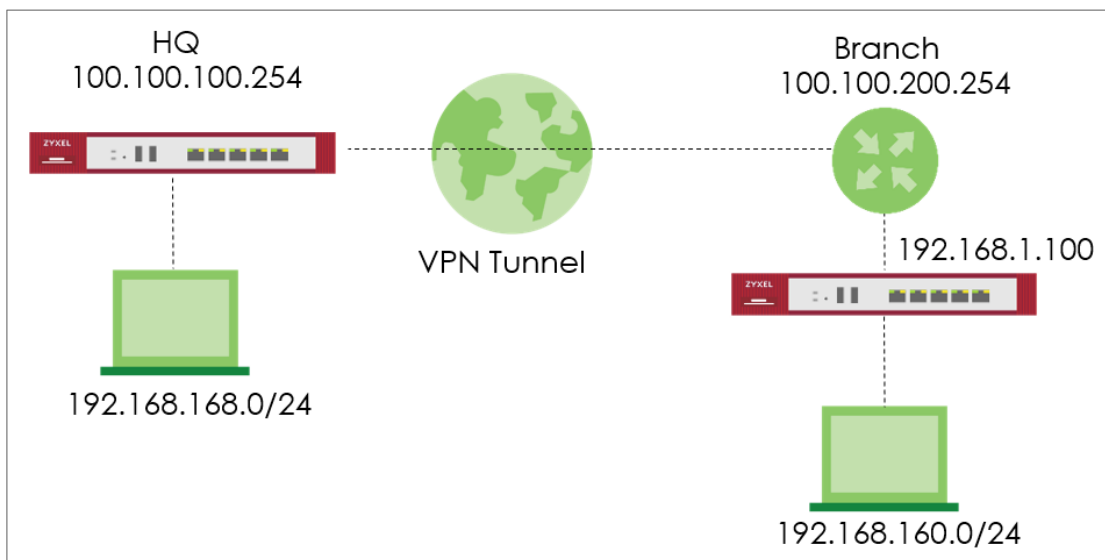
IP Address: 192.168.160.1 **Test**


Result: ICMP Connectivity Check PASS on sec\_policy1\_HQtoBranch

**OK**

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

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



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

## Set up IPsec VPN Tunnel for HQ

### VPN > Site to Site VPN > Scenario

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

The screenshot displays the ZyXel VPN configuration wizard, Step 1: Scenario. The interface includes a search bar and a navigation menu on the left. The main content area shows the configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The configuration options are as follows:

- Name: HQtoBranch
- IKE Version:  IKEv2
- Config Type:  Wizard
- Behind NAT:  Remote Site

Below the form is a diagram illustrating the network topology: a Local Site is connected to an Internet cloud, which is connected to a Router, which is connected to a Remote Site. The 'Next' button is highlighted in green.

**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**

The screenshot shows the configuration page for Site to Site VPN Authentication. At the top, a breadcrumb trail reads 'VPN > Site to Site VPN'. Below this is a progress indicator with five steps: 'Scenario' (checked), 'Network' (checked), '3 Authentication' (active), '4 Policy & Routing', and '5 Summary'. The 'Authentication' section has two radio button options: 'Pre-Shared Key' (selected) and 'Certificate' (with a 'Beta' label). The 'Pre-Shared Key' field is a text input containing seven dots, with a red box around it and a toggle icon to its right. Below the key field is a dropdown menu currently set to 'default'. At the bottom of the page, there are three buttons: 'Cancel', 'Back', and 'Next'.

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

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

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. At the top, a progress bar indicates the current step is 4 of 5. Below the progress bar, the 'Type' is set to 'Policy-Based'. The 'Local Subnet' is configured as '192.168.168.0/24' and the 'Remote Subnet' is '192.168.160.0/24'. A network diagram below shows a 'Local Site' (100.100.100.254) connected to the 'Internet', which is connected to a 'Router', which is connected to a 'Remote Site' (Dynamic Address, 192.168.160.0/24). At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**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.

The screenshot shows a web interface for configuring a Site to Site VPN. At the top, there is a breadcrumb trail: VPN > Site to Site VPN. Below this is a progress indicator with five steps: Scenario, Network, Authentication, Policy & Routing, and Summary. The Summary step is highlighted with a green circle containing the number 5. The main content area is titled 'Configuration' and contains the following details:

Name	HQtoBranch
IKE Version	2
Type	Policy-based

Below the configuration details is a 'Proposal' section with a dropdown arrow. An 'Edit' button is located in the top right corner of the configuration area. The configuration is divided into three sections:

- Network**: Local Site is 100.100.100.254. Remote Site is empty.
- Authentication**: Authentication is pre-shared-key. A masked input field with a copy icon is visible.
- Policy & Routing**: Local Subnet is 192.168.168.0/24.

A green 'Close' button is located in the bottom right corner of the configuration area.

## 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**.

The screenshot displays the ZyXel VPN configuration wizard, Step 1: Scenario. The interface includes a search bar, a navigation menu on the left, and a progress indicator at the top showing five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Site to Site VPN' option in the navigation menu is highlighted with a red box. The configuration form contains the following fields and options:

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

Below the form is a diagram illustrating the VPN setup: a Local Site (represented by a server rack icon) is connected to a Router (represented by a router icon), which is connected to the Internet (represented by a cloud icon), which is then connected to a Remote Site (represented by a server rack icon). At the bottom of the wizard, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted in green.

**VPN > Site to Site VPN > Scenario > Network**

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

VPN > Site to Site VPN

Scenario 2 Network 3 Authentication 4 Policy & Routing 5 Summary

My Address Domain Name / IP 192.168.1.100

Peer Gateway Address Domain Name / IP 100.100.100.254

Local Site 192.168.1.100 Router Internet Remote Site 100.100.100.254

Cancel Back Next

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

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

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

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

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

Below the form is a network diagram. On the left, a 'Local Site' (represented by a server rack icon) is connected to a 'Router' (represented by a router icon). The Local Site has an associated IP address of 192.168.1.100. The Router is connected to an 'Internet' cloud. The Internet cloud is connected to a 'Remote Site' (represented by a server rack icon). The Remote Site has an associated IP address of 100.100.100.254. On the far left, there is a group of computer icons with the IP address 192.168.160.0/24. On the far right, there is another group of computer icons with the IP address 192.168.168.0/24.

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

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

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

The screenshot shows a configuration wizard for Site to Site VPN. At the top, there is a breadcrumb trail: VPN > Site to Site VPN. Below this is a progress indicator with five steps: Scenario (checked), Network (checked), Authentication (active, highlighted with a green circle and number 3), Policy & Routing (4), and Summary (5). The main content area is titled 'Authentication' and contains two radio button options: 'Pre-Shared Key' (selected) and 'Certificate' (with a 'Beta' label). The 'Pre-Shared Key' option has a text input field containing seven dots, a red rectangular highlight around the dots, and a small icon to its right. Below the 'Certificate' option is a dropdown menu with 'default' selected. At the bottom of the form, there are three buttons: 'Cancel' on the left, 'Back' in the center, and 'Next' on the right.

**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	

[Edit](#)

**Network**

Local Site	192.168.1.100
Remote Site	100.100.100.254

**Authentication**

Authentication	pre-shared-key	.....
----------------	----------------	-------

**Policy & Routing**

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

[Close](#)

## Test IPsec VPN Tunnel

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

The screenshot displays two windows side-by-side. On the left is the 'Network Connection Details' window for the Intel(R) Ethernet Connection. On the right is an Administrator Command Prompt window showing the execution of a ping command to 192.168.160.1.

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 Tcpi...	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

The screenshot shows the VPN Status interface with a table of connections and a Connectivity Check dialog box. The table shows a connection named 'HQtoBranch' with a status of 'Connected'. The Connectivity Check dialog shows a successful result for IP address 192.168.160.1.

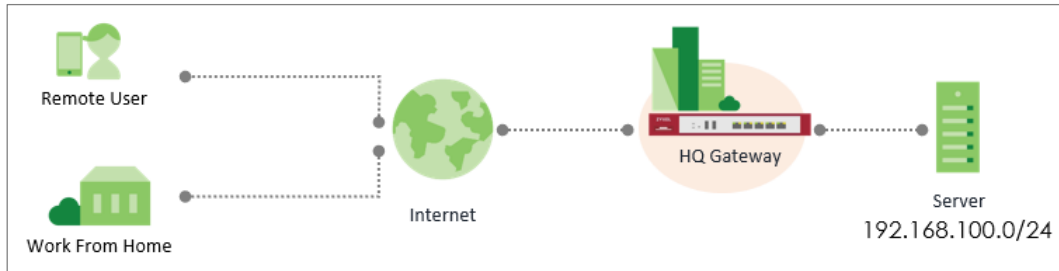
#	Name	Policy Route	Remote Gateway	My Address
1	HQtoBranch	192.168.168.0/24 <=> 192.168.160.0/24	100.100.200.254	100.100.100.254

Connectivity Check dialog box details:

- IP Address: 192.168.160.1
- Result: ICMP Connectivity Check PASS on sec\_policy1\_HQtoBranch

## 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.

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

**Profile Management**

User Name:

User Type:

Password:

Retype:

Description:

Email 1:

Email 2:

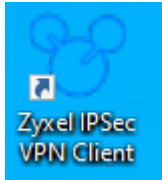
Mobile Number:

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

A screenshot of the Zyxel VPN configuration interface. The left sidebar shows a navigation menu with "SSL VPN" highlighted. The main content area is titled "VPN > SSL VPN" and contains the following sections:

- General Settings:** Includes a note about compatibility with SecuExtender and OpenVPN clients, an "Enable" toggle switch (turned on), and a "Download" button for the SSL VPN Configuration.
- Incoming Interface:** Includes a dropdown menu for "Interface" (set to "ge1 (WAN)"), a text field for "DNS Name" (Optional), and a text field for "Server Port" (set to "10443").
- Clients will use VPN to access:** Includes an "Auto DNAT" toggle switch (turned on) and two radio button options: "Internet and Local Networks (Full Tunnel)" and "Local Networks Only (Split Tunnel)". The "Local Networks Only (Split Tunnel)" option is selected and highlighted with a red box.
- Local Networks:** A table with columns for "Add", "Edit", and "Remove". It contains one entry: "Network 0" with a checkbox and the IP address "192.168.100.0/24".
- Client Network:** Includes a text field for "IP Address Pool" (set to "192.168.51.0/24") and radio button options for "First DNS Server": "zyWALL" (selected) and "Custom Defined".

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

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: ge1

Domain Name / IP:

**Certificate for VPN Validation**

Auto: default

Manual:

**Clients will use VPN to access**

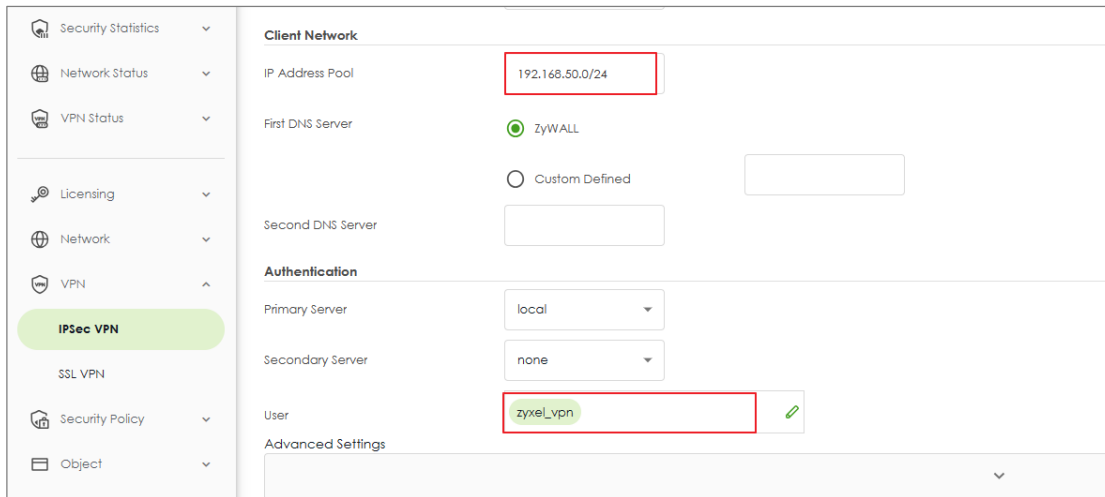
Internet and Local Networks (Full Tunnel)

Auto NAT:

Local Networks Only (Split Tunnel)

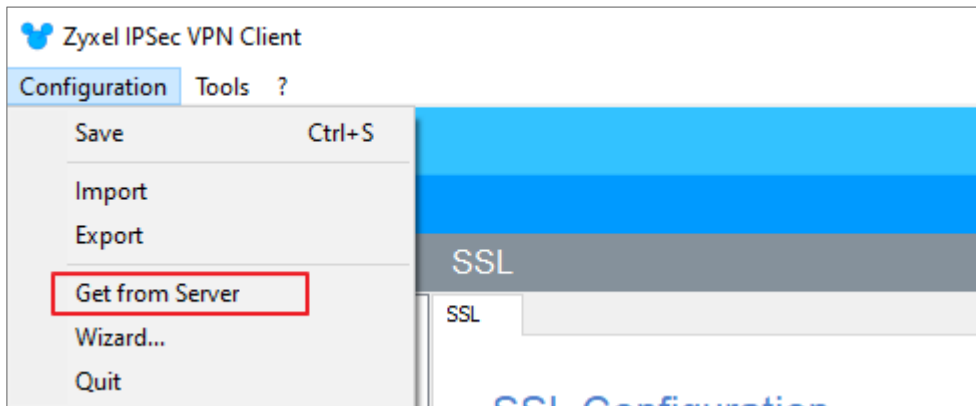
Local Network: 192.168.100.0/24

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

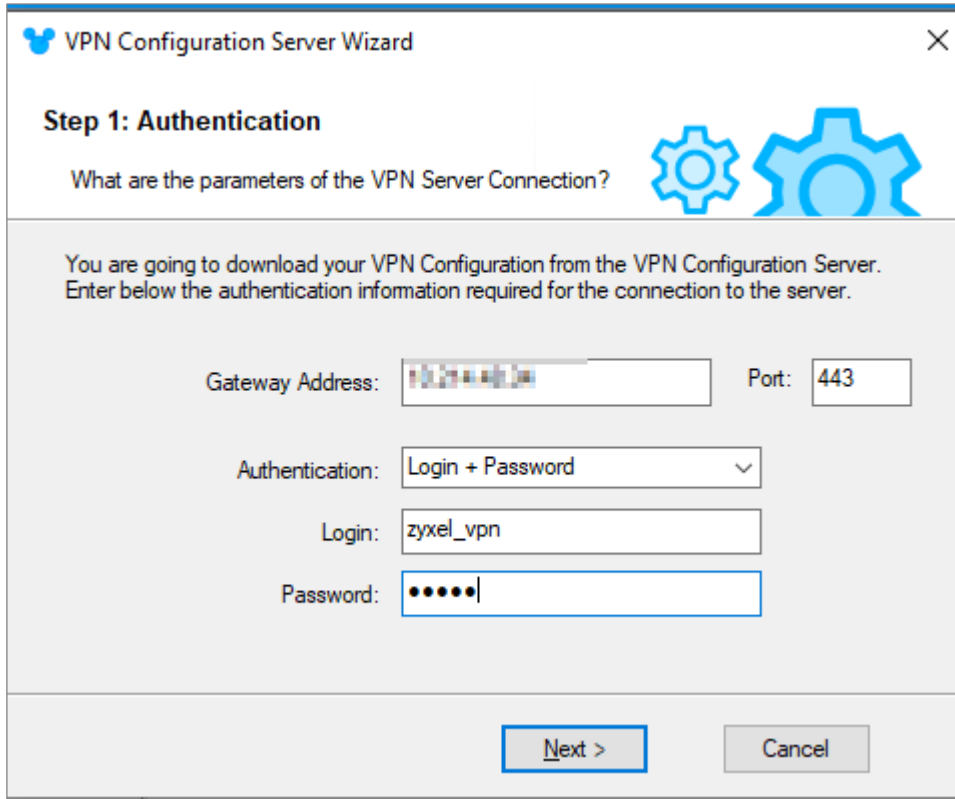


## Set up Remote Access on TGB Client

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

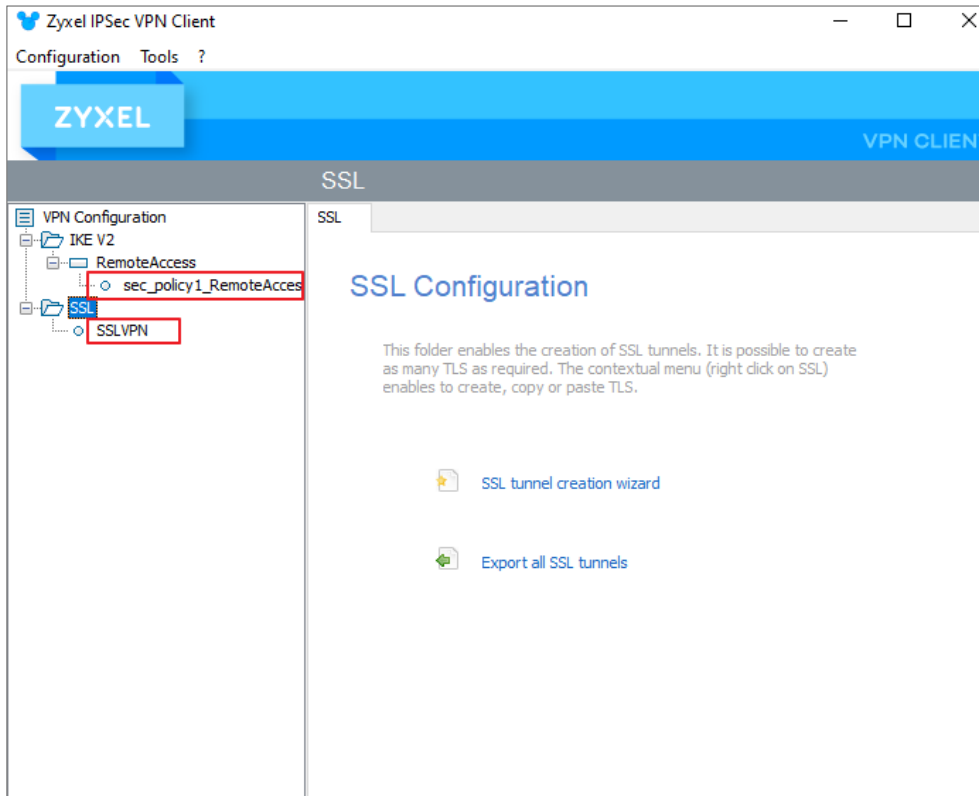


Input the Gateway Address, Username and password to fetch configuration file.



The image shows a 'VPN Configuration Server Wizard' dialog box. The title bar includes a blue icon and the text 'VPN Configuration Server Wizard' with a close button. The main content area is titled 'Step 1: Authentication' and contains the question 'What are the parameters of the VPN Server Connection?' followed by two gear icons. Below this, a grey box contains the instruction: '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.' The form fields are: 'Gateway Address:' with a text box containing '192.168.1.1', 'Port:' with a text box containing '443', 'Authentication:' with a dropdown menu set to 'Login + Password', 'Login:' with a text box containing 'zyxel\_vpn', and 'Password:' with a text box containing five dots. At the bottom, there are two buttons: 'Next >' and 'Cancel'.

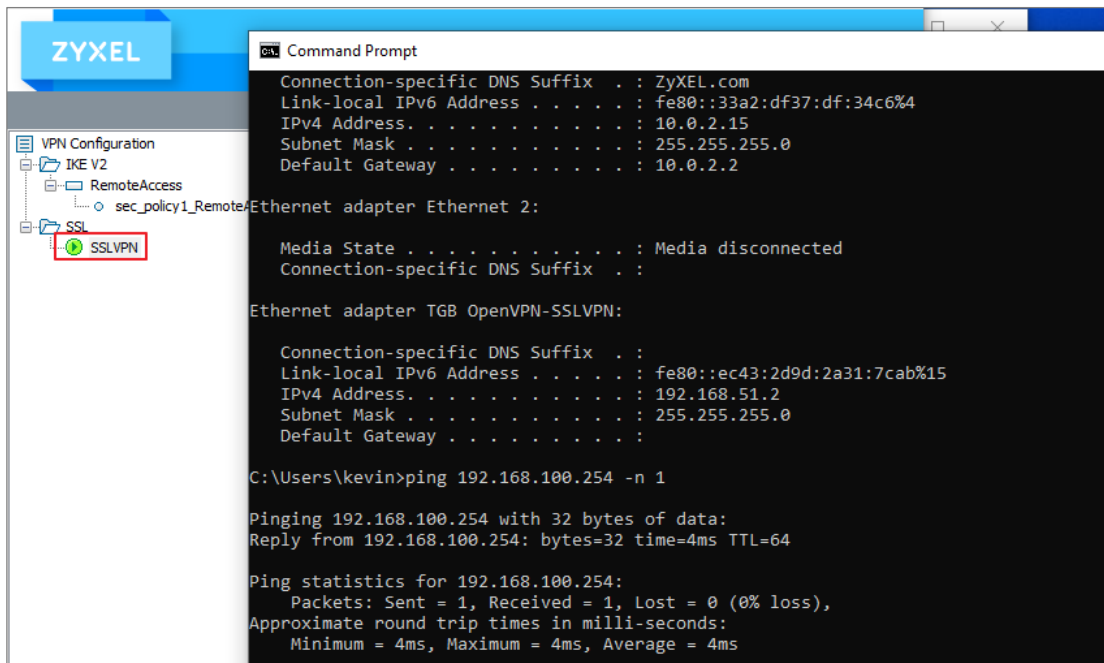
You will obtain IKEv2 as well as SSLVPN settings.



## Test SSLVPN Tunnel on TGB Client

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

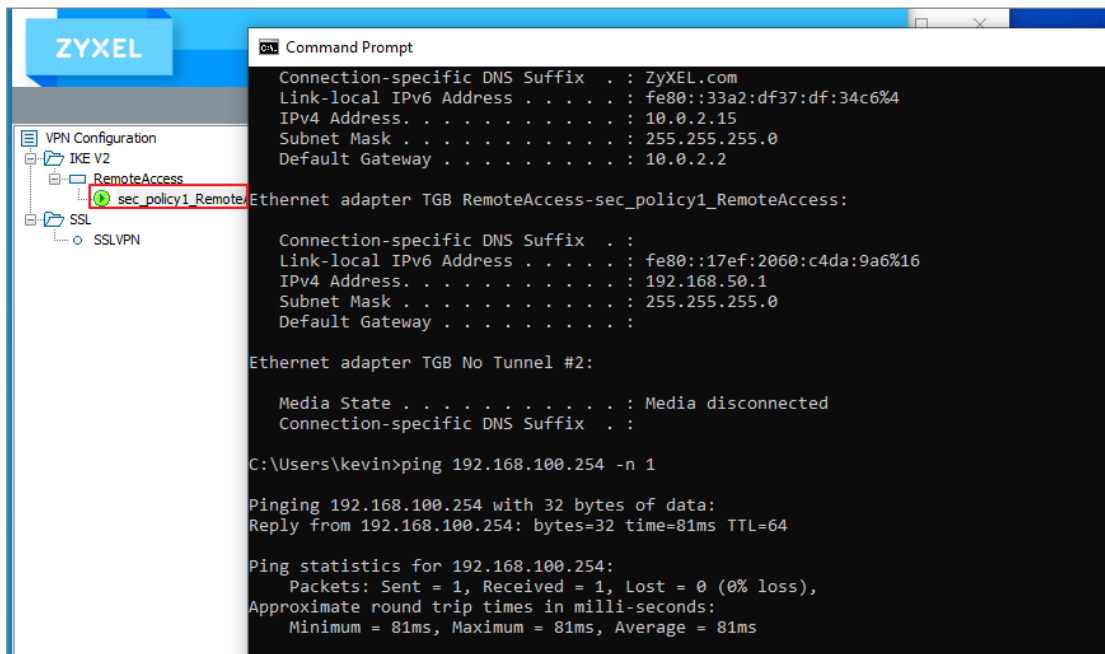
You will see the profile being green and can access internal resource now.



## Test IKEv2 Tunnel on TGB Client

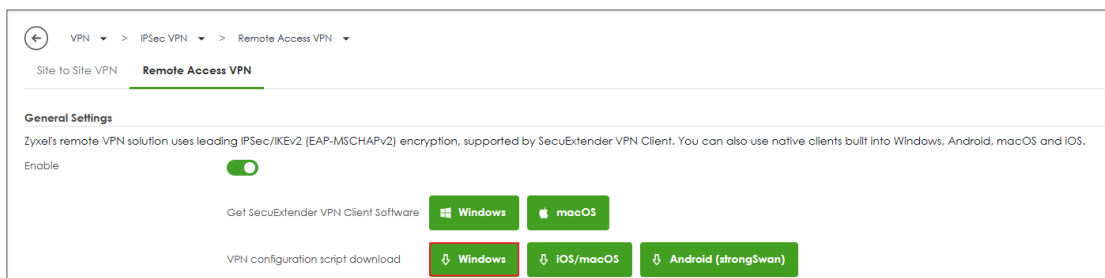
Right click the profile and "Open Tunnel" and log in.

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

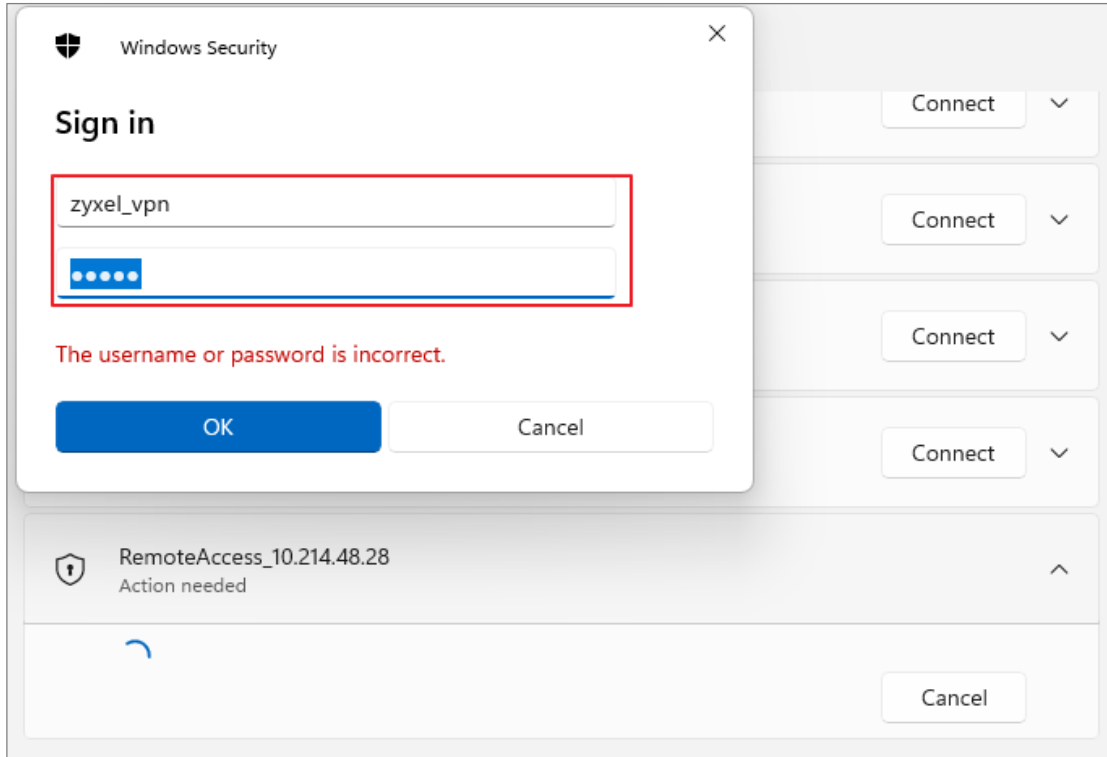


## Test IKEv2 Tunnel on Windows Client

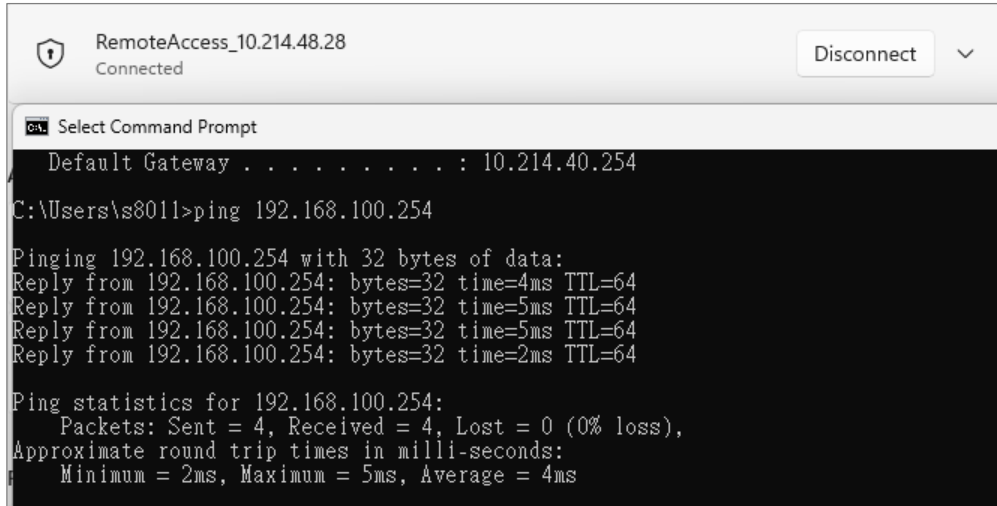
Download Windows VPN configuration script



Perform the windows bat file and input credentials.

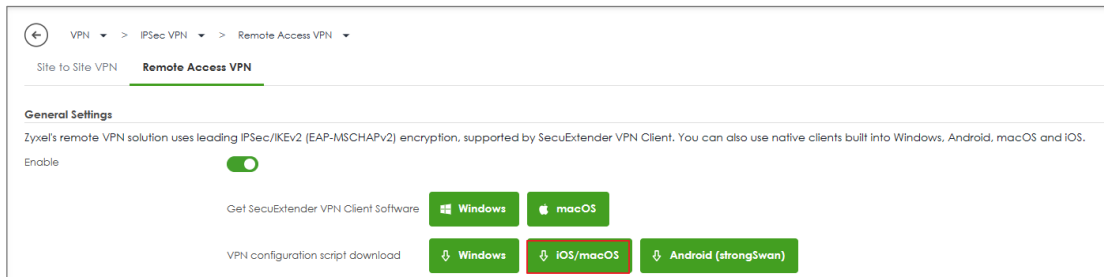


VPN is connected and can access internal resource.

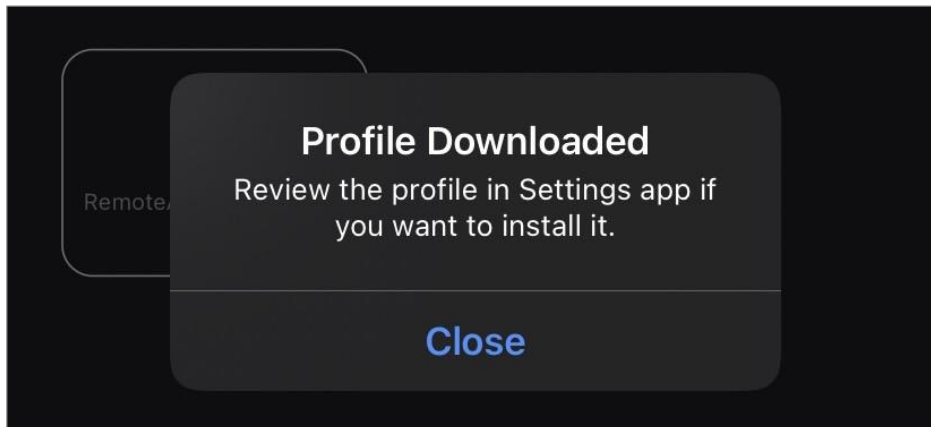


## Test IKEv2 Tunnel on iOS Client

Download iOS/macOS VPN configuration script.



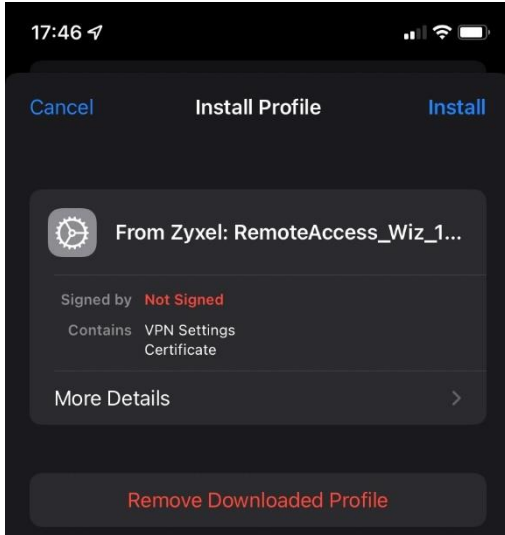
Send the script to Device.



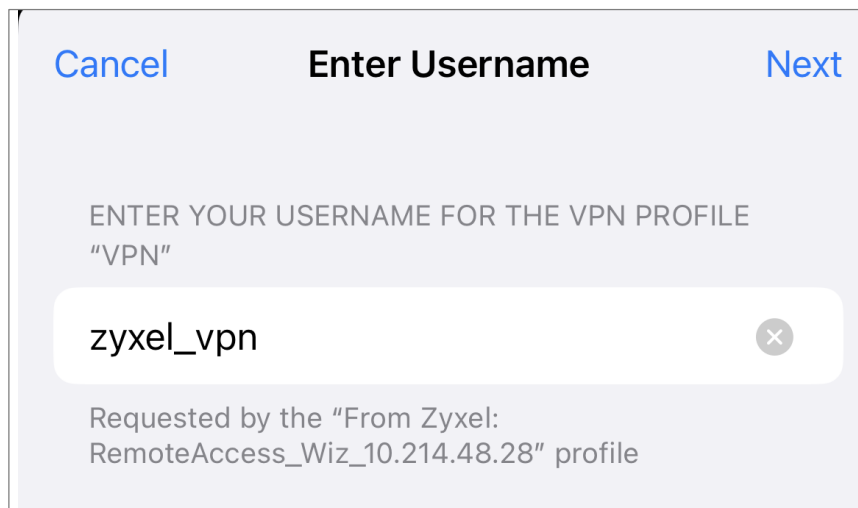
Settings > Profile Downloaded



Press Install.



Enter Username and Password.



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

ENTER YOUR PASSWORD FOR THE VPN PROFILE  
"VPN"

Requested by the "From Zyxel:  
RemoteAccess\_Wiz\_10.214.48.28" profile

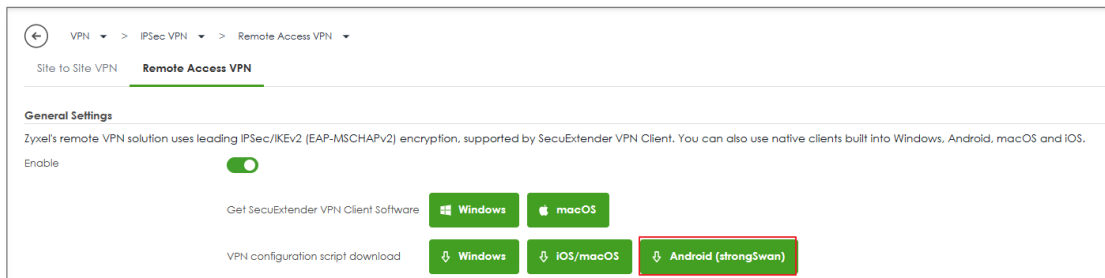
Now, it can connect.

[←](#) **RemoteAccess\_Wiz\_10.214.48.28** [Edit](#)

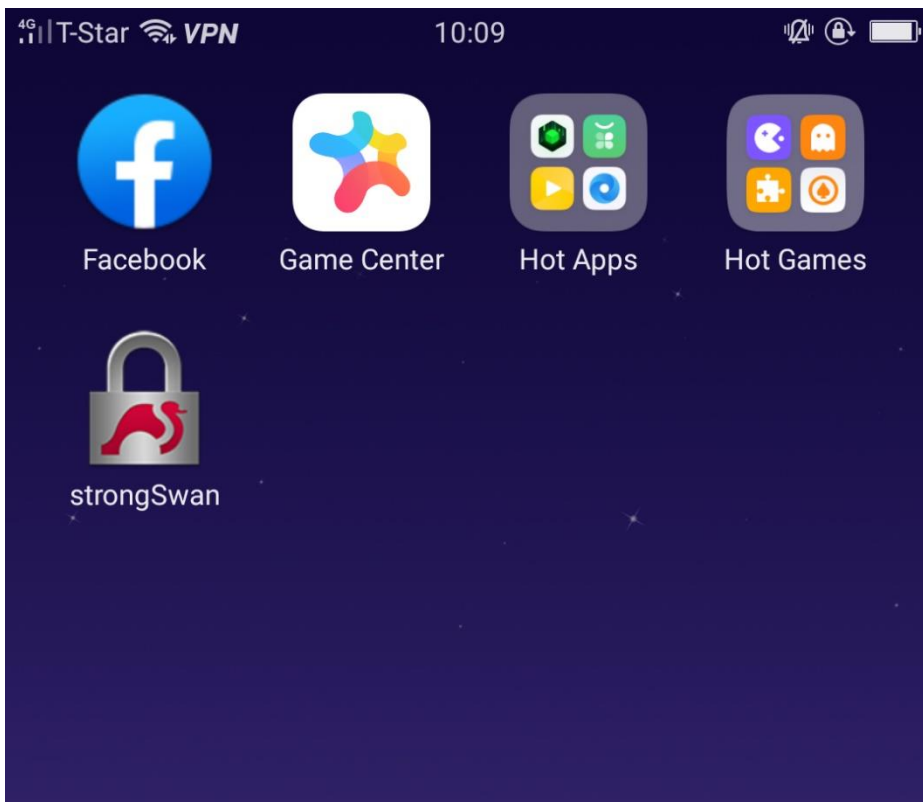
Type	IKEv2
Server	10.214.48.28
Account	zyxel_vpn
Address	192.168.50.1
Connect Time	0:09

## Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



Download strongSwan from Google Play Store.



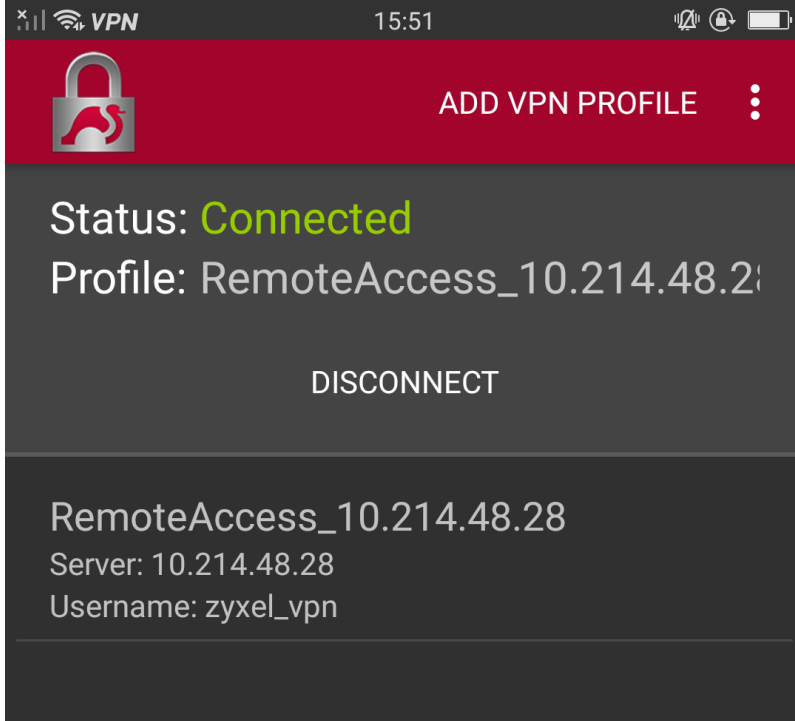
Send the script to device then Install and Import strongSwan profile.

The screenshot shows a mobile application interface for importing a VPN profile. The title bar is red and contains a close button (X), the text "Import VPN profile", and an "IMPORT" button. The main content area is dark grey and contains the following fields:

- 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 with dots)
- CA certificate: 10.214.48.28

The status bar at the top shows signal strength, Wi-Fi, time (15:51), and battery level.

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

DNS Name  (Optional)

Server Port

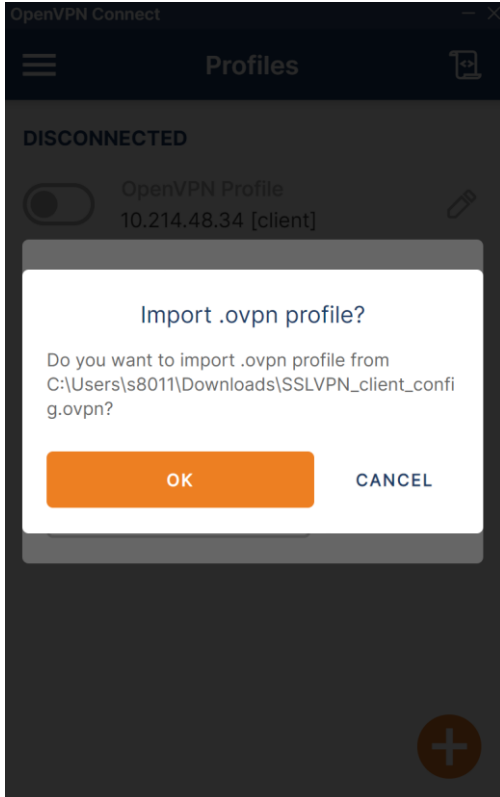
#### Clients will use VPN to access

Internet and Local Networks (Full Tunnel)

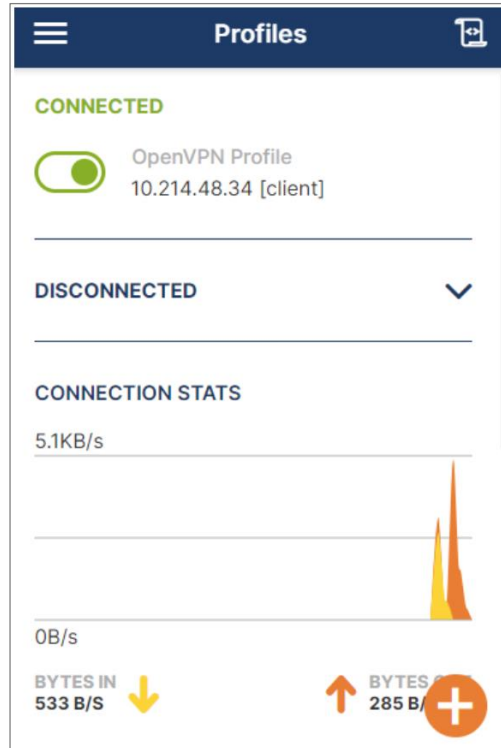
Auto SNAT

Local Networks Only (Split Tunnel)

Import the config file.

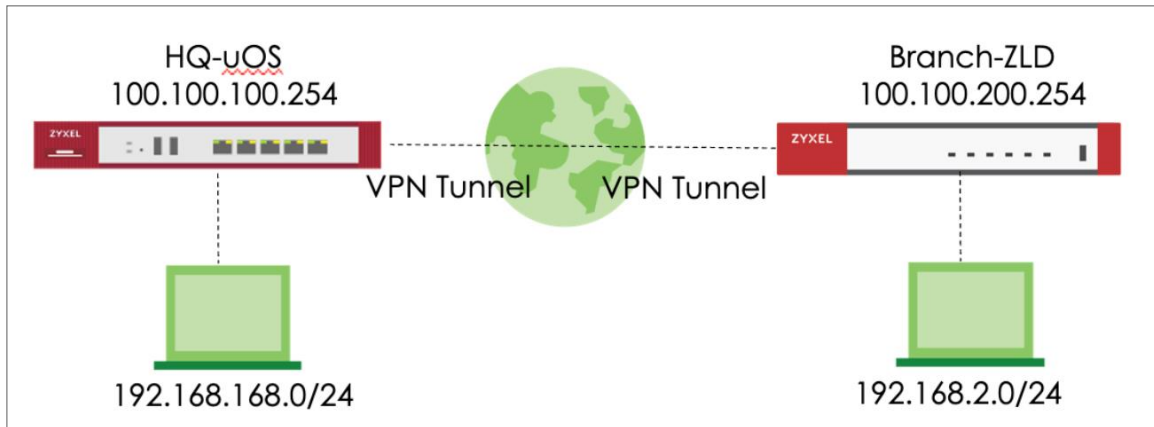


VPN is connected.



## 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**.

The screenshot displays the ZyXEL uOS configuration interface for a Site-to-Site VPN. The left sidebar contains a navigation menu with 'Site to Site VPN' highlighted. The main content area shows the 'Scenario' configuration step. The 'Name' field is set to 'HQ10FLEX'. The 'IKE Version' is set to 'IKEv2'. The 'Config Type' is set to 'Wizard'. The 'Behind NAT' option is set to 'None'. A diagram at the bottom shows a 'Local Site' connected to an 'Internet' cloud, which is connected to a 'Remote Site'. 'Cancel' and 'Next' buttons are at the bottom.

**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.

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. The breadcrumb trail is 'VPN > Site to Site VPN'. The progress bar indicates the current step is '4 Policy & Routing', with previous steps 'Scenario', 'Network', and 'Authentication' completed, and '5 Summary' remaining.

**Type:**  Route-Based  Policy-Based

**Local Subnet:** 192.168.168.0/24

**Remote Subnet:** 192.168.2.0/24

The network diagram below shows two sites connected via the Internet:

- Local Site:** 100.100.100.254 (connected to 192.168.168.0/24)
- Remote Site:** 100.100.200.254 (connected to 192.168.2.0/24)

Navigation buttons at the bottom include '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: HQtoFLEX  
IKE Version: 2  
Type: Policy-based  
Proposal: [dropdown]

**Network**

Local Site: 100.100.100.254  
Remote Site: 100.100.200.254

**Authentication**

Authentication: pre-shared-key [password field]

**Policy & Routing**

Local Subnet: 192.168.168.0/24

[Edit](#)

[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

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

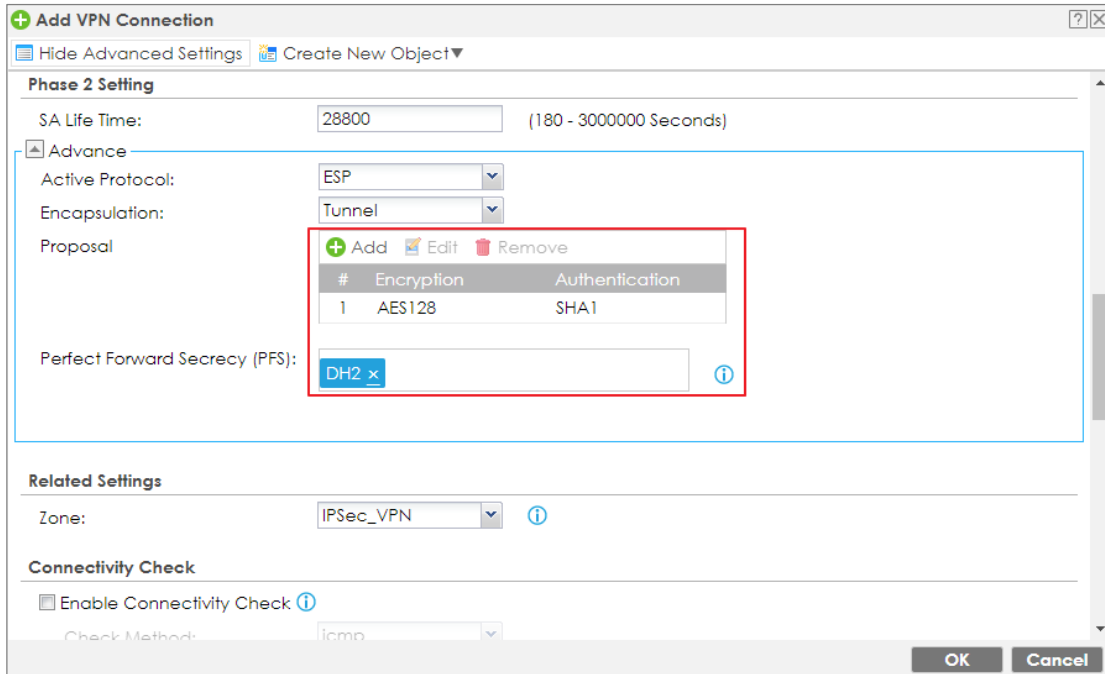
**Policy**

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.



## Test IPSec VPN Tunnel

### Ping the PC that is connected to ZLD device

Win 11 > cmd > ping 192.168.2.34

```

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

Ethernet adapter 4:

C:\Windows\system32>ping 192.168.2.34

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

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

### VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check

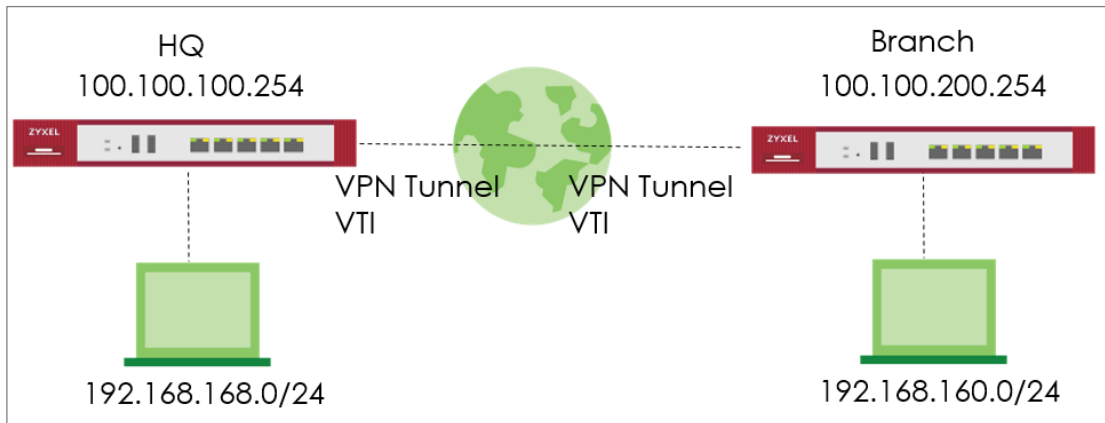
The screenshot shows the 'VPN Status' window with the 'IPSec VPN' tab selected. Under 'Site to Site VPN', there are buttons for 'Disconnect', 'Refresh', and 'Connectivity Check'. A table below lists the VPN configuration:

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

A 'Connectivity Check' dialog box is open on the right. It has an input field for 'IP Address' containing '192.168.160.1' and a green 'Test' button. The 'Result' area shows: 'ICMP Connectivity Check PASS on sec\_policy1\_HQtoFLEX'. An 'OK' button is at the bottom right of the dialog.

## How to Configure Route-Based VPN

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



## Set up IPsec VPN Tunnel for HQ

### VPN > Site to Site VPN > Scenario

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

The screenshot displays the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The 'VPN' section is expanded, and 'Site to Site VPN' is selected. The main area shows a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are: \*Name: HQtoBranch; IKE Version: IKEv2 (selected); Type: Site-to-Site (selected); Behind NAT: None (selected). Below the fields is a diagram showing a 'Local Site' and a 'Remote Site' connected via an 'Internet' cloud. 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	<input type="text" value="100.100.100.254"/>
Peer Gateway Address	Domain Name / IP	<input type="text" value="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**

The screenshot shows the ZyXel configuration interface for Site to Site VPN Authentication. At the top, a breadcrumb trail reads 'VPN > Site to Site VPN'. Below this is a progress indicator with five steps: 'Scenario' (checked), 'Network' (checked), 'Authentication' (active, highlighted with a green circle and number 3), 'Policy & Routing' (number 4), and 'Summary' (number 5). The main content area is titled 'Authentication' and contains two radio button options: 'Pre-Shared Key' (selected) and 'Certificate'. To the right of the 'Pre-Shared Key' option is a text input field containing seven asterisks, highlighted with a red border. Below the input field is a dropdown menu currently set to 'default'. At the bottom of the interface, there are three buttons: 'Cancel' on the left, 'Back' in the center, and 'Next' on the right.

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

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

The screenshot displays the ZyXel VPN configuration interface for a Site to Site VPN. At the top, a progress bar shows five steps: Scenario, Network, Authentication, Policy & Routing (current step, highlighted with a green circle and the number 4), and Summary (highlighted with a grey circle and the number 5). Below the progress bar, the 'Type' section has two radio buttons: 'Route-Based' (selected and highlighted with a red box) and 'Policy-Based'. The 'Remote Subnet' field is a text input box containing '192.168.160.0/24', also highlighted with a red box. Below these settings is a network diagram showing a central green cloud labeled 'Internet'. To the left of the Internet cloud is a 'Local Site' represented by a server rack icon, with the IP range '100.100.100.254' below it. To the right of the Internet cloud is a 'Remote Site' represented by a server rack icon, with the IP range '100.100.200.254' below it. On the far left, there is an 'Any' icon representing a client device. On the far right, there is another 'Any' icon representing a client device. At the bottom of the interface, there are three buttons: 'Cancel' on the left, 'Back' in the middle, and 'Finish' on the right.

**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 navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area is titled 'VPN > Site to Site VPN' and has a progress bar with five steps: 1 Scenario (active), 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step contains the following configuration options: \*Name: BranchtoHQ; IKE Version: IKEv2 (selected); Type: Site-to-Site (selected); Behind NAT: None (selected); Local Site (radio button); Remote Site (radio button). Below the text is a diagram showing a 'Local Site' and a 'Remote Site' connected via an 'Internet' cloud. At the bottom 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

Peer Gateway Address Domain Name / IP



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

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 ZyXel VPN Status page. The breadcrumb navigation is: VPN Status > IPsec VPN > Site to Site VPN. There are two tabs: 'Site to Site VPN' (selected) and 'Remote Access VPN'. Below the tabs are buttons for 'Disconnect', 'Refresh', and 'Connectivity Check'. A search bar for insights is also present. The main content is a table with columns: #, Name, Policy Route, Remote Gateway, My Address, Uptime, Rekey, Inbound (Bytes), and Outbound (Bytes). A single entry is shown under a 'Custom' dropdown.

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

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

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

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

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

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

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

C:\WINDOWS\system32>
  
```

## How to Use Tailscale

### What's Tailscale?

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

### Start to Tailscale and implement on Firewall

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

The screenshot shows the Tailnet Settings interface for a user with a trial period. The top navigation bar includes 'zyxel.com.tw', 'Trial 14 days left', 'Download', 'Support', 'Docs', and a user profile icon 'K'. The main navigation menu includes 'Machines', 'Apps', 'Services', 'Users', 'Access controls', 'Logs', 'DNS', 'Settings', and 'Get started'. The left sidebar lists settings categories: Tailnet Settings, General, User management, Device management, OAuth clients, Webhooks, Contact preferences, and Billing. The 'Personal Settings' and 'Keys' items are highlighted with red boxes. The main content area is titled 'Keys' and contains the following 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](#)' and a 'Generate auth key...' button. A message box states 'You don't have any valid auth keys' and a link shows '> 1 recently invalidated auth key'.

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

### Generate auth key ✕

**Description**  
Add an optional description for the key.

**Reusable**

Use this key to authenticate more than one device.

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

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 ↗](#)

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".

The screenshot shows the ZyXel Firewall configuration interface for Tailscale. The left sidebar has 'VPN' selected, and 'Tailscale' is highlighted. The main panel shows 'General Settings' for Tailscale. The 'Enable' toggle is turned on. The 'Auth Keys' field contains a masked key and has a 'Logout' button next to it. The 'Server Port' is set to 41641. The 'Zone' dropdown is set to 'Tailscale'. The 'Routing' section has 'As an Exit Node' turned on.



- 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.

5. Go back to the Tailscaler admin page. You will see the Firewall device.

The screenshot shows the Tailscaler admin interface for 'zyxel.com.tw'. The 'Machines' section is active, displaying a table of connected devices. The 'usgflex500h' machine is highlighted with a red box.

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

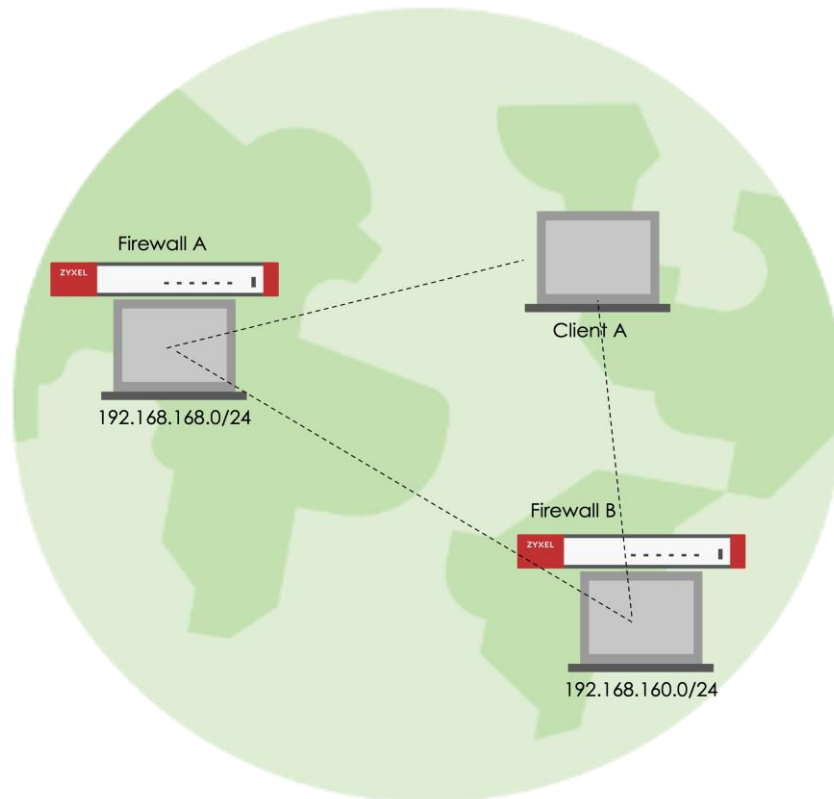
Click "Disable key expiry" for all client to prevent lost connection while expire.

The screenshot shows a detailed view of the 'usgflex500h' machine. A dropdown menu is open, and the 'Disable key expiry' option is highlighted with a red box.

<b>usgflex500h</b> Kevin.Wu4@zyxel.com.tw <a href="#">Subnets</a> <a href="#">Exit Node</a>	100.115.120.97	1.75.16 Linux 4.14.207-10.3.7.0-2	Connected	Share... ⋮
<b>client-a</b> Kevin.Wu4@zyxel.com.tw	100.95.1.123	1.80.2 Windows 11 22H2	Mar 5, 4:50 PM GMT+8	
<b>iphone-15</b> 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.

The screenshot shows the configuration page for Firewall A. The breadcrumb navigation is VPN > Tailscale. Under 'General Settings', the 'Enable' toggle is turned on. The 'Auth Keys' field is masked with dots and has a 'Logout' button. The 'Server Port' is 41641 (1-65535) and the 'Zone' is 'Tailscale'. Under 'Routing', 'As an Exit Node' is turned off. The 'Advertised Networks' section has a table with one entry: N\_192\_168\_168.

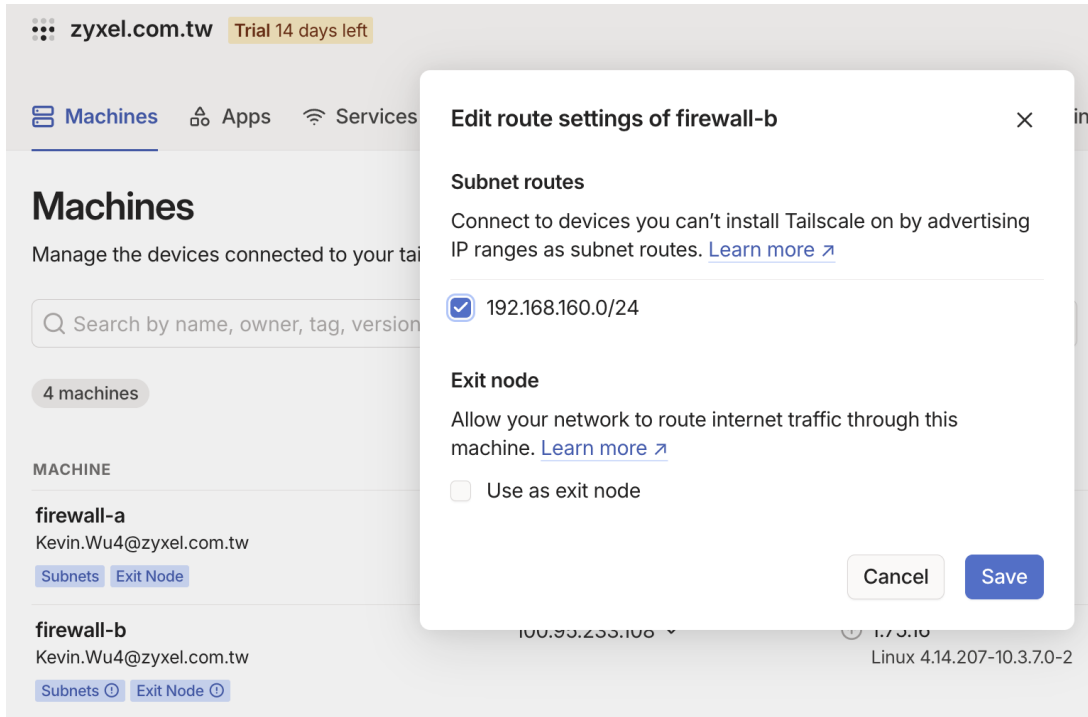
Network
N_192_168_168

2. Advertised 192.168.160.0/24 in Firewall B.

The screenshot shows the configuration page for Firewall B. The breadcrumb navigation is VPN > Tailscale. Under 'General Settings', the 'Enable' toggle is turned on. The 'Auth Keys' field is masked with dots and has a 'Logout' button. The 'Server Port' is 41641 (1-65535) and the 'Zone' is 'Tailscale'. Under 'Routing', 'As an Exit Node' is turned off. The 'Advertised Networks' section has a table with one entry: N\_192\_168\_160.

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

Server Port  (1-65535)

Zone

### Routing

As an Exit Node

### Advised Networks

+ Add Remove

Network
<input type="checkbox"/> 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

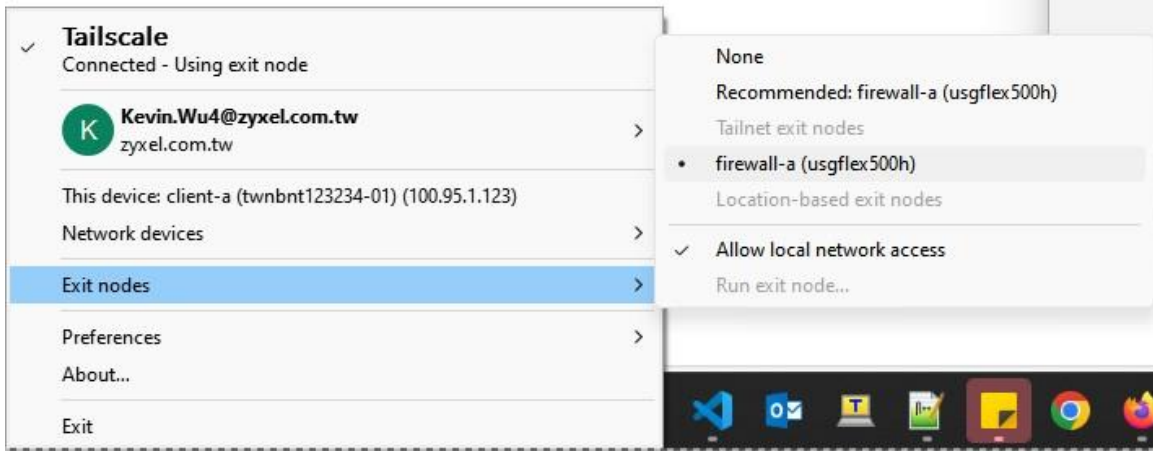
Allow your network to route internet traffic through this machine. [Learn more ↗](#)

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 0xfffff00 broadcast 192.168.168.255
  nd6 options=201<PERFORMNUD,DAD>
  media: autoselect (1000baseT <full-duplex>)
  status: active
[kevin@wujiayuandeMacBook-Air 0219 % ping 192.168.160.33
PING 192.168.160.33 (192.168.160.33): 56 data bytes
64 bytes from 192.168.160.33: icmp_seq=0 ttl=126 time=3.301 ms
64 bytes from 192.168.160.33: icmp_seq=1 ttl=126 time=3.267 ms
--
```

The ping test from Firewall B

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

Wireless LAN adapter Wi-Fi:

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

Ethernet adapter 藍牙網路連線:

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

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

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

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

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

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

### Before Begin

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

### User & Authentication > User/Group > User

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

The screenshot shows the configuration page for a new user in the VPN system. The breadcrumb navigation at the top reads "User & Authentication > User/Group > User". The page is titled "Profile Management".

The configuration fields are as follows:

- User Name:** VPN
- User Type:** ext-group-user
- Authentication Server:** AD / AD (dropdown menu)
- Group Identifier:** cn=vpngroup,ou=Group,dc=cso,dc=com (dropdown menu, highlighted with a red box)
- Description:** (empty text field)
- Authentication Timeout Settings:**  Use Default Settings,  Use Manual Settings
- Lease Time:** 1440 minutes
- Reauthentication Time:** 1440 minutes

Below the configuration fields is a "Configuration Validation" section with the instruction: "Please enter an existing user account in this server to validate the above settings." It contains a "User Name" text input field and a green "Test" button.

**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

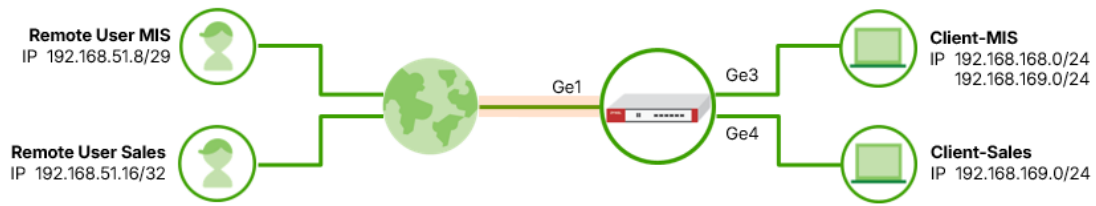
Remote Access VPN


Disconnect Refresh Search insights

#	Username	Assigned IP	Remote IP	Up Time	Reauth/Lease Time	Inbound (Bytes)	Outbound (Bytes)
1	vpn1est	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

- 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)

Auto SNAT  i

Local Networks Only (Split Tunnel)

**Local Networks**

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

+ Add Remove

Network
<input type="checkbox"/> 192.168.169.0/24
<input type="checkbox"/> 192.168.168.0/24

**Client Network**

IP Address Pool  i

DNS Server

DNS Domain Suffix

**Members**

User  i

- 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)

Auto SNAT  i

Local Networks Only (Split Tunnel)

**Local Networks**

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

+ Add - Remove

<input type="checkbox"/> Network ↕
<input type="checkbox"/> 192.168.169.0/24

---

**Client Network**

IP Address Pool  i

DNS Server

DNS Domain Suffix

**Members**

User  ✎ i

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

The screenshot shows the ZyXel VPN configuration interface. The 'Client Network' section has the 'IP Address Pool' set to 192.168.51.0/24, 'DNS Server' set to ZyWALL, and 'DNS Domain Suffix' is empty. The 'Advanced Settings' section shows a table of 'Client Profile' entries. Two entries are listed, both with 'IP Address Pool' values highlighted in red: 192.168.51.16/32 and 192.168.51.8/29. Both profiles use 'ZyWALL' as the DNS Server and 'Split Tunnel' as the Tunnel Type.

#	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 shows the OpenVPN Connect application window on the left and a Windows Command Prompt window on the right. The OpenVPN Connect window displays the 'Profiles' section with a status bar showing 'BYTES IN 332 B/S' and 'BYTES OUT 840 B/S'. 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 address '10.214.48.38' and 'PORT 10443'. The 'VPN PROTOCOL' is listed as 'TCP'. The Command Prompt window shows the execution of two ping commands: 'ping 192.168.169.1' and 'ping 192.168.168.1'. Both commands show successful results with 4 packets sent and received, 0% loss, and round trip times ranging from 1ms to 2ms.

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 shows the OpenVPN Connect application window on the left and a Windows Command Prompt on the right. The OpenVPN Connect window displays the 'Profiles' section with a status bar showing 0B/s. Below the status bar, it shows 'BYTES IN 3.96 KB/S' and 'BYTES OUT 632 B/S'. The 'DURATION' is 00:01:42 and 'PACKET RECEIVED' is 4 sec ago. Under the 'YOU' section, the username 'sales1' and 'YOUR PRIVATE IP 192.168.51.16' are highlighted with red boxes. The 'SERVER' section shows '10.214.48.38' and 'SERVER PUBLIC IP 10.214.48.38'. The 'PORT' is 10443 and 'VPN PROTOCOL' is TCP.

The Command Prompt 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),
```

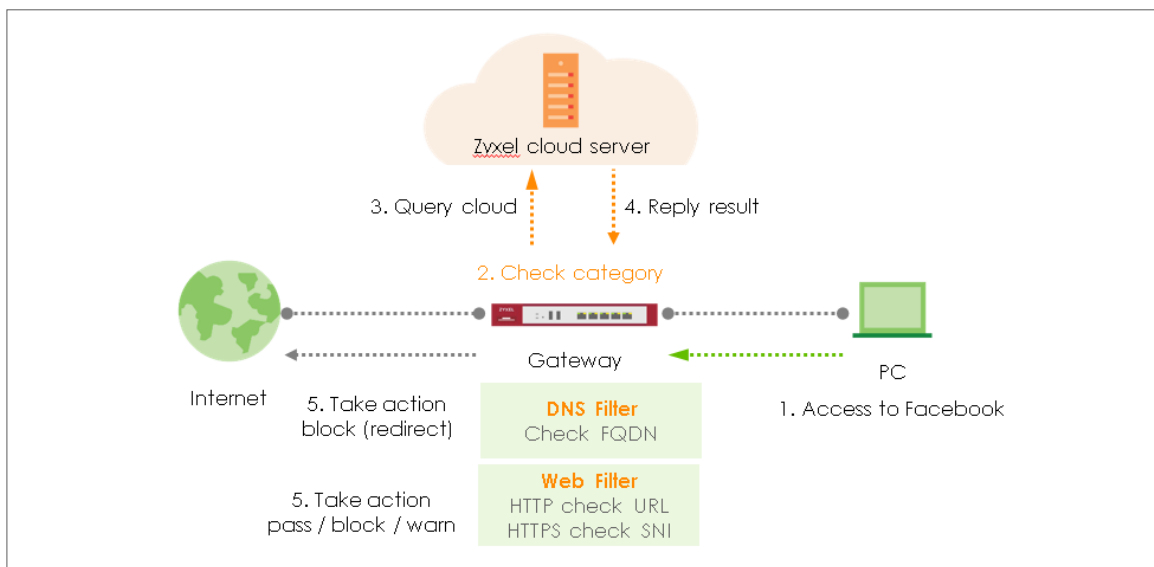
Verify the SSL VPN status in Log & Report > System.

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[redacted]) 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

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

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

General Settings

Name:

Description:

Action:

Log:

Log allowed traffic:

SSL V3 or previous version Connection Drop:

Drop Log:

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

Managed Categories

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

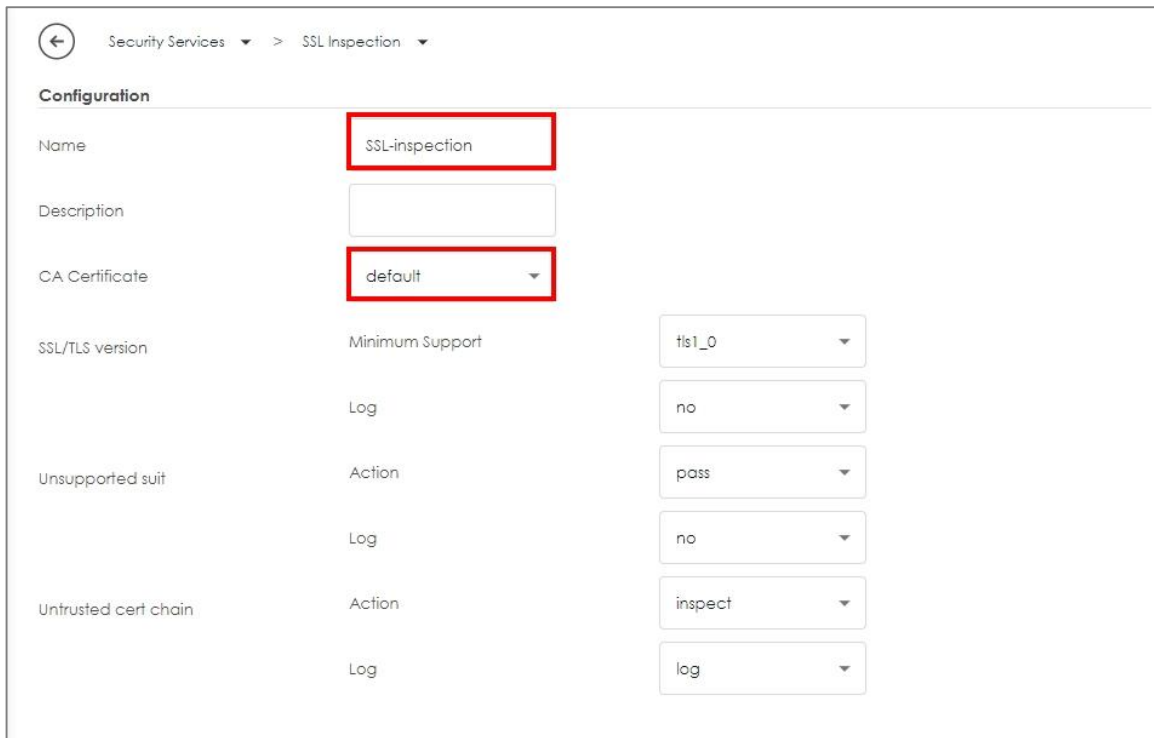
Some changes were made  
What do you want to do then?

## Set Up SSL Inspection

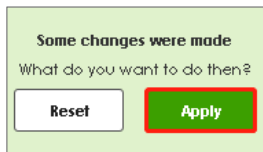
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



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



Click Apply to add SSL Inspection profile.



## 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

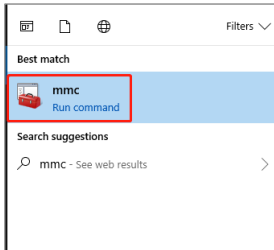
## Export Certificate from FLEX and Import it to Windows

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.

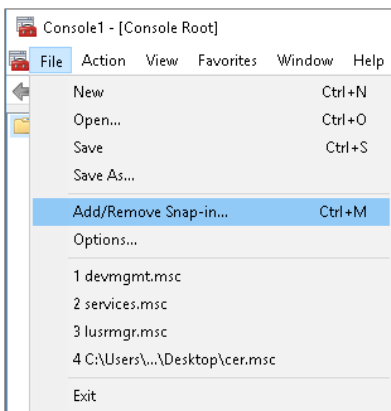
Go to System > Certificate > My Certificates to export default certificate from FLEX.

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

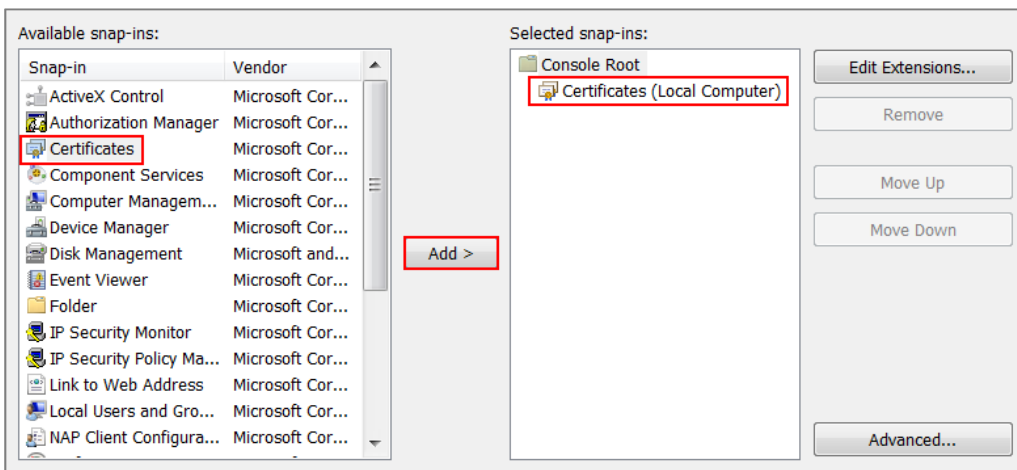
In Windows Start Menu > Search Box, type MMC and press Enter.



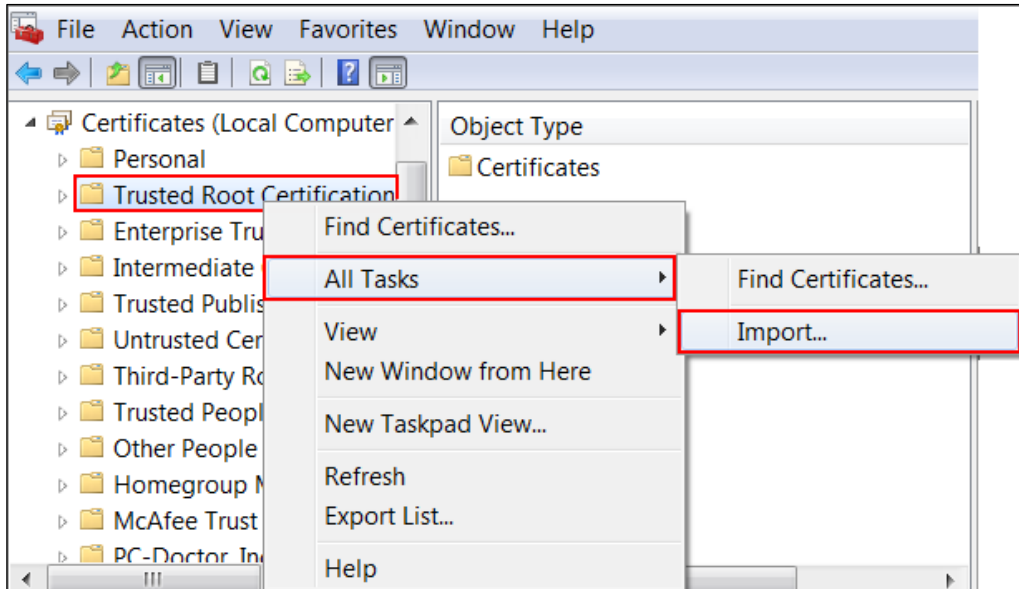
In the mmc console window, click File > Add/Remove Snap-in...



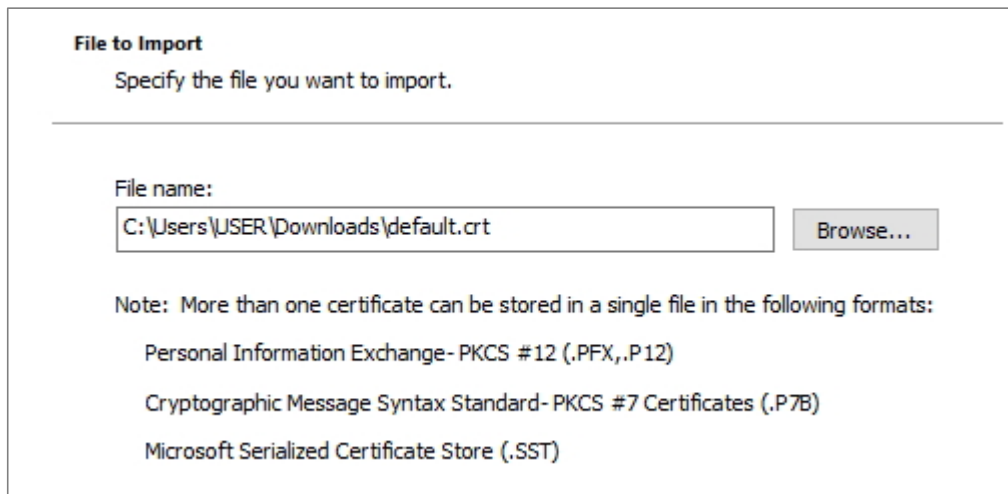
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



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.



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



← 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

## Test the Result

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


**Content Filtering**

### Access Restricted

**Web access is restricted. Please contact the administrator.**

Category      Block Web Sites

Blocked URL    https://www.youtube.com/bw/



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

#	Time	Category	Message	Source	Destination	Note
71	2023-05-29 19:11:15	content-filter	www.youtube.com:Streaming Media, Rule_name:LAN_Outgoing, SSIN (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
103	2023-05-29 19:11:02	content-filter	youtube-ui.l.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, SSIN (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
258	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS REDIRECT
259	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK
260	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK

Rows per page: 50    1-6 of 6

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

Security Statistics > SSL Inspection > Summary

**Summary** Certificate Cache List

**General Settings**

Refresh Flush Data

**Status**

Maximum Concurrent Sessions **1000**

Concurrent Sessions **238**

**Summary**

SSL Sessions	Total	
	Inspected	<b>3430 (96.54%)</b>
	Decrypted	<b>48.24 Mbytes</b>
	Encrypted	<b>48.05 Mbytes</b>
	Blocked	<b>0</b>
	Passed	<b>123</b>

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	Hit Count
Streaming Media	<b>18 (100%)</b>

**Content Filter Events**

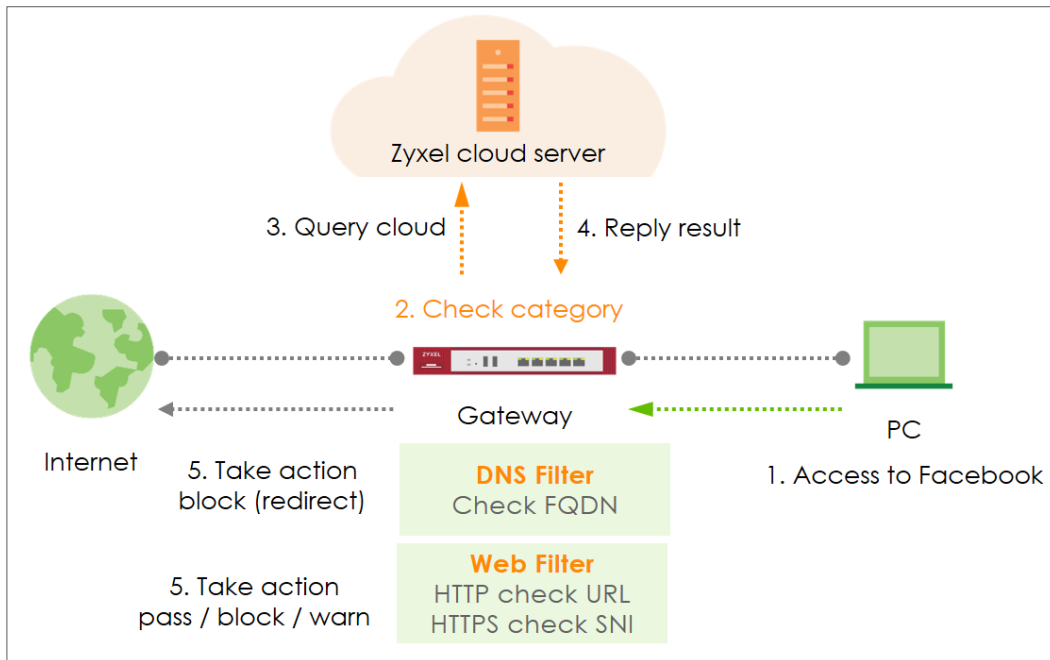
Search insights


Time	Action	URI/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.

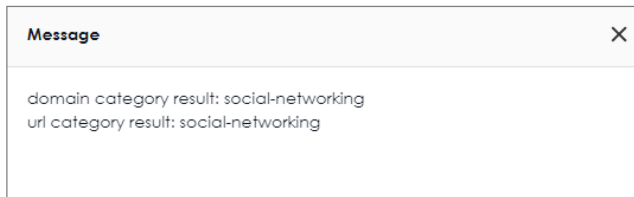
The screenshot shows the configuration page for a Content Filter profile. The breadcrumb navigation is "Security Service > Content Filtering". The "General Settings" section includes the following fields:

- Name:** Social\_Networking
- Description:** (empty text box)
- Action:** block (highlighted with a red box)
- Log:** log alert
- Log allowed traffic:** (checked toggle switch)
- SSL V3 or previous version Connection:** Drop (with a checked toggle switch)
- Drop Log:** log alert

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

The screenshot shows the "Test Web Site Category" page. It features a text input field labeled "URL to test" containing the URL "https://www.facebook.com" (highlighted with a red box). To the right of the input field is a red button labeled "Query" (also highlighted with a red box). Below the input field, there is a green link that reads: "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 shows the configuration page for a Security Policy in the Policy Control section. The page is titled "Security Policy" and "Policy Control". Under the "Configuration" section, there are several fields:

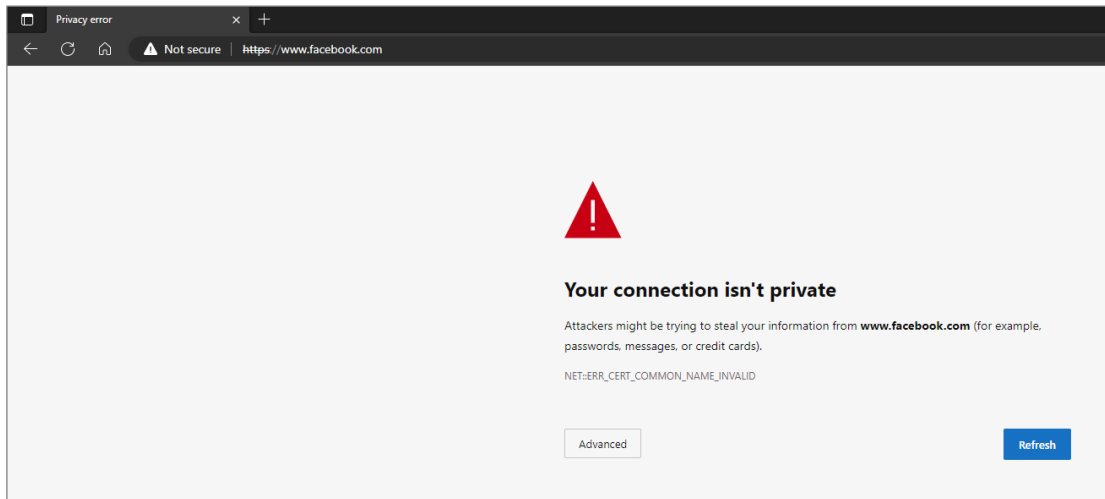
- Enable:** A toggle switch is turned on.
- Name:** A text input field containing "Block\_Social\_Networkir".
- Description:** An empty text input field.
- From:** A dropdown menu with "LAN" selected.
- To:** A dropdown menu with "WAN" selected.
- Source:** A dropdown menu with "any" selected.
- Destination:** A dropdown menu with "any" selected.
- Service:** A dropdown menu with "any" selected.
- User:** A dropdown menu with "any" selected.
- Schedule:** A dropdown menu with "none" selected.
- Action:** A dropdown menu with "allow" selected.
- Log:** A dropdown menu with "no" selected.

Under the "Profile" section, there are three rows:

- Application Patrol:** A dropdown menu with "none" selected, a "Log" checkbox, and a dropdown menu with "by profile" selected.
- Content Filter:** A dropdown menu with "Social\_Networking" selected, a "Log" checkbox, and a dropdown menu with "by profile" selected.
- SSL Inspection:** A dropdown menu with "none" selected, a "Log" checkbox, and a dropdown menu with "by profile" selected.

## Test Result

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

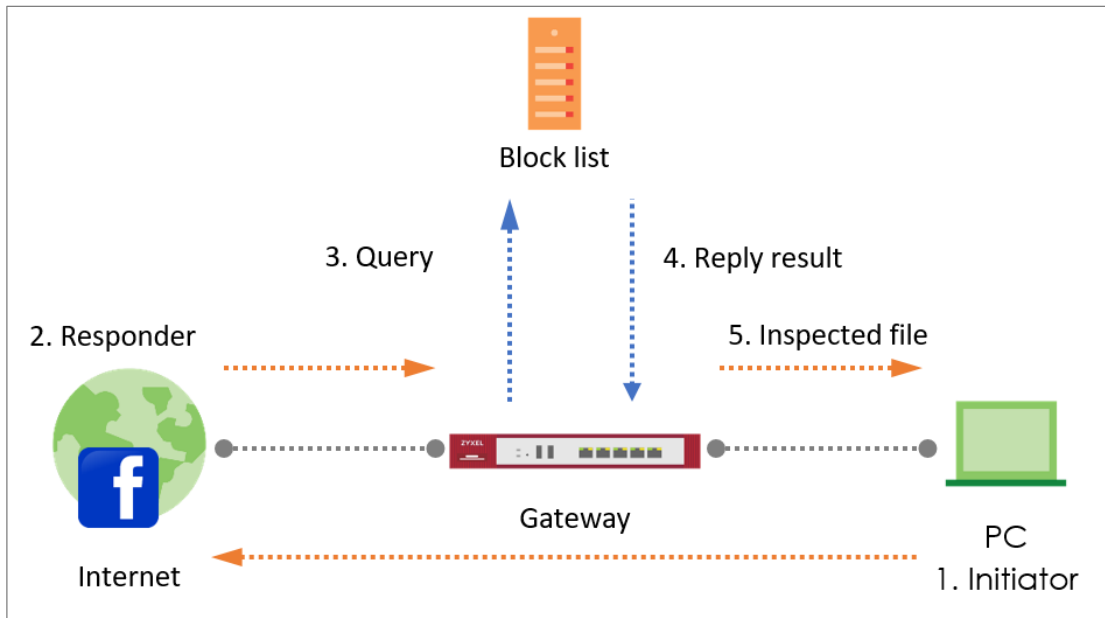



Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

Log ID	Time	Filter	Destination	Source	Port	Action
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 0
*.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.

The screenshot displays the configuration page for a Security Policy in the Policy Control section. The page is divided into two main sections: Configuration and Profile.

**Configuration Section:**

- Enable:** A green toggle switch is turned on.
- Name:** A text input field contains "Facebook\_Block".
- Description:** An empty text input field.
- From:** A dropdown menu is set to "LAN".
- To:** A dropdown menu is set to "any (Excluding ZyWALL)".
- Source:** A dropdown menu is set to "any".
- Destination:** A dropdown menu is set to "any".
- Service:** A dropdown menu is set to "any".
- User:** A dropdown menu is set to "any".
- Schedule:** A dropdown menu is set to "none".
- Action:** A dropdown menu is set to "allow".
- Log:** A dropdown menu is set to "no".

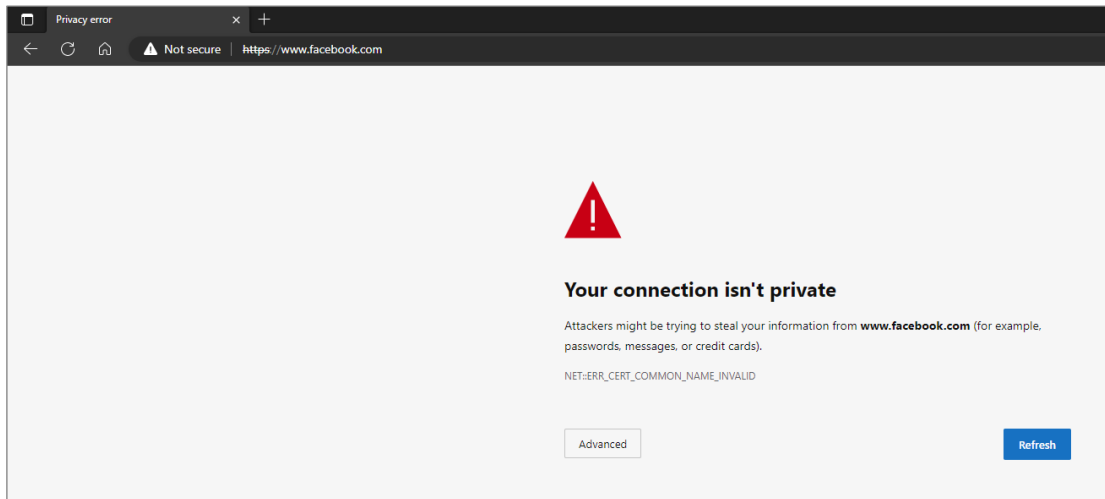
**Profile Section:**

- Application Patrol:** A dropdown menu is set to "none".
- Content Filter:** A dropdown menu is set to "Facebook\_Block".
- SSL Inspection:** A dropdown menu is set to "none".

Each dropdown menu in the Configuration section has a green pencil icon to its right, indicating it can be edited. The "Log" column in the Profile section has a "Log" label next to each dropdown.

## Test the Result

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

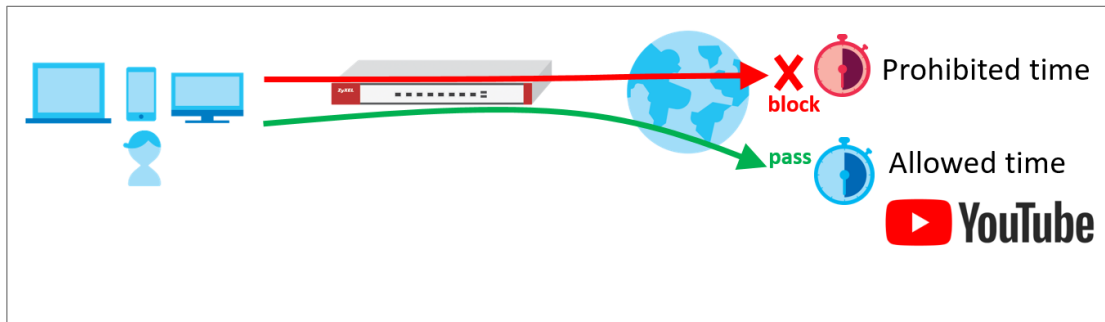



Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

#	Time	Category	Message	Source	Destination	Note
1	2023-05-22 15:36:59	content-filter	www.facebook.com:Block List, Rule_name:Facebook_Block_S333N (Content Filter)	192.168.168.33	52.23.24.85	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**.

The screenshot shows the 'Add Application' dialog box with the following configuration:

- Category and Application:** Search term: youtube
- Search Results:**
  - Audio/Video (1/205) - [checked]
  - YouTube TV - [checked]
  - Web (6/2568) - [checked]
  - YouTube.com - [checked]
  - youtube Audio/Video - [checked]
  - youtube Upload - [checked]
  - YouTube HD - [checked]
  - YouTube Kids - [checked]
  - YouTube Music - [checked]
- Log:** Log Alert
- Action:** Reject
- Buttons:** Cancel, Add

## Set Up the Security Policy

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

 Object ▾ > Service ▾

---

**Configuration**

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

Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **service** QUIC\_UDP443 and select the **Schedule** that defines when the policy would be applied.

In this example, select "Youtube\_Blocked\_Time".

← Security Policy > Policy Control

**Configuration**

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

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

←
Security Policy ▾ > Policy Control ▾

### Configuration

---

Enable

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

---

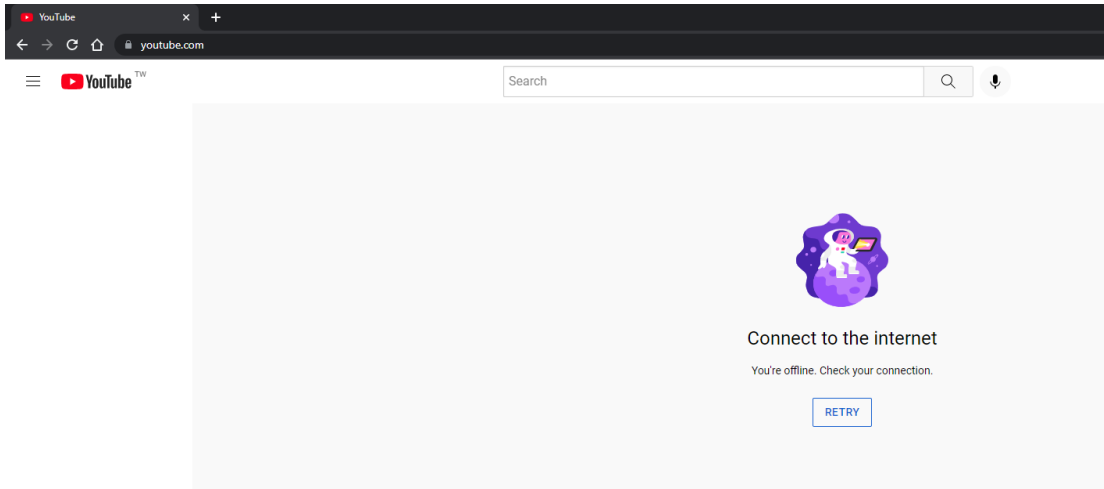
Application Patrol	<span style="border: 1px solid red; padding: 2px;">Youtube</span> ▾	Log	<span style="border: 1px solid #ccc; padding: 2px;">by profile</span> ▾
Content Filter	<span style="border: 1px solid #ccc; padding: 2px;">none</span> ▾	Log	<span style="border: 1px solid #ccc; padding: 2px;">by profile</span> ▾
SSL Inspection	<span style="border: 1px solid #ccc; padding: 2px;">none</span> ▾	Log	<span style="border: 1px solid #ccc; padding: 2px;">by profile</span> ▾

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

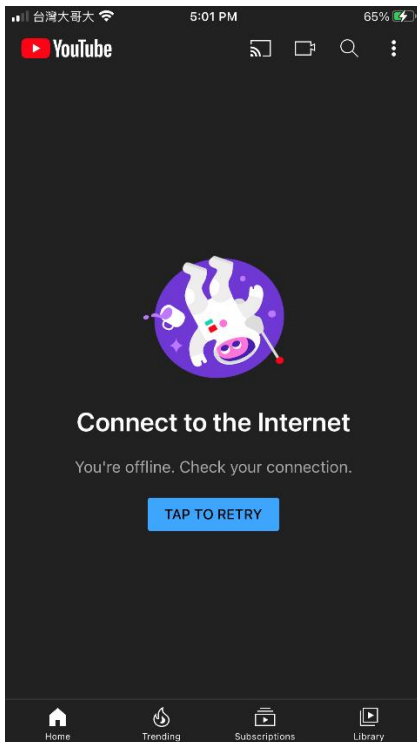
<input type="checkbox"/>	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
<input type="checkbox"/>	🟢	1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
<input type="checkbox"/>	🟢	2	Block_Youtube	LAN	WAN	LAN1_SUBNET	any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

## Test the Result

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



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




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

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

## How to Control Access to Google Drive

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



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

## Create app patrol profile

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

**App Patrol**

**General Settings**

Collect Statistics: Enable

Analyze All Traffic:  ⓘ

**Profile Management**

+ Add Edit Remove Reference

<input type="checkbox"/>	Name	Description	Reference
<input type="checkbox"/>	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

<input type="checkbox"/>	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** [X]

Category and Application

Google document [X]

- 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 [Q] [Menu]

<input type="checkbox"/>	Name ⇅	Description ⇅	CA Certificate ⇅	Reference ⇅
--------------------------	--------	---------------	------------------	-------------

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

← Security Services > > SSL Inspection

**Configuration**

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

### Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN\_Outgoing, and scroll down to profile section.

Select Application Patrol, and SSL Inspection.

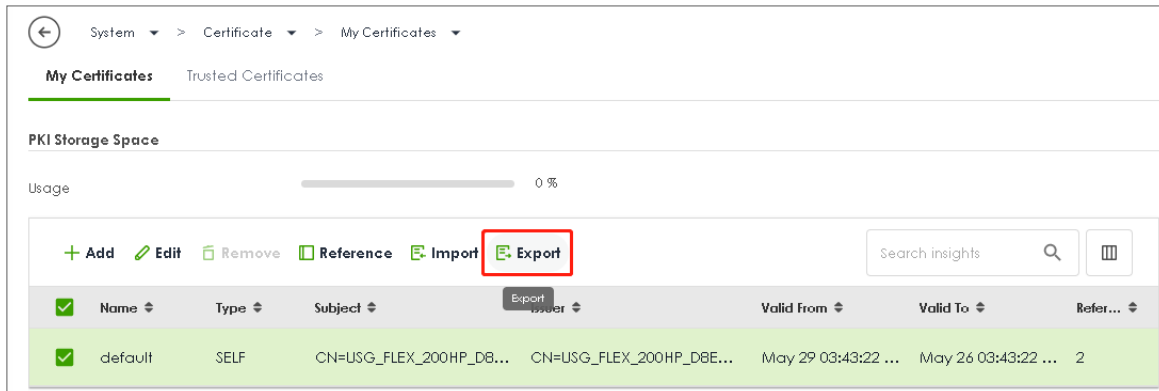
**Profile**

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

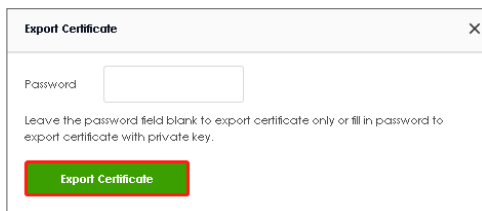
## Export Certificate from FLEX and import to Lan hosts

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

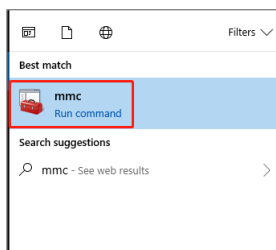
Go to System > Certificate > My Certificates to export default certificate from FLEX.



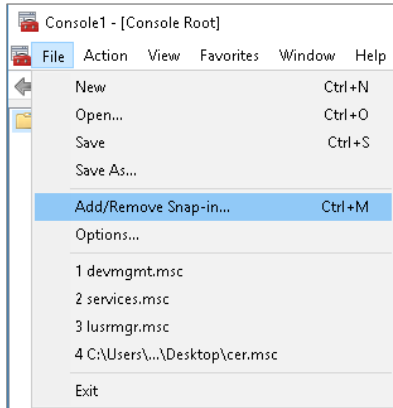
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



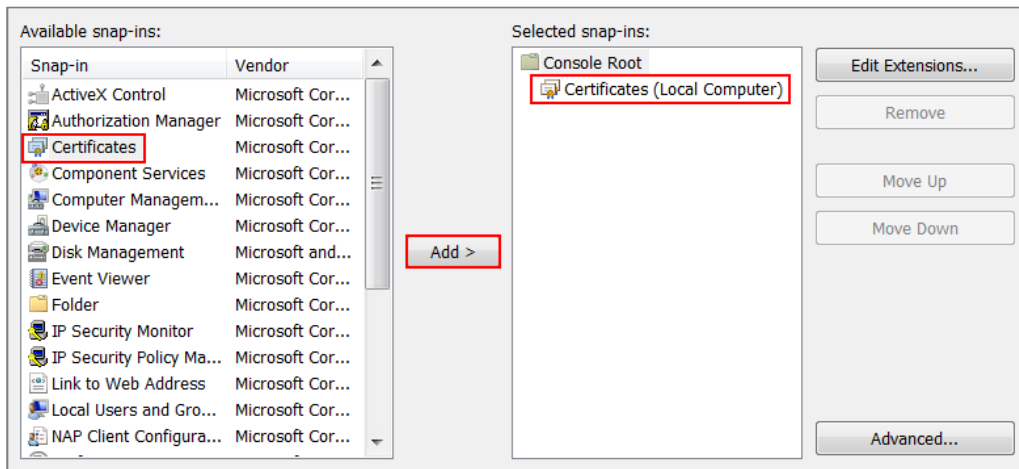
In Windows Start Menu > Search Box, type MMC and press Enter.



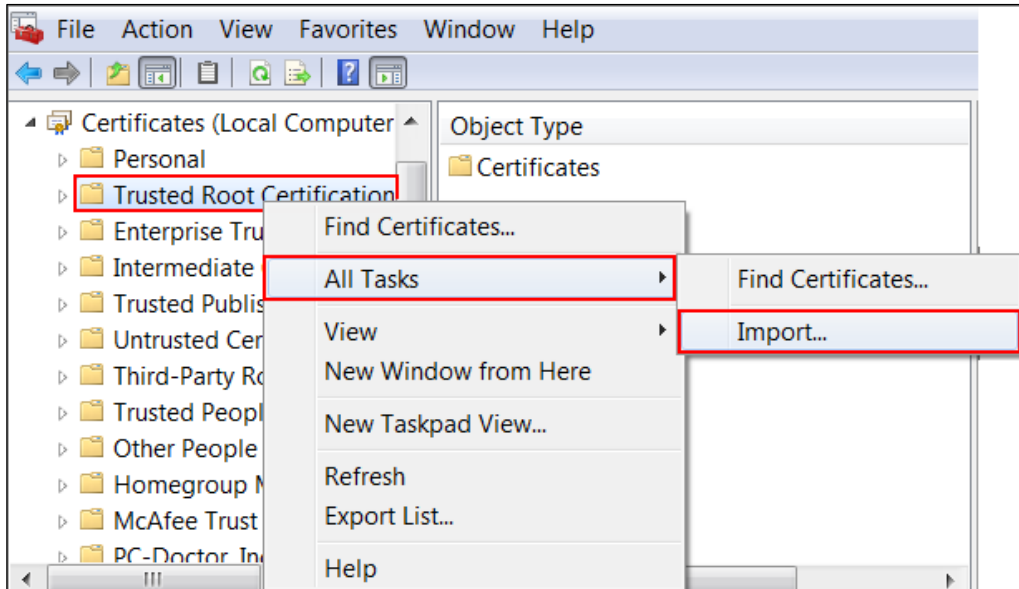
In the mmc console window, click File > Add/Remove Snap-in...



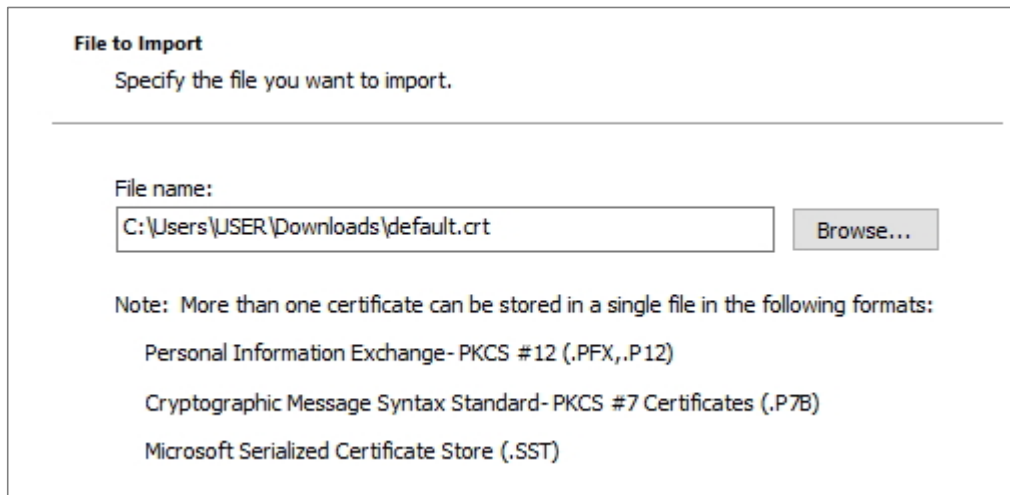
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



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



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



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



## Test the Result

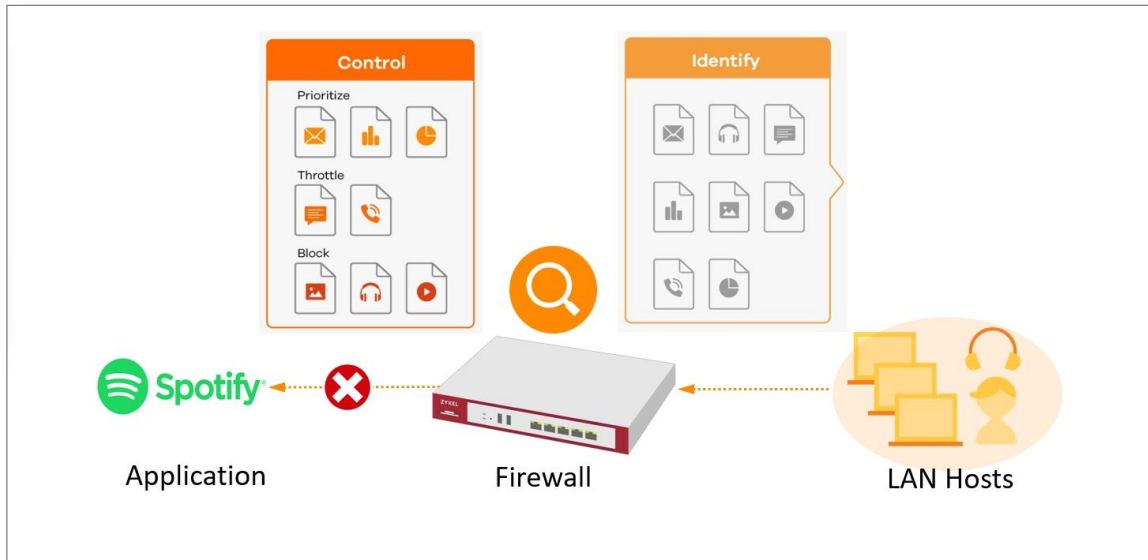
Access to Google drive from Lan host to verify if it is blocked by firewall Application patrol.


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

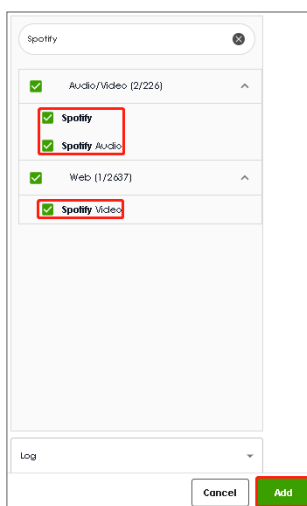
Go to Security Service > App patrol > Profile management, and click Add to create profile.



Click add to add application in this profile.



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

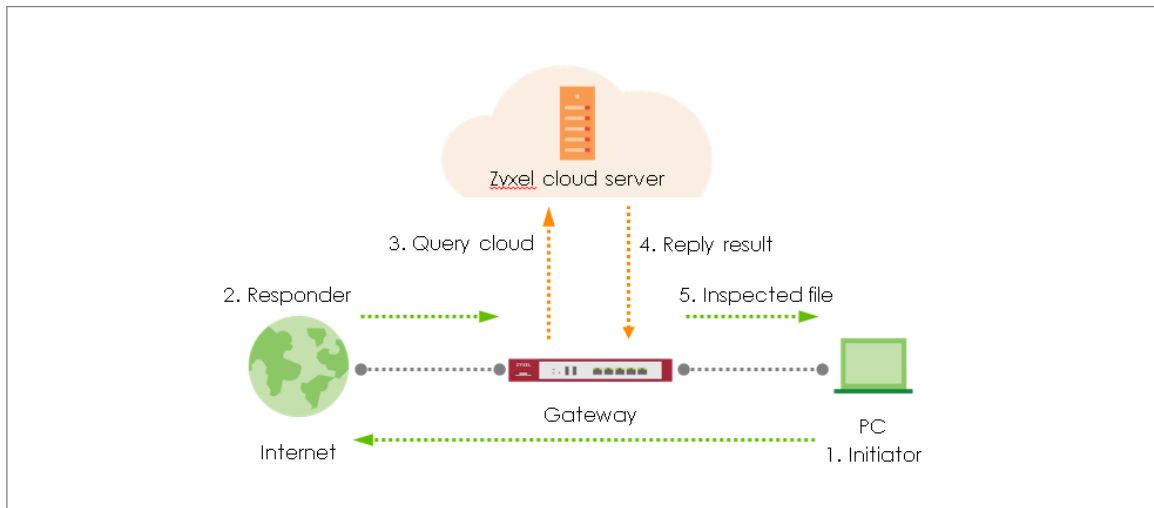
Access to Spotify from Lan host to verify if it is blocked by firewall Application patrol.

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

#	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.



The screenshot shows the 'Anti-Malware' configuration page. The breadcrumb trail is 'Security Service > Anti-Malware > Anti-Malware'. The page title is 'Anti-Malware'. Under the 'General Settings' section, there are four items: 'Enable Anti-Malware', 'Collect Statistics', 'Scan and detect EICAR test virus', and 'File size limit'. The first three items have green toggle switches that are turned on. The 'File size limit' is set to '10 (MB)'. A red box highlights the three toggle switches.

Select Destroy infected file and log in Actions When Matched



The screenshot shows the 'Actions When Matched' configuration page. There are two items: 'Destroy infected file' and 'Log'. The 'Destroy infected file' has a green toggle switch that is turned on. The 'Log' has a dropdown menu with 'log' selected. A red box highlights the toggle switch and the dropdown menu.

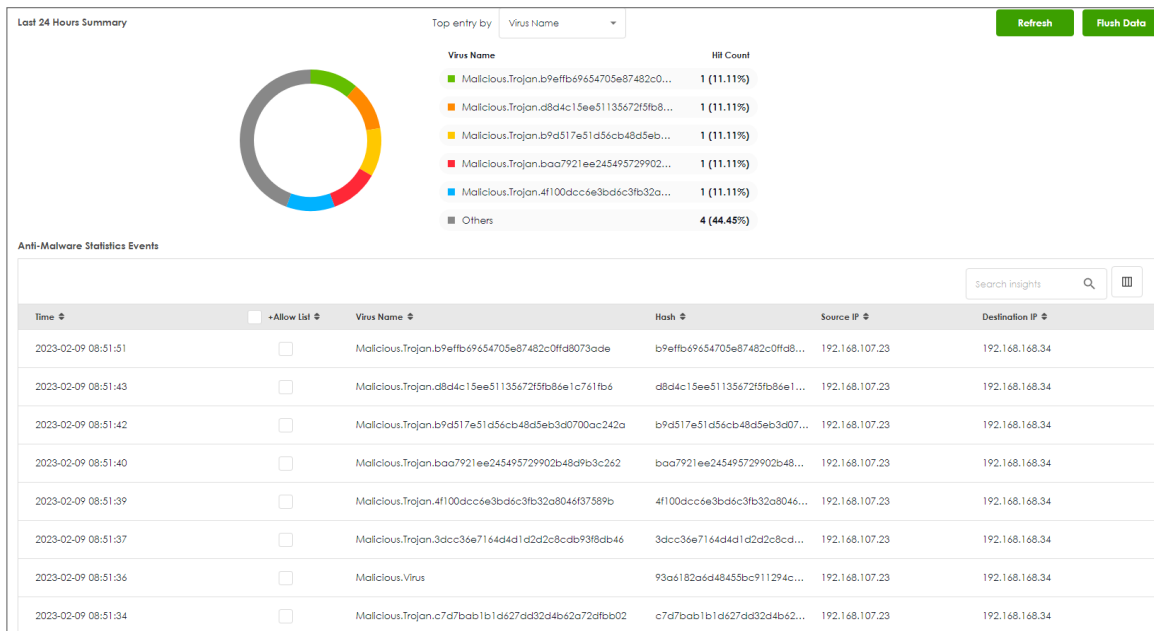
## Test the Result

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.

#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus Infected SSIN Type:Cloud Query Virus:Malicious.Trojan.44d88612fea8a8f36de82e1278abb02f File:eicar.com.txt Protocol:HTTP md5:44d88612fea8a8f36de82e1278abb02f	89.238.73.97	192.168.168.36	FILE DESTROY

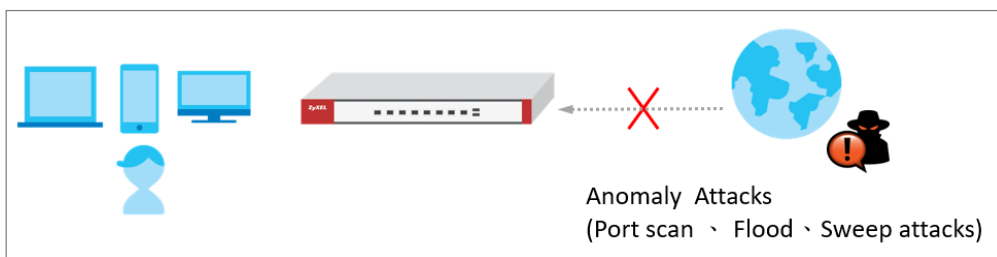
Go to Security Statistics > Anti-Malware to check summary of all events.




## How to Detect and Prevent TCP Port Scanning with DoS

### Prevention

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



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

## Set Up the DoS Prevention

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

Security Policy > Dos Prevention

**General Settings**

Name: DoS\_Prevention

Description:

**Scan Detection**

Sensitivity: Medium

Block Period: 5 (1-3600 seconds)

Active Inactive Log Action

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

**Flood Detection**

Block Period: 5 (1-3600 seconds)

Edit Active Inactive Log Action

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

The screenshot shows the configuration page for a DoS Prevention Policy. The breadcrumb navigation is Security Policy > DoS Prevention > DoS Prevention Policy. The page title is DoS Prevention Policy Profile. Under General Settings, the 'Enable DoS Prevention' toggle is turned on. Under Policies, there is a table with one entry:

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

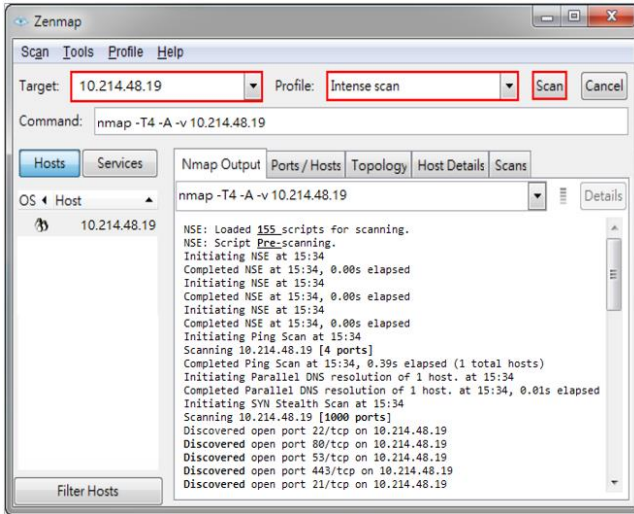
|

## 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.



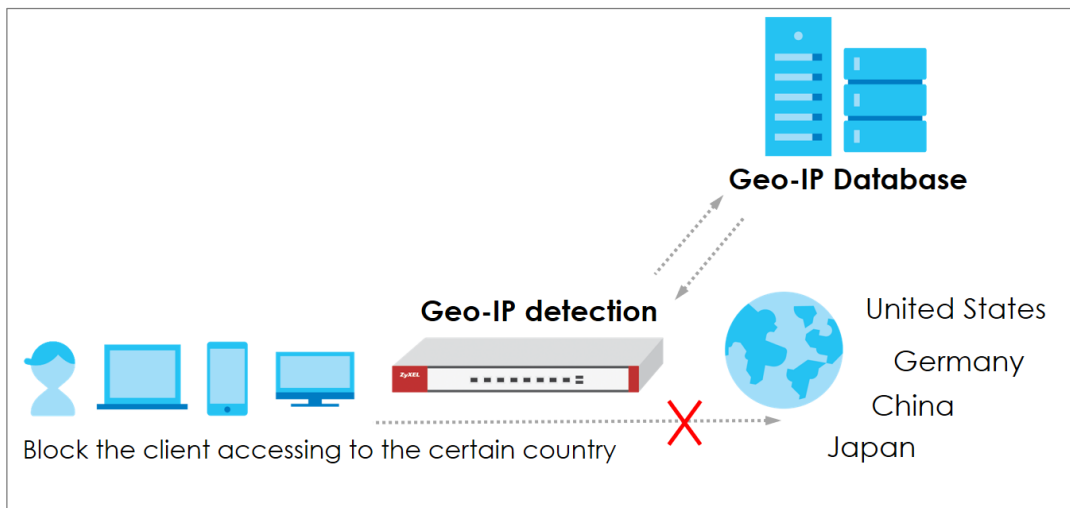
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.


#	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.**

The screenshot shows the configuration page for a Geo IP object. The breadcrumb navigation is "Object > Address". The "Configuration" section contains the following fields:

- Name: geo\_ip
- Description: (empty)
- Address Type: GEOGRAPHY (highlighted with a red box)
- Region: China (highlighted with a red box)

The screenshot shows the configuration page for a second Geo IP object. The breadcrumb navigation is "Object > Address". The "Configuration" section contains the following fields:

- Name: geo\_ip\_2
- Description: (empty)
- Address Type: GEOGRAPHY (highlighted with a red box)
- Region: Germany (highlighted with a red box)

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

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	10.0.0/8	0
RFC1918_2	CIDR	172.16.0.0/12	0
RFC1918_3	CIDR	192.168.0.0/16	0
geo_ip	GEOGRAPHY	China	1
geo_ip_2	GEOGRAPHY	Germany	1

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

Group Members

Name:

Description:

Member List

=== Object ===

- IP6to4-Relay
- LAN1\_SUBNET
- LAN2\_SUBNET
- RFC1918\_1
- RFC1918\_2
- RFC1918\_3
- geo\_ip
- geo\_ip\_2

=== Group ===

=== Object ===

=== Group ===

## Set Up the Security Policy

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

Security Policy > Policy Control

**Configuration**

Enable

Name geo\_block\_policy

Description

From LAN

To WAN

Source any

Destination geo\_block

Service any

User any

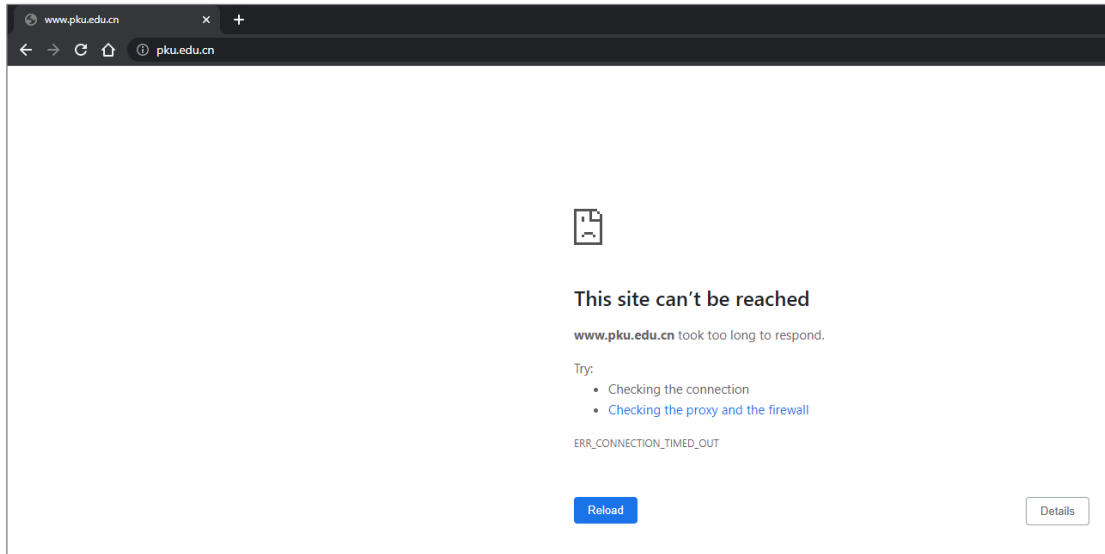
Schedule none

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.

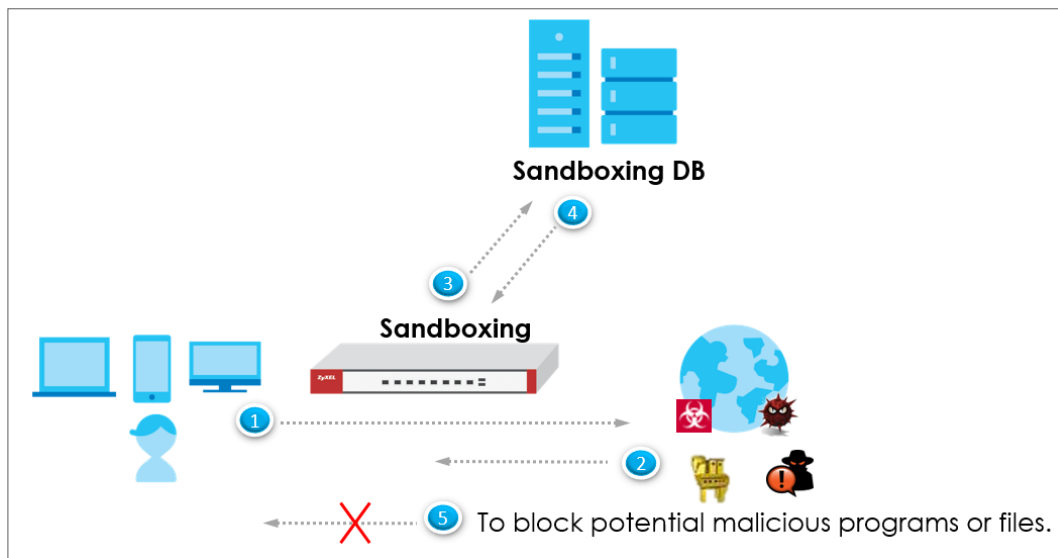



To view the log message, go to **USG Flex H Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

#	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?

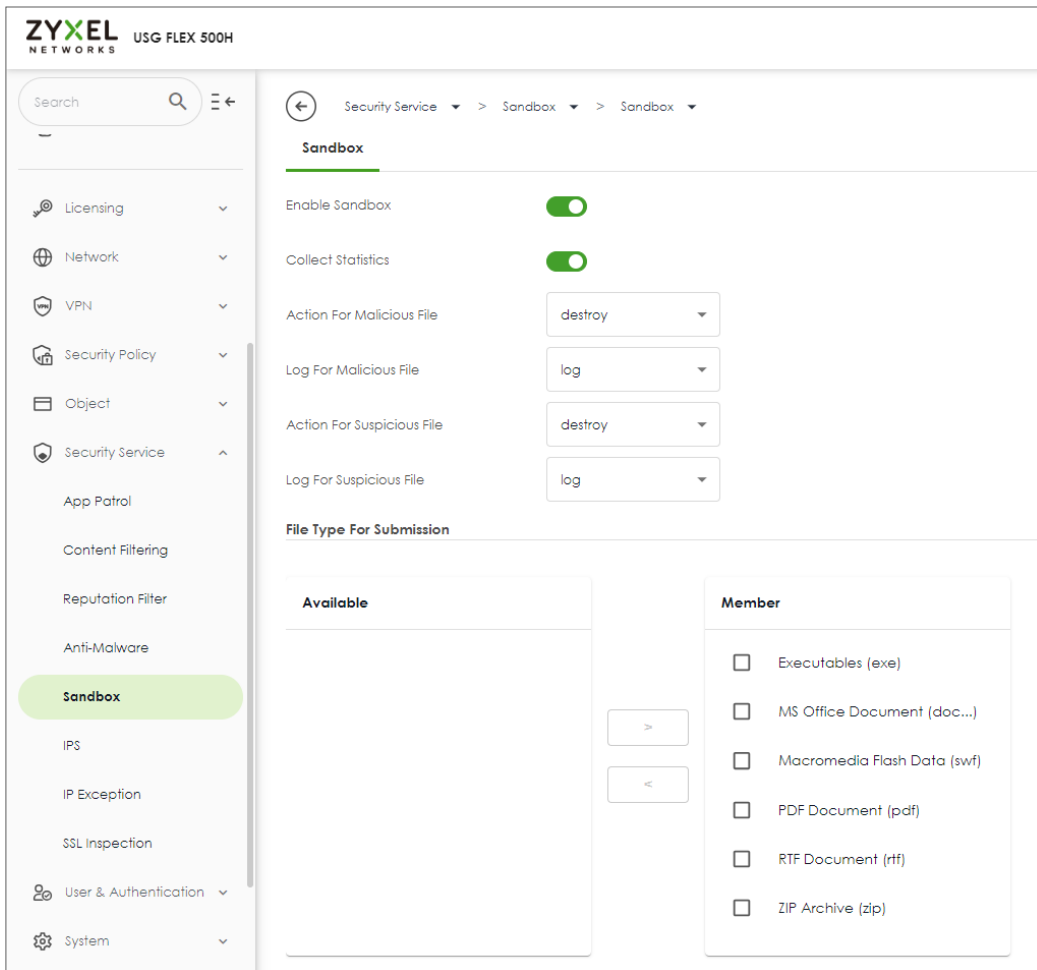
This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



 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 > Log / Events' interface. At the top, there is a breadcrumb navigation, a category dropdown set to 'Sandbox', and buttons for 'Filter', 'Refresh', and 'Clear Log'. A search bar labeled 'Search insights' is also present. Below this is a table with the following data:

#	Time	Category	Message	Source	Destination	Note
2	2023-07-31 16:18:14	Sandbox	Query File name: wildfire-test-pe-file.exe, md5: a2b6580b52aebc6a7e164b70114b4a57, file id: 58207, protocol: HTTP, hId: 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
<b>IP Blocking</b>		
Enable	<input checked="" type="checkbox"/>	
Action	block ▼	
Threat Level Threshold	high ▼	
Log	log ▼	
Statistics	<input checked="" type="checkbox"/>	

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

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

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

The screenshot displays the 'IP Reputation' configuration page. It is divided into two main sections: 'Allow List' and 'Block List'. Both sections have an 'Enable' toggle set to 'on' and a 'Log' dropdown menu. The 'Allow List' section shows a table with the header 'IPv4 Address' and a 'No data' message. The 'Block List' section shows a table with the header 'IPv4 Address' and one entry: '107.155.48.246', which is highlighted with a red box. The interface includes navigation tabs at the top for 'IP Reputation', 'DNS Threat Filter', and 'URL Threat Filter'. Below the table headers, there are icons for '+ Add', 'Edit', 'Remove', 'Active', and 'Inactive'. At the bottom right of the table area, there is a 'Rows per page' dropdown set to '50' and a '0 of 0' indicator.

## 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

**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

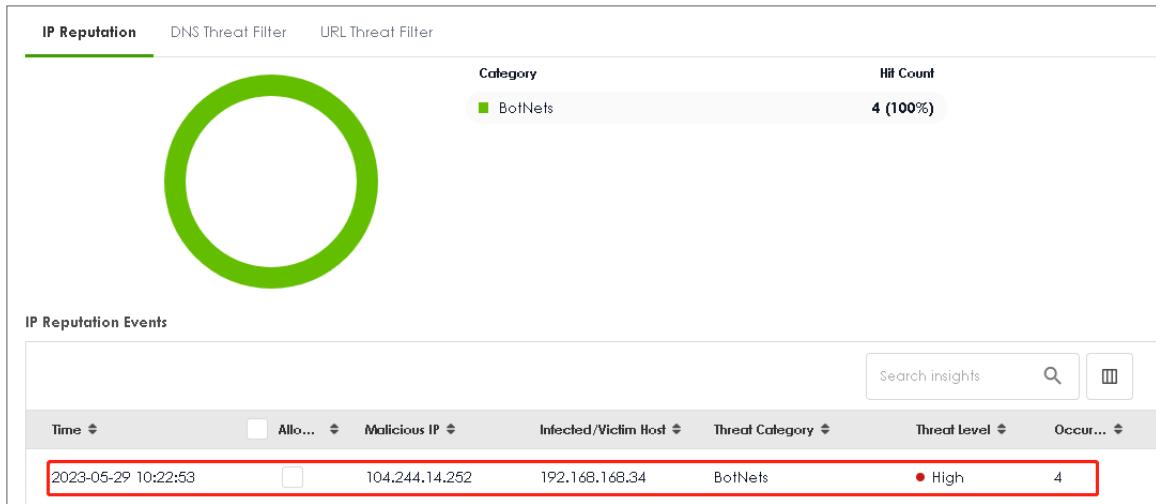
Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.

← 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

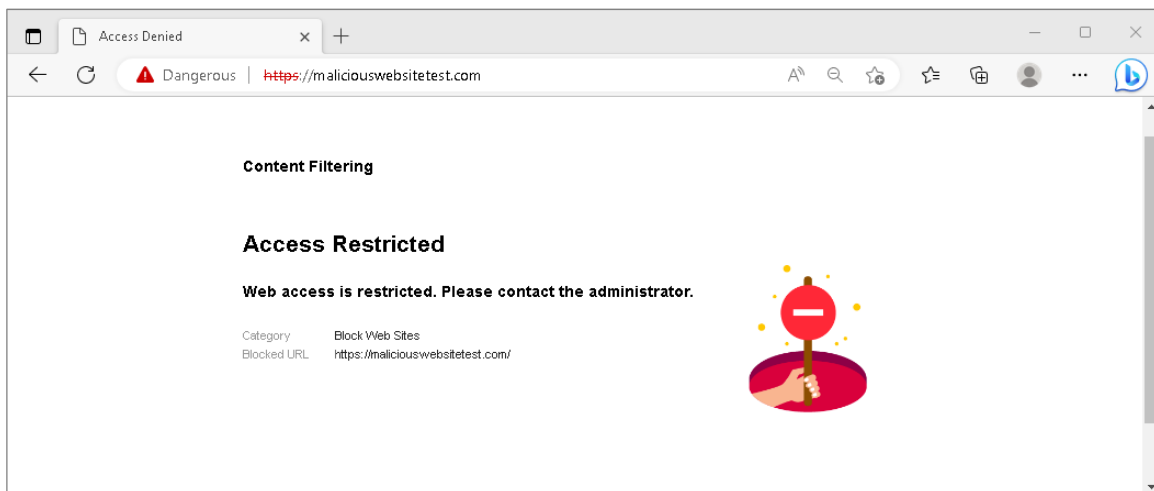
## Test the Result

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	<input type="text" value="https://maliciouswebs"/> <input type="button" value="Query"/>

Message	X
domain category result: <b>information-security,malicious-sites(threat)</b>	
url category result: information-security,malicious-sites(threat)	

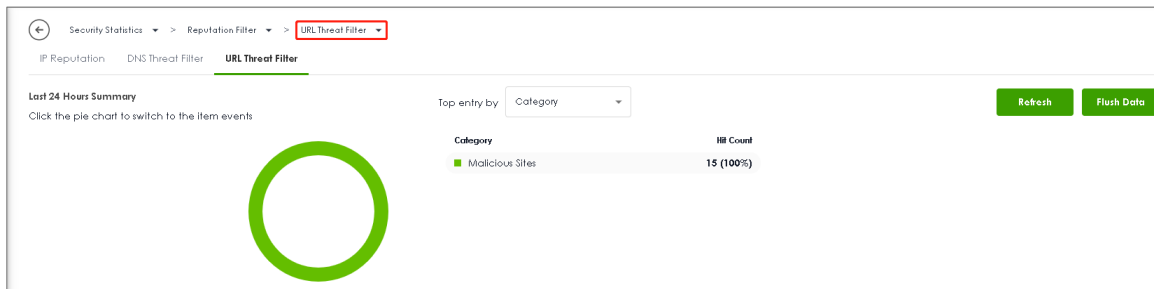
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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

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

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



URL Threat Filter Events

Search insights

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

## How to Configure Reputation Filter- DNS Threat Filter

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

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



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

## Set Up the DNS Threat Filter

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

IP Reputation
DNS Threat Filter
URL Threat Filter

**DNS Threat Filter**

Enable

Action

Log

Redirect IP

Malform DNS packets

	Action	<input type="text" value="drop"/>
	Log	<input type="text" value="log"/>

Statistics

**Security Threat Categories**

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

## Test the Result

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

**Test Domain Name Category**

Domain name to test  Query

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

**Message** ✕

---

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

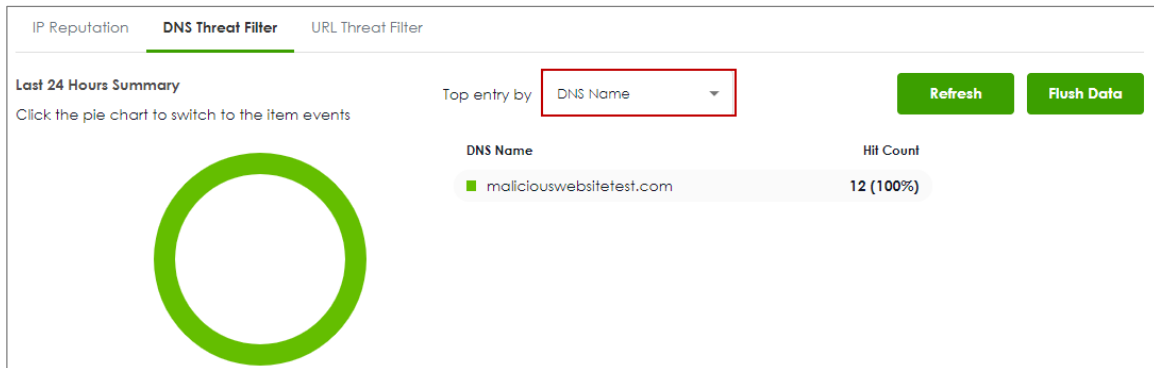
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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

#	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.



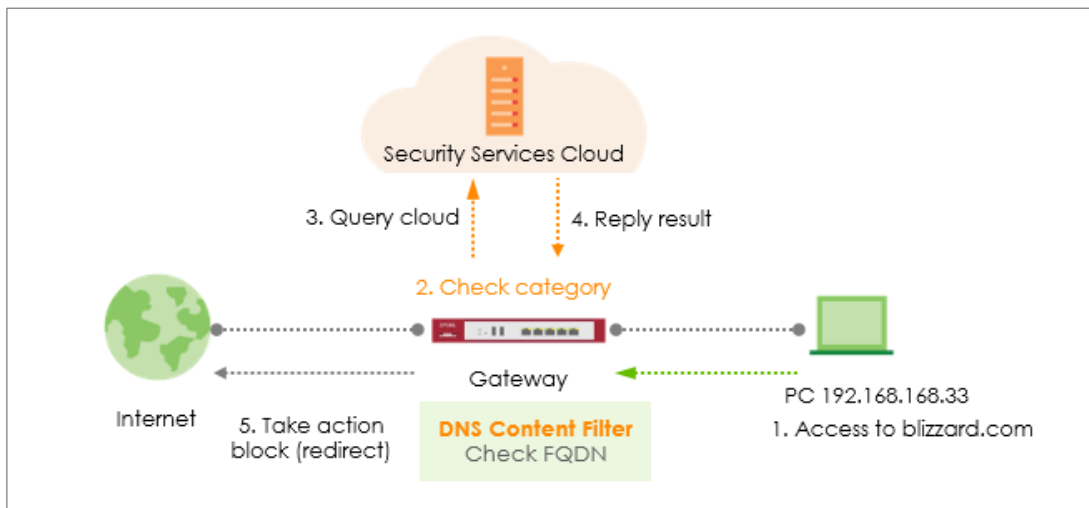
DNS Threat Filter Events


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

## How to Configure DNS Content Filter

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

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



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

## Set Up the DNS Content Filter

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

**Content Filtering**

**For DNS Domain scan:**

Enable DNS Domain scan

Blocked Domain Redirect IP default

Category Server is unavailable Action pass

Log log

Collect Statistics

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

**Profile Management**

+ Add Edit Remove Search insights

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

Action: block

Log: log or log alert

**General Settings**

Name:

Description:

Action:

Log:

Log allowed traffic:

SSL V3 or previous version Connection: Drop

Drop Log:

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  Gristling 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:

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

## Test the Result

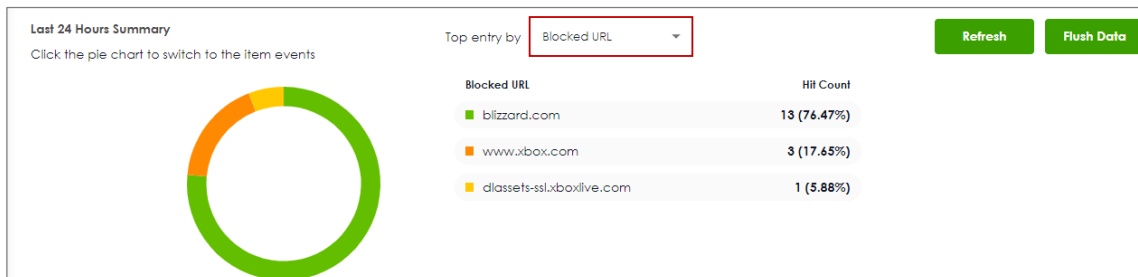
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



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

#	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.



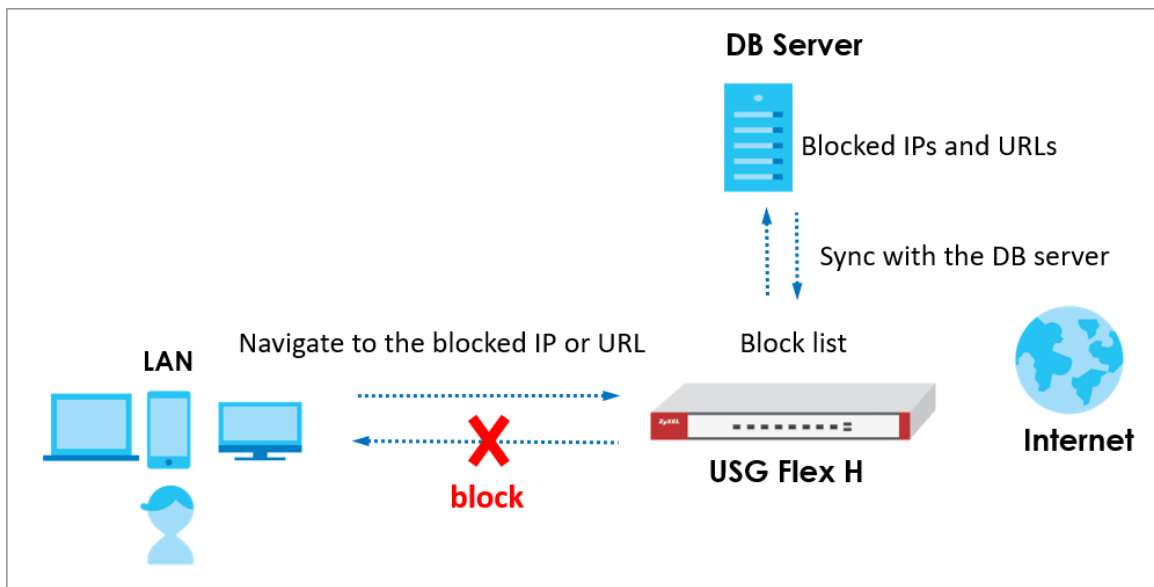
Content Filter Events


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.

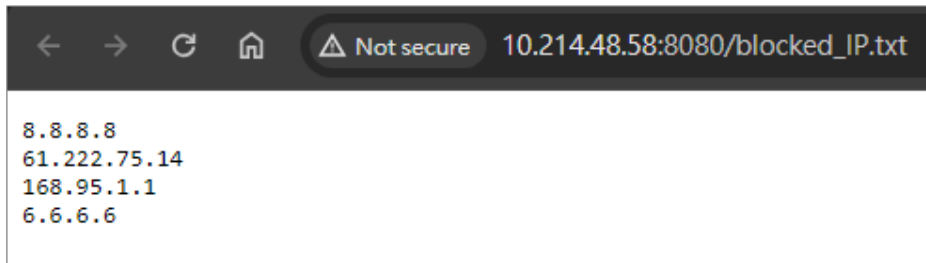


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

## 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_IP.txt)



[http://10.214.48.58:8080/blocked\\_URL.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](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: 1  
 Daily: 4, am  
 Weekly: Monday, 1, am

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](http://10.214.48.58:8080/blocked_URL.txt) and then click "Update Now" to update the block list.

Security Services > External Block List > DNS Threat Filter/URL Threat Filter

IP Reputation    **DNS Threat Filter/URL Threat Filter**

**External Block List**

Enable

**Profile Management**

+ Add    Remove

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

**Signature Update**

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

**Update Now**

Auto Update

Every N Hours    1
   
 Daily    4    pm
   
 Weekly    Monday    1    am

If the DNS/URL threat filter 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 19:31:06	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\>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\>ping 168.95.1.1

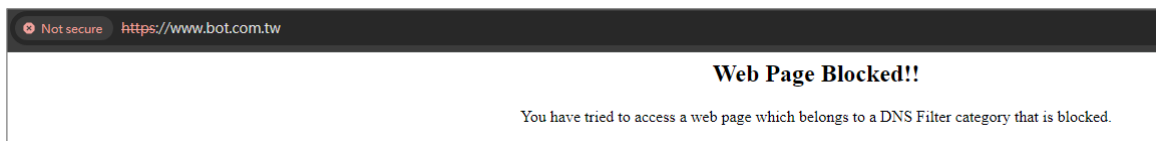
Pinging 168.95.1.1 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.

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.

#	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.



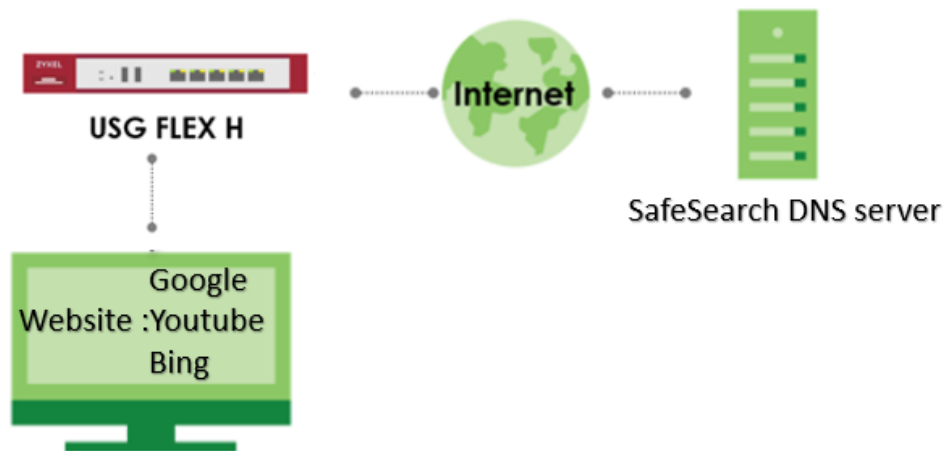
Go to Log & Report > Log / Events to observe block messages.


#	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.

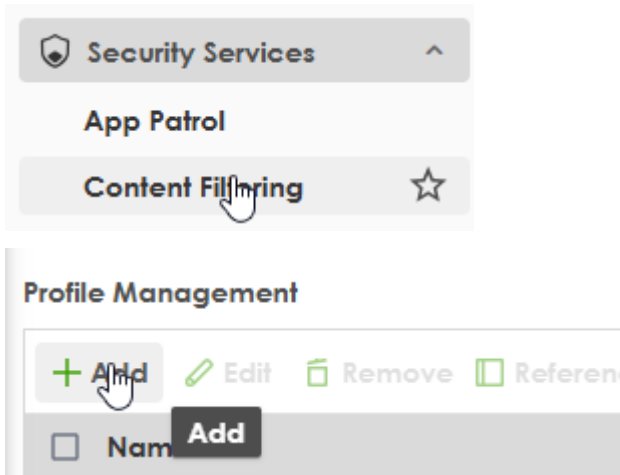
This guide explains how to configure your gateway to set up DNS Safe Search.



 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.



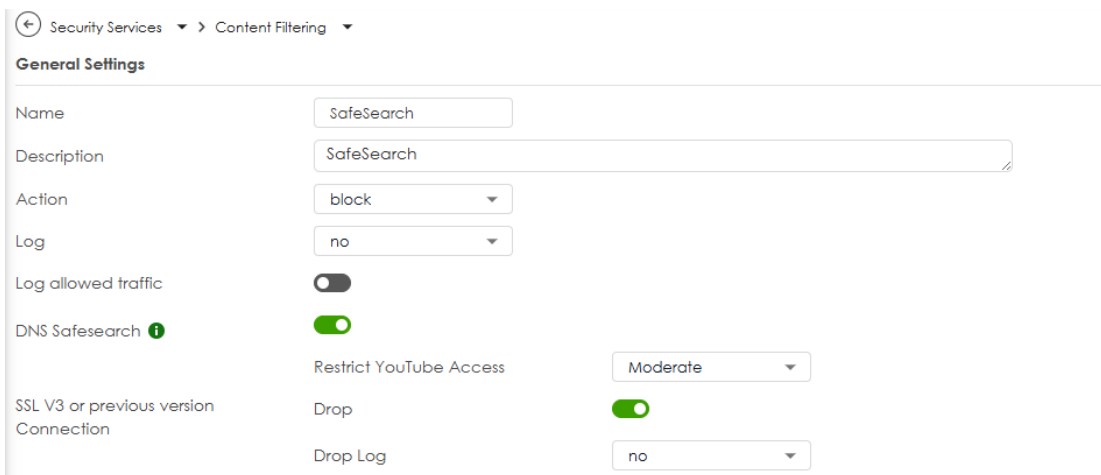
Configure the Profile

**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.



DNS Safesearch ⓘ

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

SSL V3 or previous version Connection

Restrict YouTube Access

Drop

Drop Log

## 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?

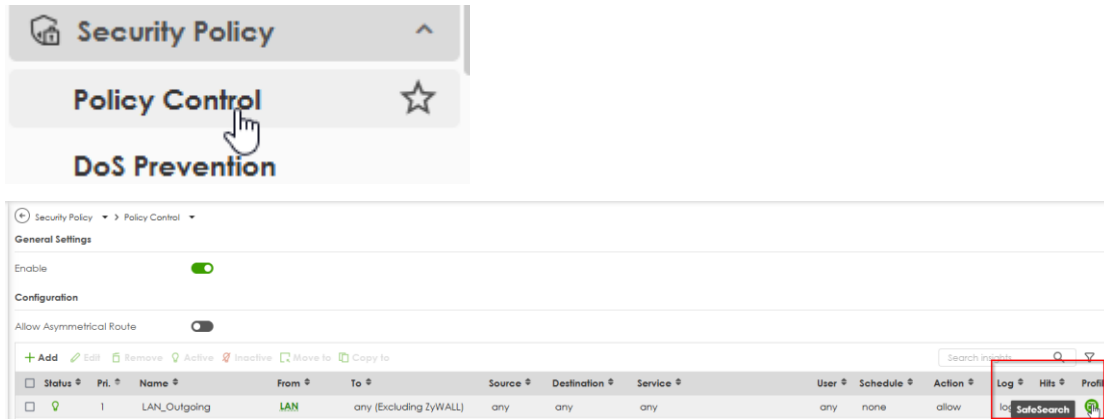


Click OK and apply the profile to the desired rule

Apply SafeSearch to a security policy

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

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



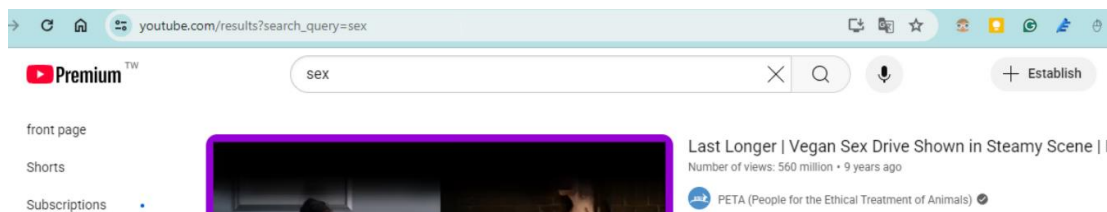
### Step 3: Verified SafeSearch Function

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

www.youtube.com

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

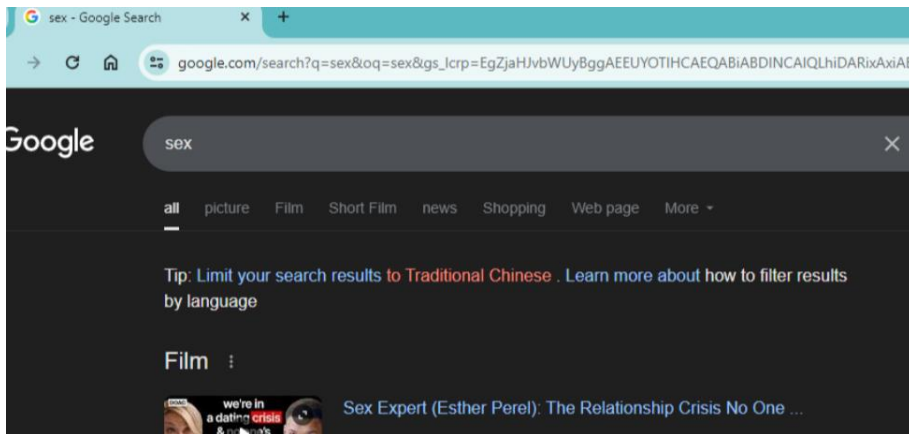
Non-authoritative answer:
Name: youtube-ui.l.google.com
Addresses: 2404:6800:4012:9::200e
           2404:6800:4012:6::200e
           2404:6800:4012:5::200e
           2404:6800:4012:8::200e
           142.250.66.78
           142.250.204.46
           142.250.196.206
           142.250.198.78
Aliases: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



www.google.com

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

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

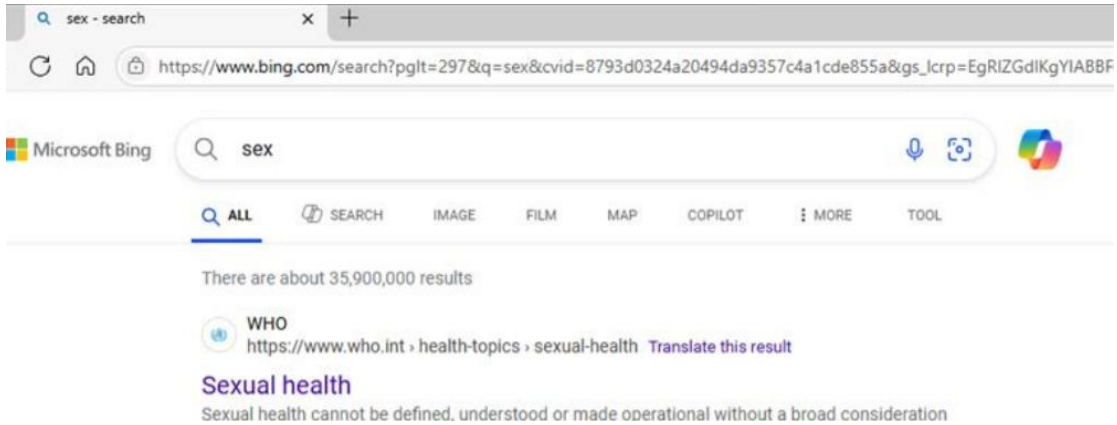


www.bing.com

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

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

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



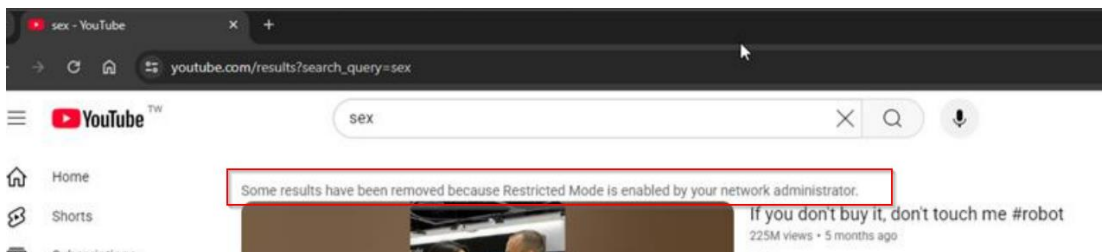
Ensure that the DNS server assignment is automatic get from the firewall.

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

www.youtube.com

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

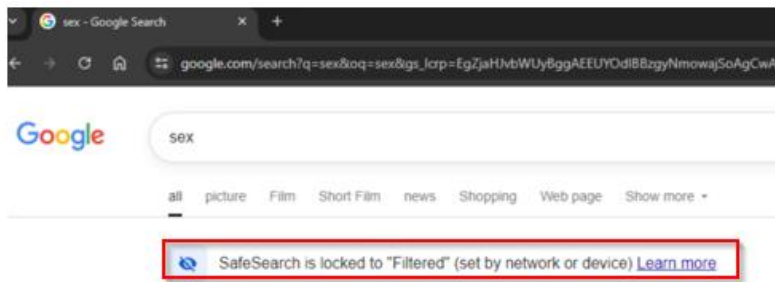
Name: www.youtube.com
Address: 216.239.38.120
Aliases: www.youtube.com
```



www.google.com

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

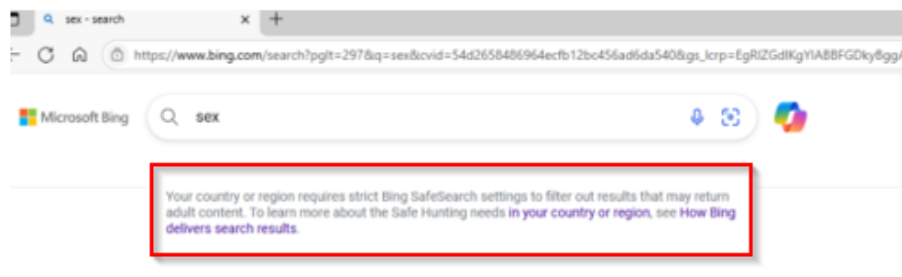
Name:      www.google.com
Address:  216.239.38.120
Aliases:   www.google.com
```



www.bing.com

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

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



## Troubleshooting

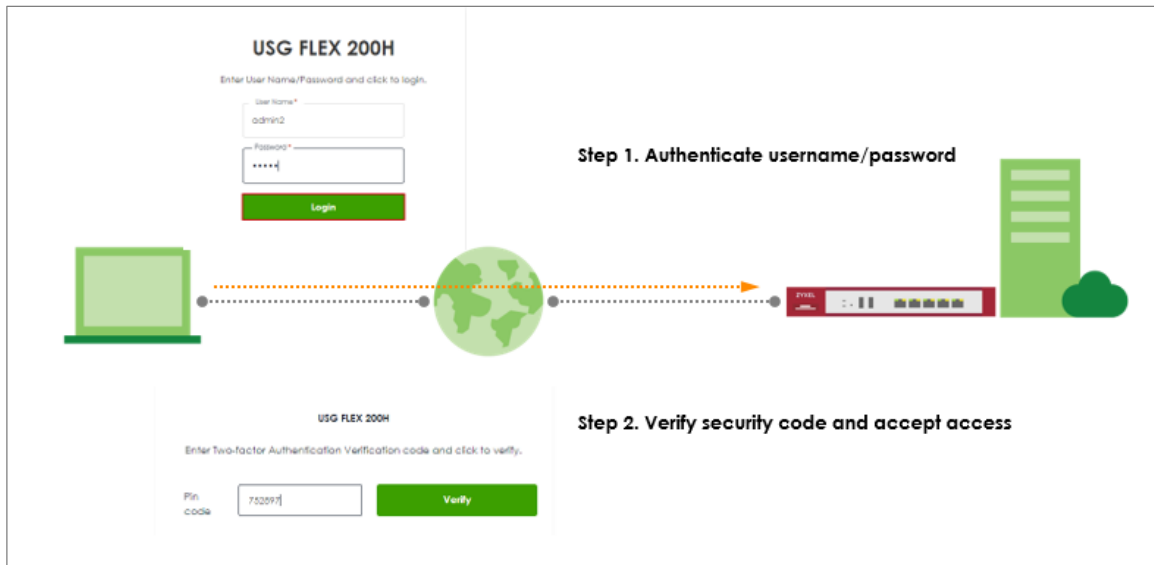
DNS Safe Search is not working

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

## Chapter 3- Authentication

### How to Use Two Factor with Google Authenticator for Admin Access

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



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

## Two Factor with Google Authenticator Flow

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

### Enable Google Authentication on specific admin user

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

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.

**Two-factor Authentication**

Enable Two-Factor Authentication for Admin Access

Finish Setting up Google Authenticator to enable 2FA


Set up Google Authenticator

## Set up Google Authenticator

Set up Google Authenticator

Step 1

Download & install Google Authenticator on your mobile device.




Google Authenticator

GET IT ON Google Play
GET IT ON the App Store

Step 2

Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.



Can not scan the QR code?

Step 3

Verify your device

Enter code

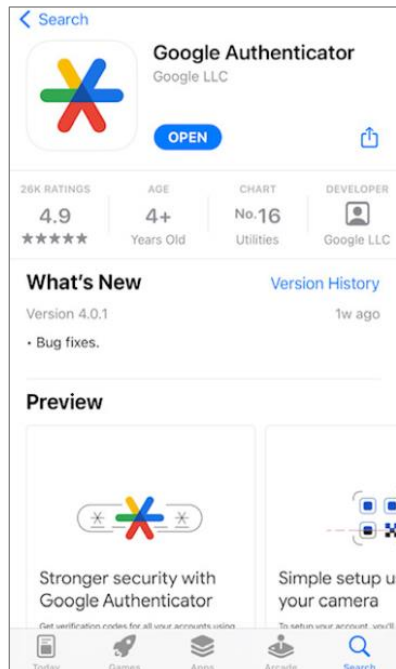
Verify code and finish

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

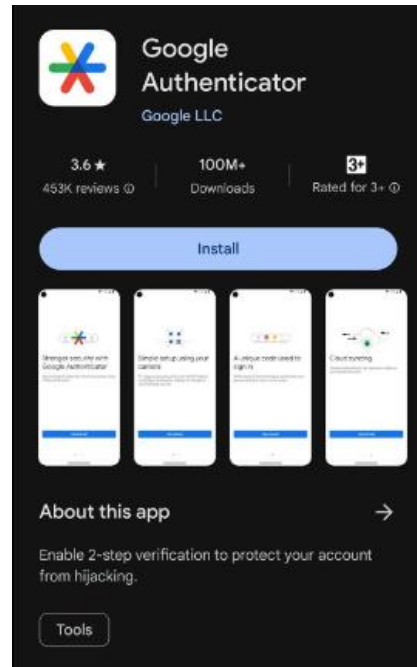
Reset
Apply

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

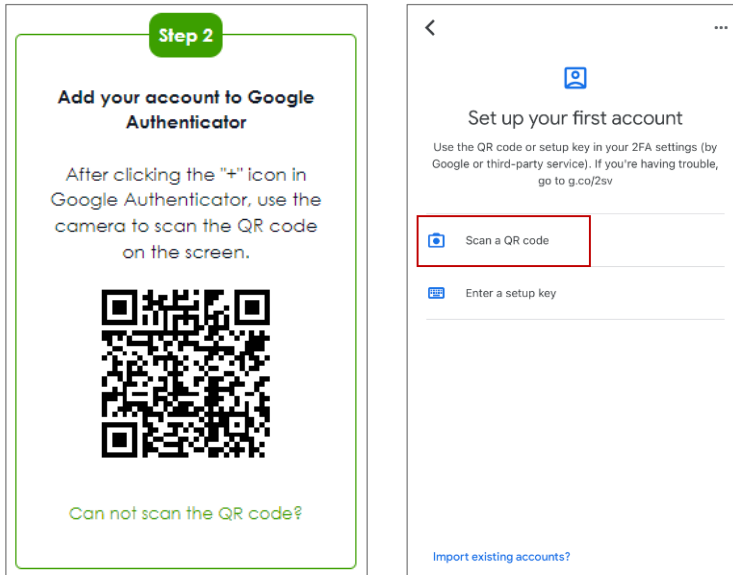
### Apple Store



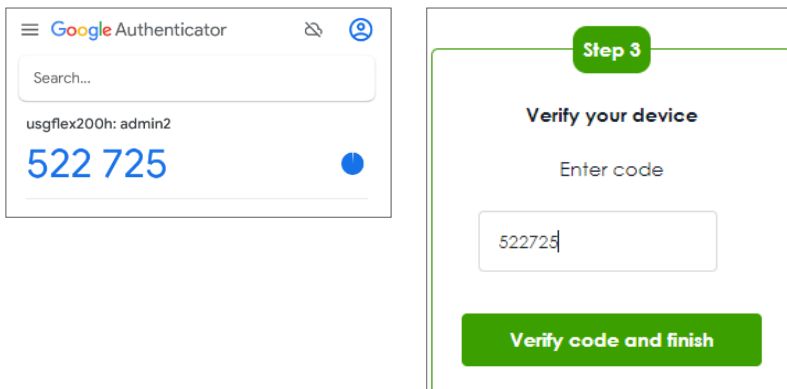
### Google Play



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



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



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

**View your backup codes**

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

**Download**

84177830

93398990

96834809

97350265

59001448

**Regenerate backup codes**

## Configure valid time and login service types

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

**Two-factor Authentication**

---

**Admin Access**

Enable

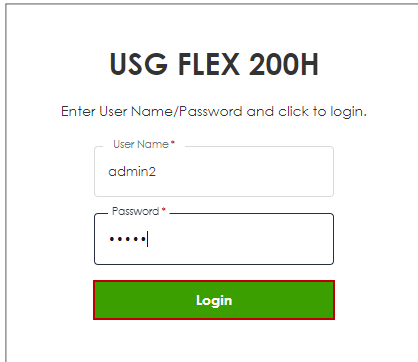
Valid Time  (1-5 minutes)

**Two-factor Authentication for Services:**

Web  SSH

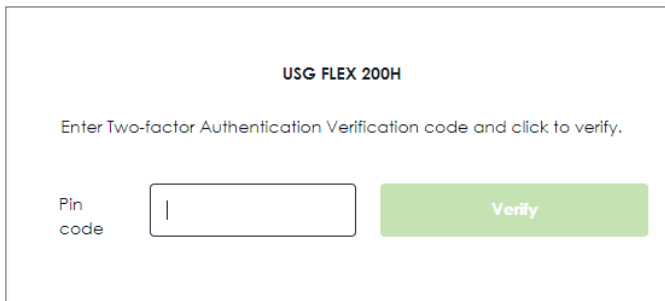
## Test the Result

1. Login with the admin account "admin2".



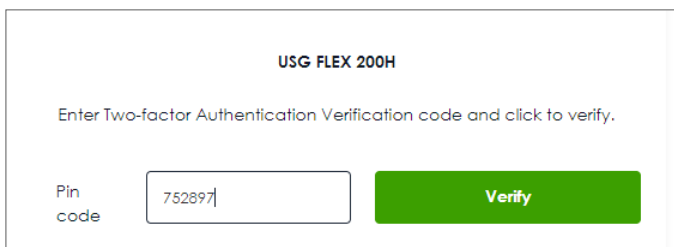
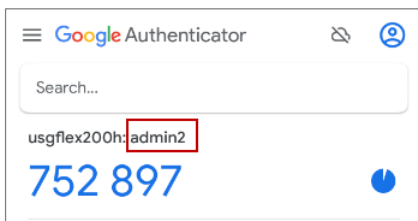
The image shows the login page for the USG FLEX 200H. At the top, it says "USG FLEX 200H". Below that, it says "Enter User Name/Password and click to login." There are two input fields: "User Name" with the value "admin2" and "Password" with masked characters ".....". A green "Login" button is at the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

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



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

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



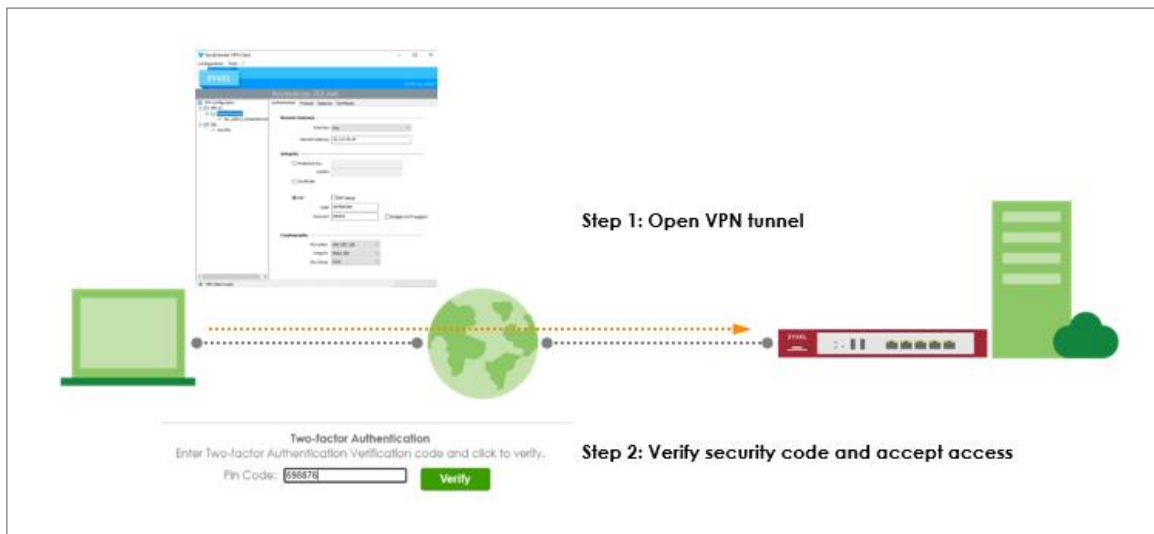
The image shows the verification page for the USG FLEX 200H, similar to the previous one. The "Pin code" input field now contains the code "752897". The "Verify" button is still present.


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

#	Time	Category	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

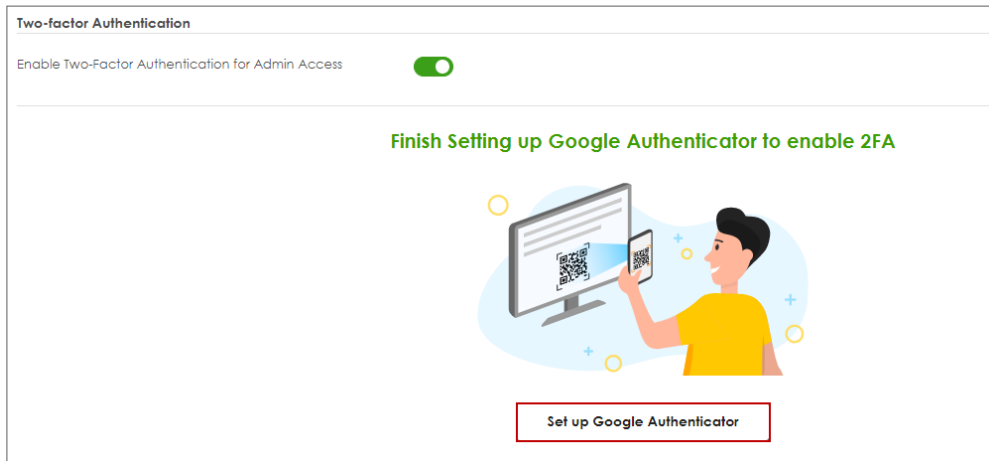
Use Default Settings     Use Manual Settings

Lease Time	1440	minutes
Reauthentication Time	1440	minutes

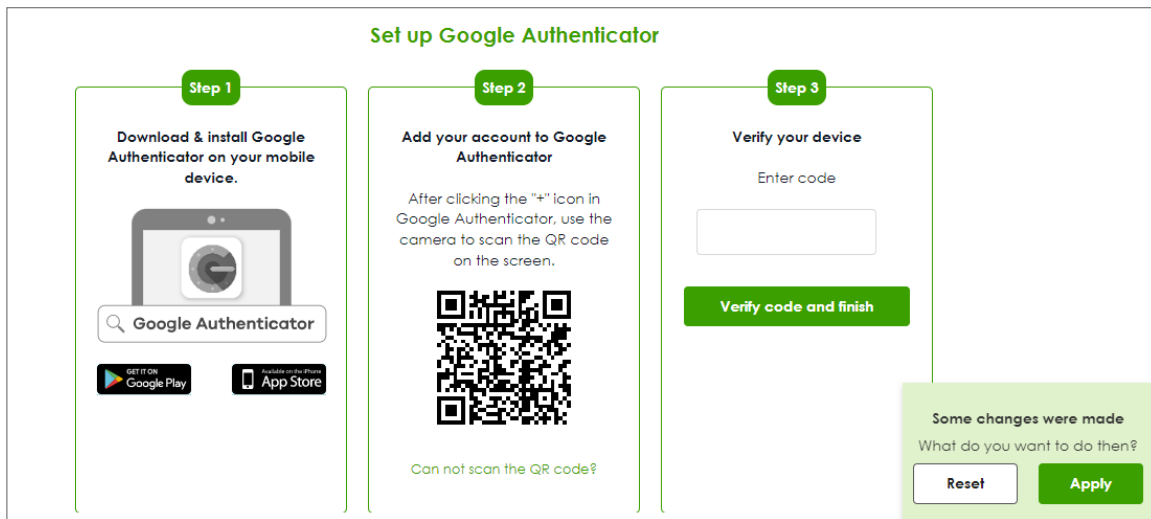
#### Two-factor Authentication

Enable Two-Factor Authentication for VPN Access

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

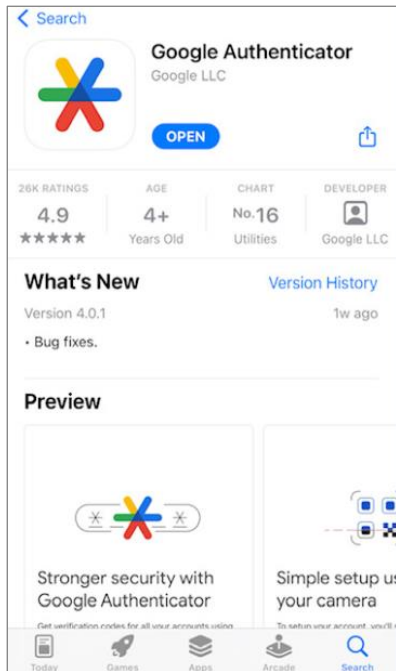


## Set up Google Authenticator

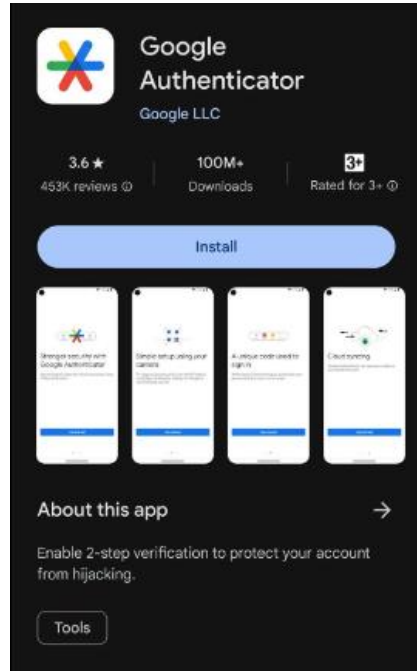


- Download and install Google Authenticator on your mobile device.

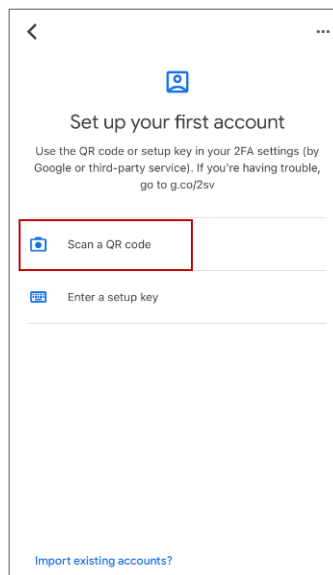
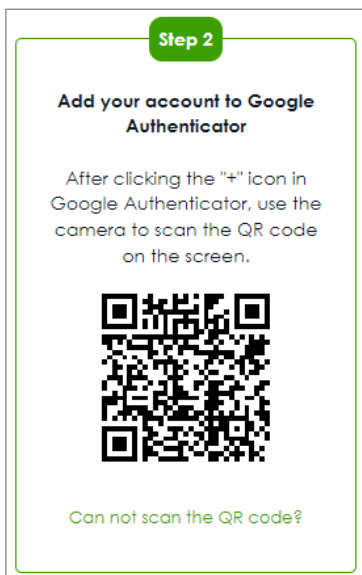
**Apple Store**



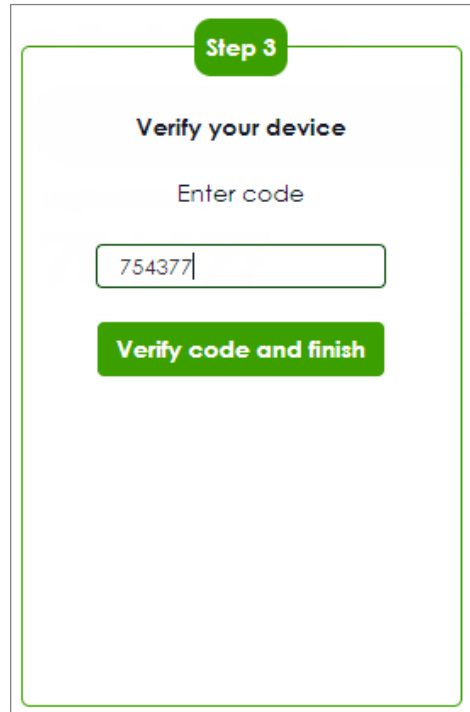
**Google Play**



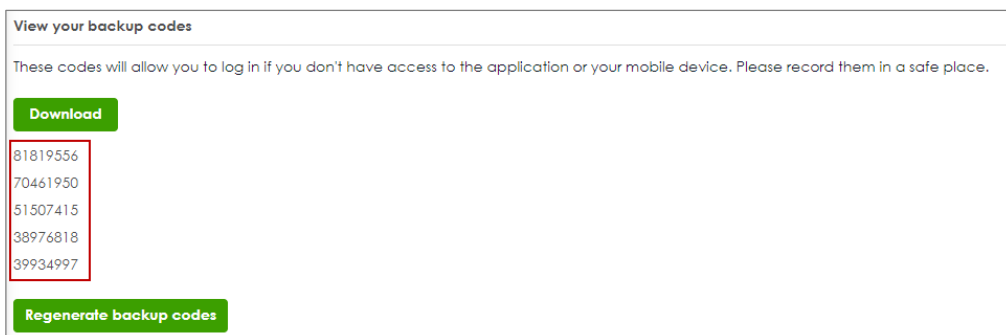
- Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



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.



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.



## Configure valid time and login service types

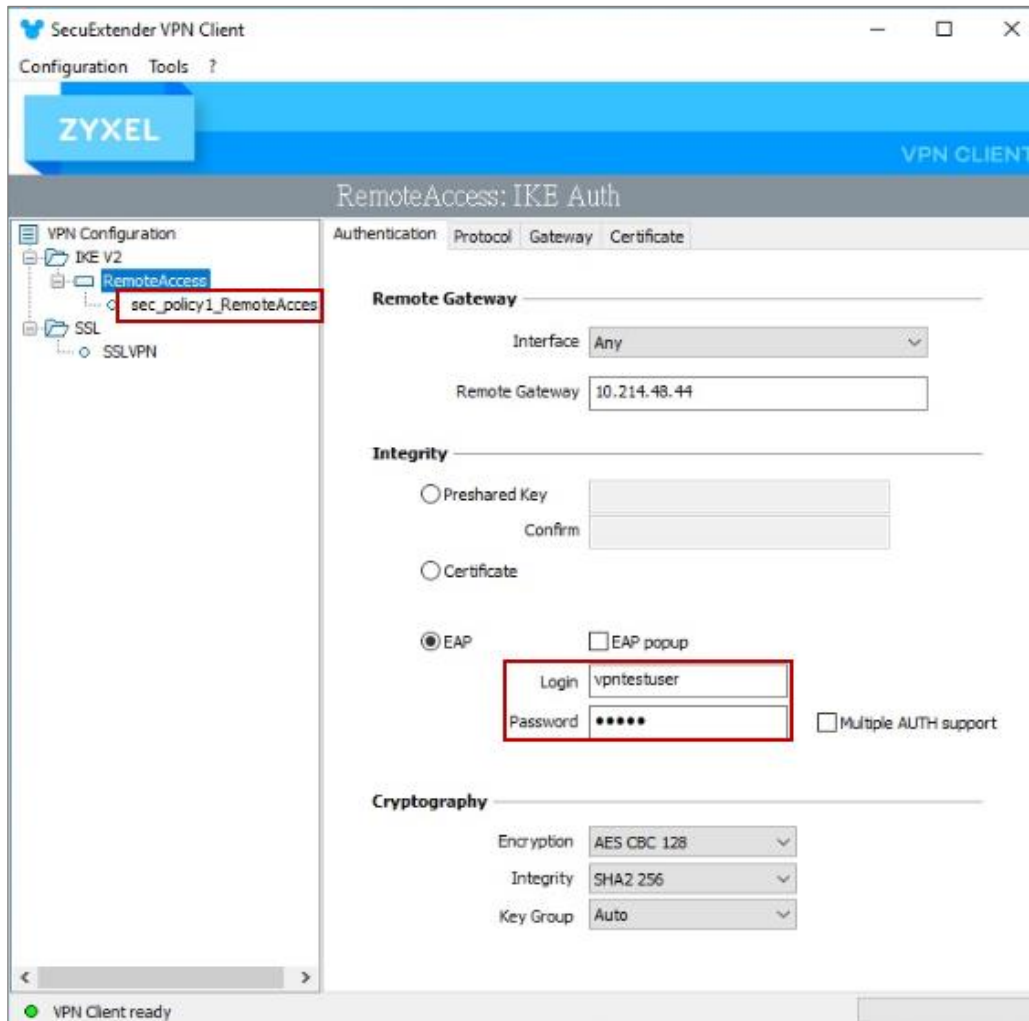
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the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

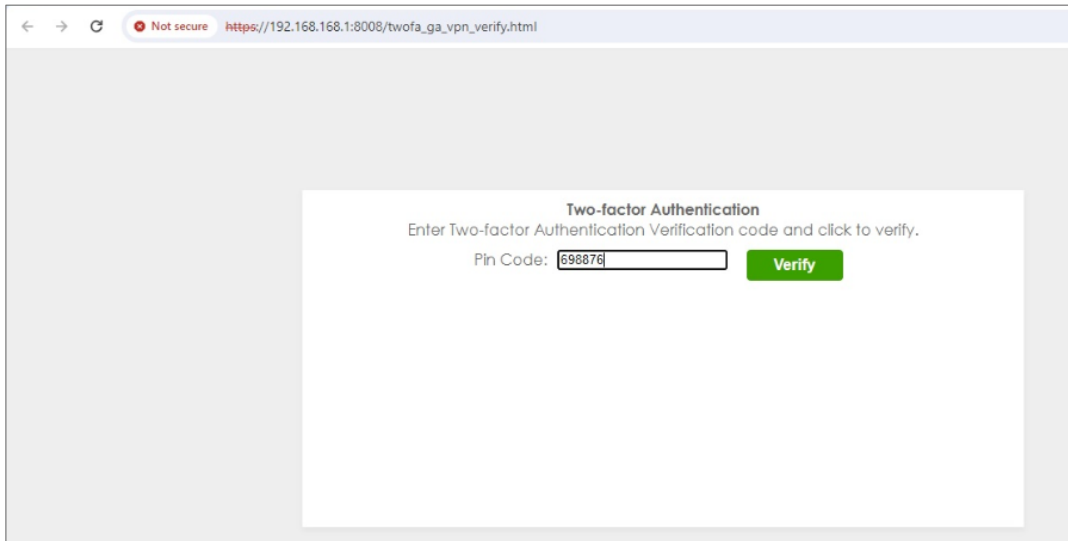
## Test the Result

### Remote Access VPN (IKEv2)

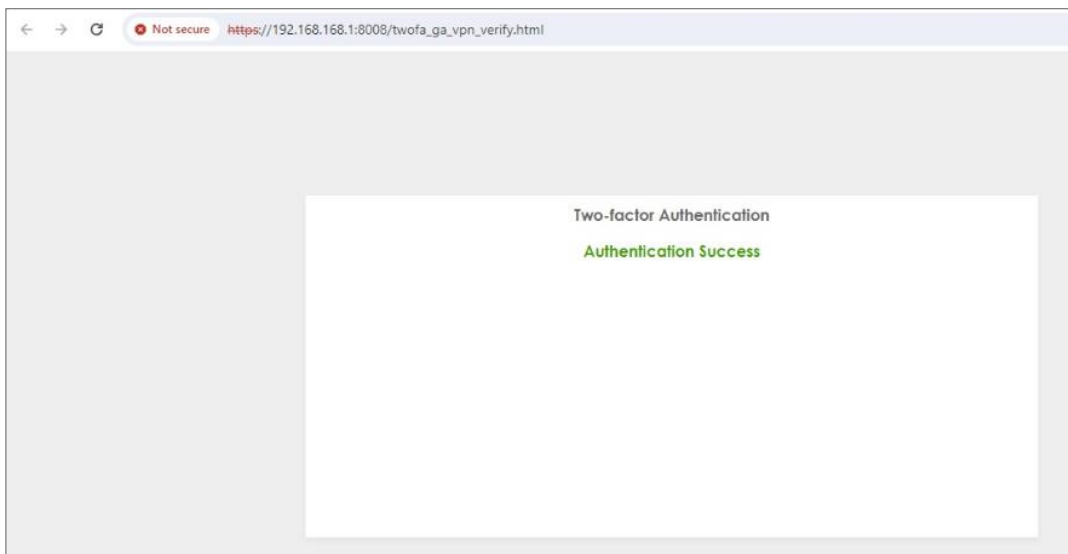
1. Open Remote Access VPN tunnel on SecuExtender VPN Client.



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



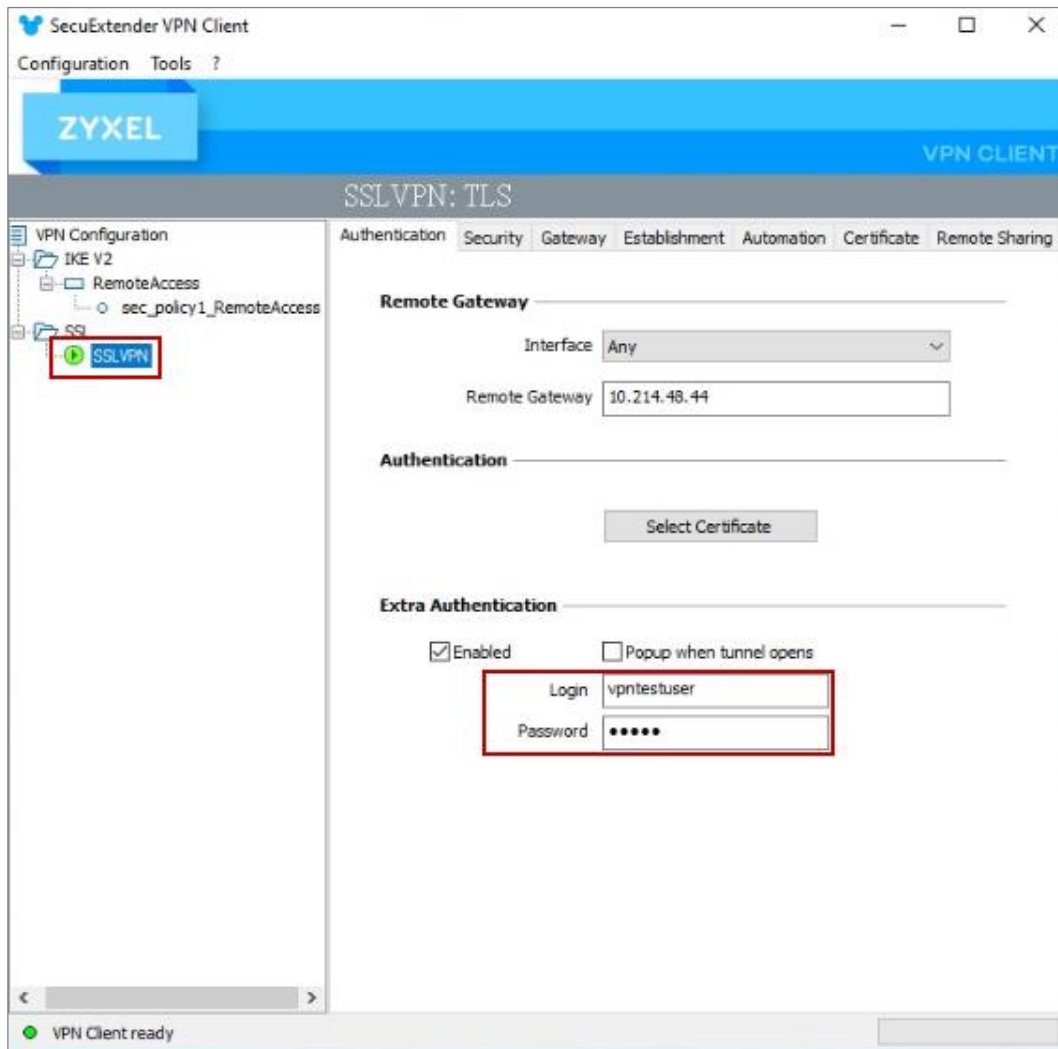
- Authorize with username, password and the token code successfully.



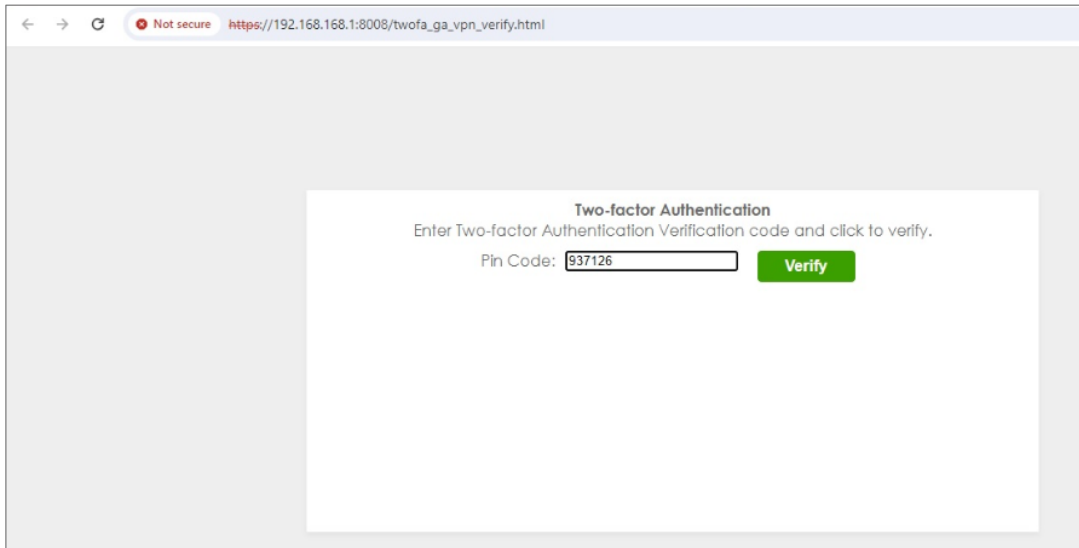
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	user: vptestuser(192.168.50.1) is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
67	2024-03-13 18:22:45	User	User vptestuser(MAC=) from eap-cfg has logged in Device	10.214.48.49	0.0.0.0	0	Account: vptestuser
72	2024-03-13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

## SSL VPN

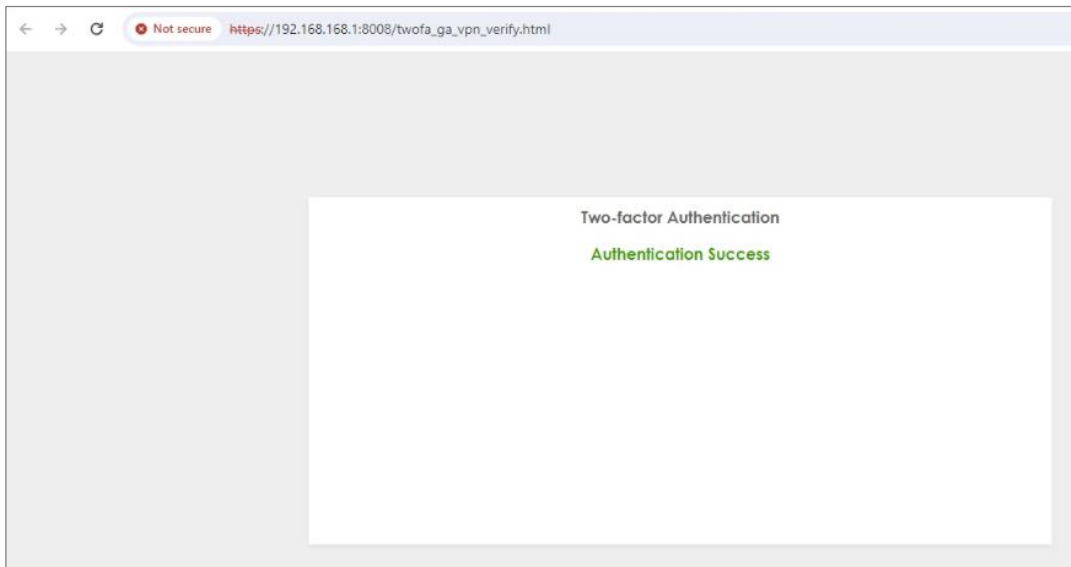
1. Open SSL VPN tunnel on SecuExtender VPN Client.



- 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.



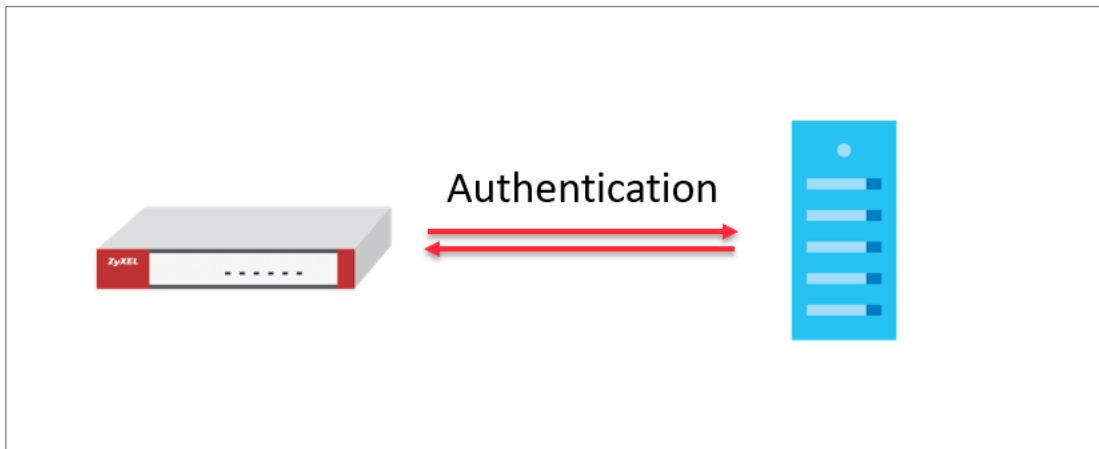
- Authorize with username, password and the token code successfully.



#	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

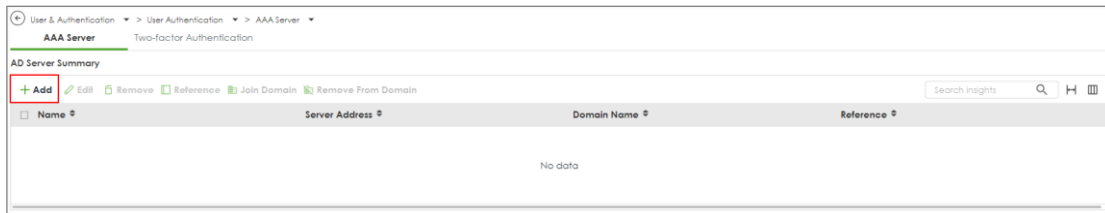
## How to set up AD authentication with Microsoft AD

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.

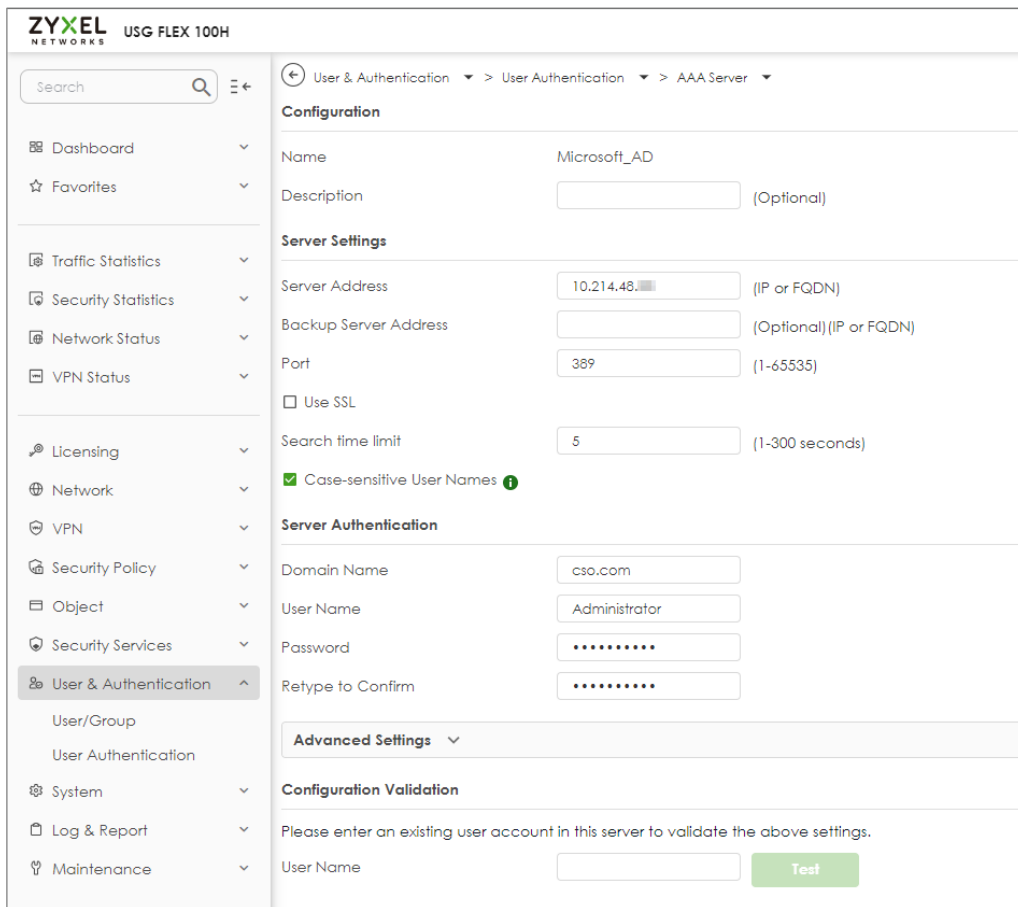


## Set Up a profile for AD server

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.



## 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	DNS Server	Query Via
cs0.com	10.214.48.20	ge1 (WAN)

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

Name	Server Address	Domain Name	Reference
Microsoft_AD	10.214.48.20	cs0.com	0

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

Name	Server Address	Domain Name
Microsoft_AD	10.214.48.20	cs0.com

**Join AD Domain**

Associated AD Server Object: Microsoft\_AD

AD Domain Name: cs0.com

NetBIOS Domain Name: cs0

User Name: Administrator

Password: \*\*\*\*\*

Retype to Confirm: \*\*\*\*\*

After join domain successfully, you can see this icon.

Name	Server Address	Domain Name	Join Domain	Reference
Microsoft_AD	10.214.48.20	cs0.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	<input type="text" value="cso.com"/>
User Name	<input type="text" value="Administrator"/>
Password	<input type="password" value="....."/>
Retype to Confirm	<input type="password" value="....."/>

**Advanced Settings** ▾

### Configuration Validation

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

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

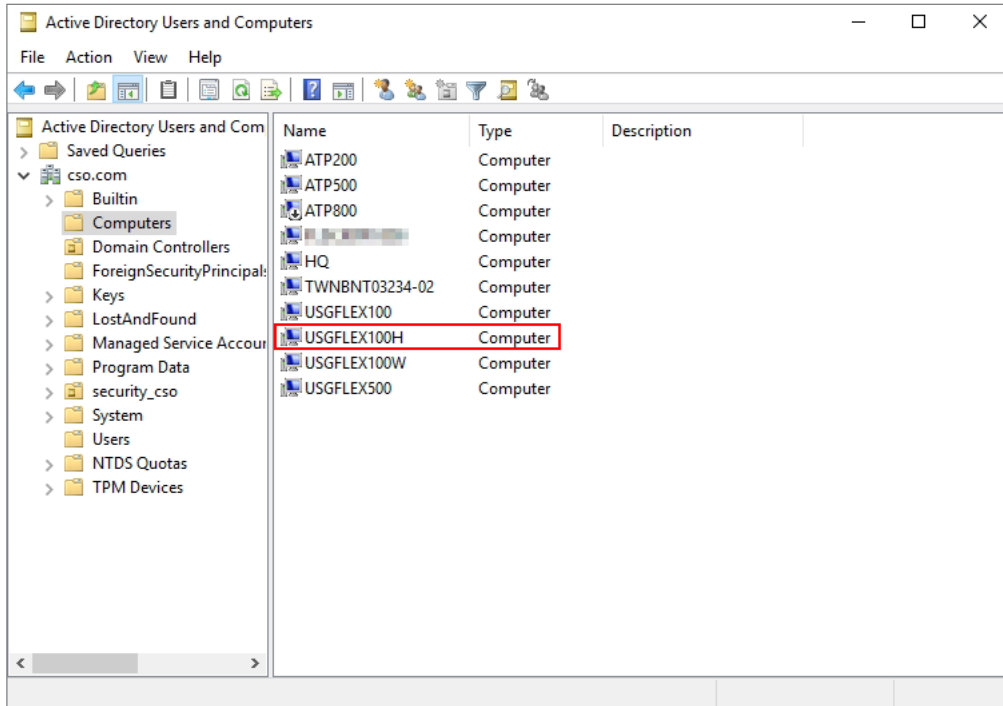
Test Status

OK

Returned User Attributes

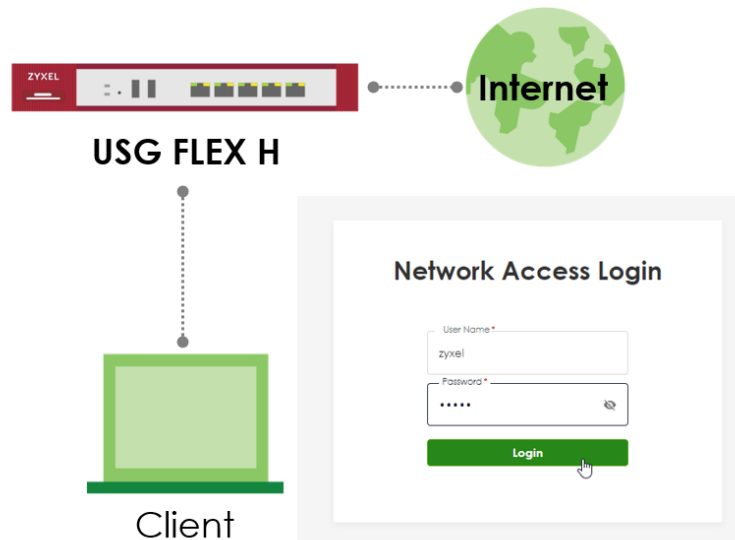
```
dn: CN=stanley,CN=Users,DC=cso,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: stanley
distinguishedName: CN=stanley,CN=Users,DC=cso,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: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


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



## How to Set Up Captive Portal?

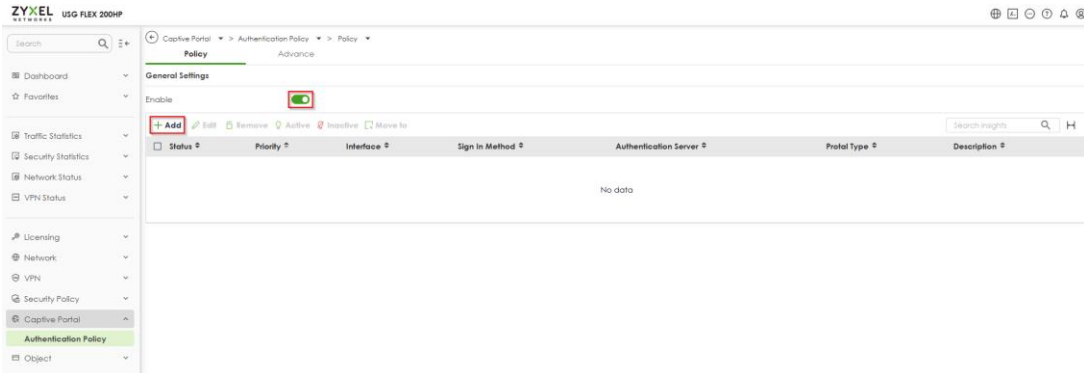
The Captive Portal feature provides functionality that requires LAN client users to complete the authentication procedure of Network Access Login page before accessing the internet. This article will guide users on how to set up and verify this feature.



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

## Configure the Captive Portal via the Web-GUI

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



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

Captive Portal > Authentication Policy

**General Settings**

Enable

Description

**Criteria**

Incoming

Source Address

Destination Address

Exempt List

+ Add - Remove

Type	Object
<input type="checkbox"/> Service	<input type="text" value="DNS"/>

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

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

Portal Type

Internal

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:

Redirect TCP Port 443 Traffic to Login Page

Idle Timeout

Log

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

← Captive Portal > > Authentication Policy > > Policy >

**Policy** Advance

**General Settings**

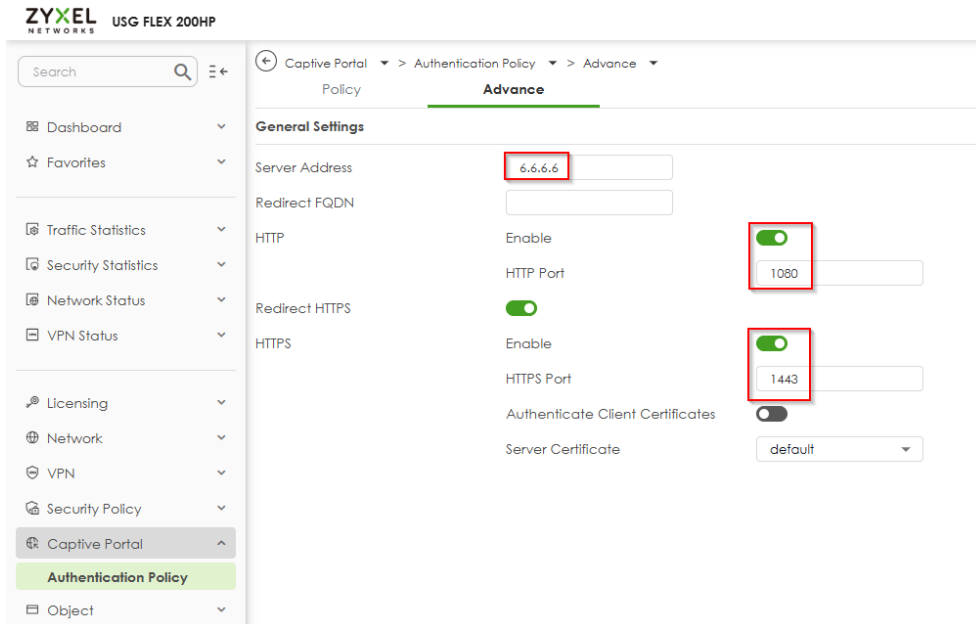
Enable

+ Add Edit Remove Active Inactive Move to

Search insights

Status	Pri.	Incoming	Source	Destination	Sign-in Method	Sign-on With	Portal Type	Description
<input type="checkbox"/>	1	ge3	any	any	sign-on	local	internal	test captive portal

- 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.



## Verify the Captive Portal function

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

- 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:

5. Enter the login User Name and Password.

Welcome

---

Username/Email

Password:

Login

---

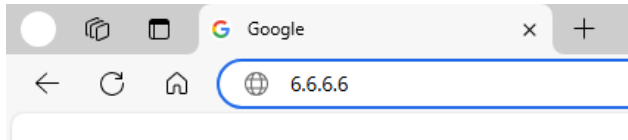
Powered by **ZYXEL**

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.

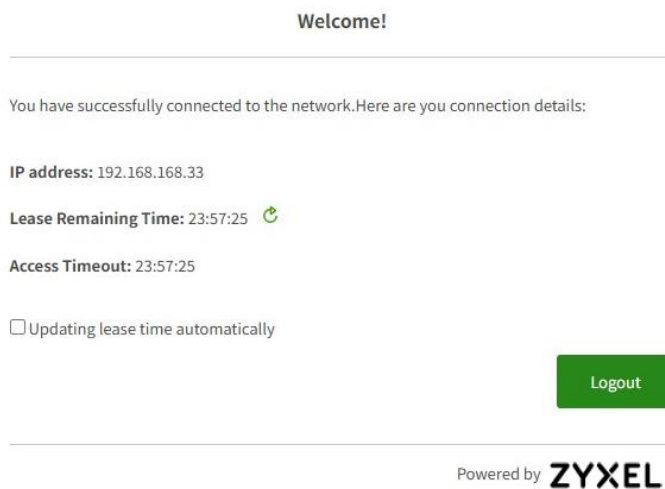


## How to logout the Captive Portal?

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



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



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.



## 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.

#	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.

#	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.

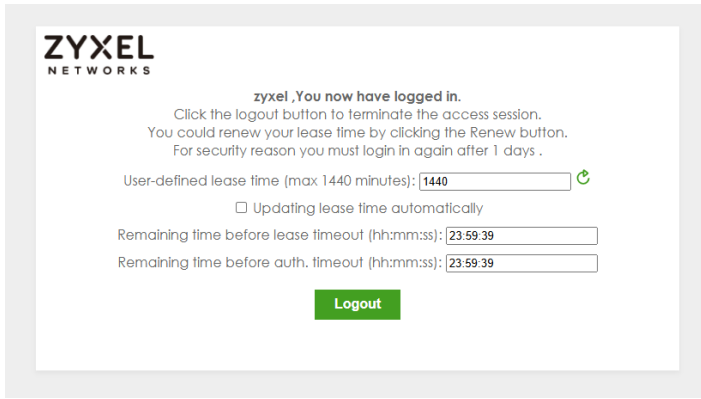
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
59	2025-03-17 14:13:34	User	User zyxel from captive portal has logged out Device	192.168.168.35	192.168.168.1	0	Account: zyxel

## Feature Change:

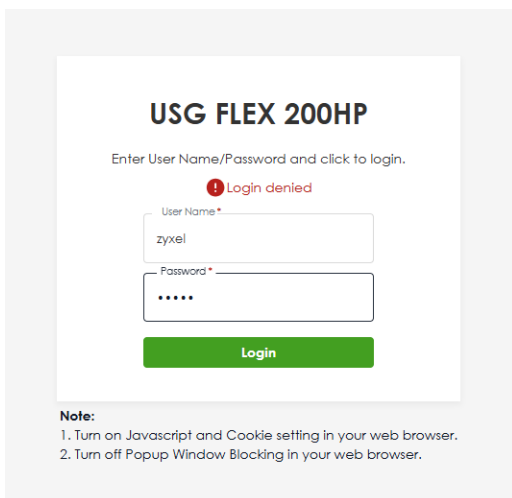


Starting from firmware version uOS 1.32, the user must log in to the Captive Portal before using the User Aware function for security policy or BWM policy utilization.

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

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
<input checked="" type="checkbox"/>	1	For_The_User	LAN	any (Excluding ZyWALL)	any	any	any	zyxel	none	allow	no	3	

Network > BWM

General Settings

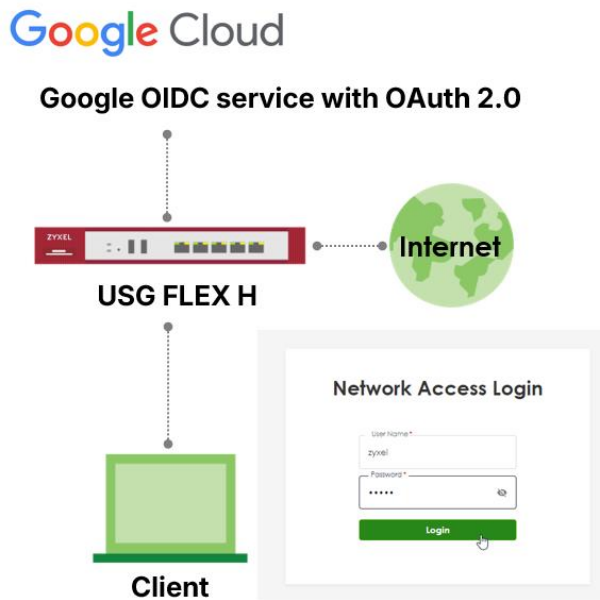
Enable

Configuration

Status	Pri.	Name	Description	User	Incoming Interface	Outgoing Interface	Source	Destination	Service	BWM Download/Upload/Pri
<input checked="" type="checkbox"/>	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  Browse... Upload

Password  (PKCS#12 only)

## 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' page for a Captive Portal. The breadcrumb navigation is 'Captive Portal > Authentication Policy > Settings'. The page is divided into 'Policy' and 'Settings' tabs, with 'Settings' selected. Under 'Server Settings', the following fields are visible:

Server Address	<input type="text" value="6.6.6.6"/>
Redirect FQDN	<input type="text" value="portal.company.com"/>
HTTP	Enable <input checked="" type="checkbox"/>
HTTP Port	<input type="text" value="1080"/>
Redirect HTTPS	<input type="checkbox"/>
HTTPS	Enable <input checked="" type="checkbox"/>
HTTPS Port	<input type="text" value="1443"/>
Authenticate Client Certificates	<input type="checkbox"/>
Server Certificate	<input type="text" value="portal.company.com"/>

## 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

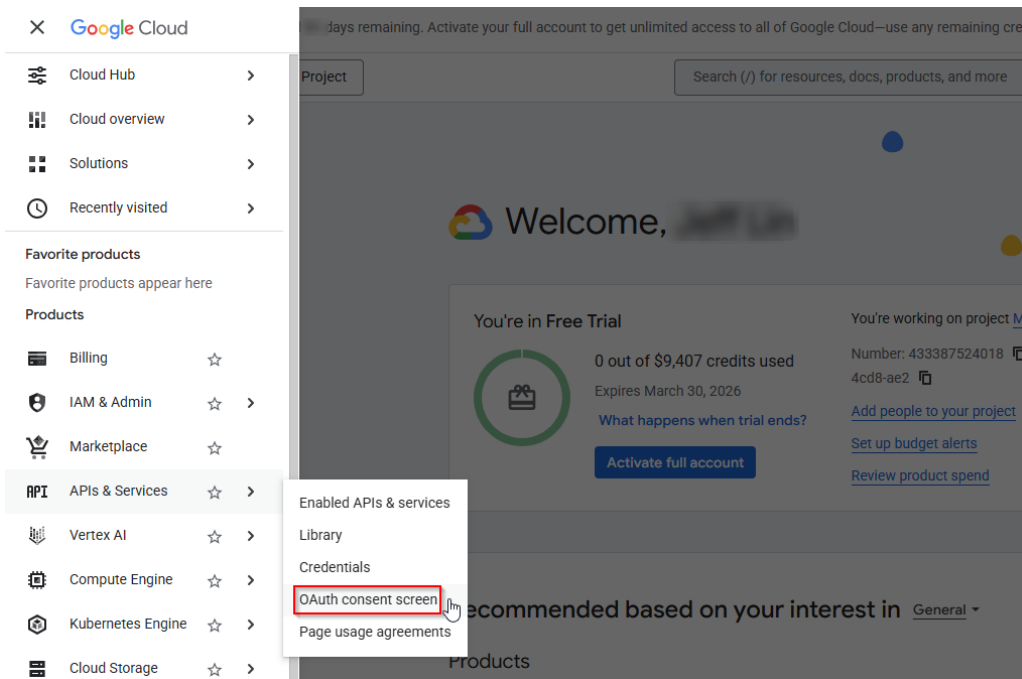
HTTPS Port

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 navigation menu on the left. Under the 'APIs & Services' category, a dropdown menu is open, and 'OAuth consent screen' is highlighted with a red box. The background shows the Google Cloud console interface with a 'Welcome' message and a 'Free Trial' status.

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

Google Auth Platform / Overview / Create branding

Overview | Project configuration

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

### 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

Project configuration

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

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.

The image displays two sequential screenshots of the ZyXel project configuration interface. Both screenshots feature a left-hand navigation menu with the following items: Overview (selected), Branding, Audience, Clients, Data Access, Verification Center, and Settings. The main content area is titled 'Project configuration' and shows a progress indicator with four steps: 1. App Information (checked), 2. Audience (checked), 3. Contact Information (active), and 4. Finish (disabled).

In the top screenshot, the 'Contact Information' step is active. It contains a text input field labeled 'Email addresses \*' with the value '1@gmail.com'. Below the field is a note: 'These email addresses are for Google to notify you about any changes to your project.' and a 'Next' button. At the bottom of the configuration area are 'Create' and 'Cancel' buttons.

In the bottom screenshot, the 'Finish' step is highlighted with a blue border, indicating it is the current step. The 'Next' button is no longer visible, and the 'Create' and 'Cancel' buttons remain at the bottom.

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: eaub2oagv05a8c0d39u91yjd6956t8.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

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

Search insights


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: eaub2oagv05a8c0d39u91vjd6956tf8.apps.googleusercontent.com

← Client ID for Web application

**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.)

**Client secrets**

Client secret	****s06h
Creation date	December 29, 2025, 4:53:52 PM GMT+8
Status	Enabled

**Authorized redirect URIs**

For use with requests from a web server

**Authorized JavaScript origins**

For use with requests from a browser

**Name \***

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.

**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.)

**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

**Authorized JavaScript origins**

For use with requests from a browser

**Authorized redirect URIs**

For use with requests from a web server

URIs 1 \*

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

**Save** **Cancel**

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:   
 user\_attr\_name: email  
 state: t\_ce13fddfacaef4fd97192f748b1a32077

#### ID Token Claims

- iss: https://accounts.google.com
- azp: ...oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- aud: ...oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- sub: ...10187679099756
- email: ...@gmail.com
- email\_verified: True
- at\_hash: ...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 > User Authentication > Advanced'. The 'Authentication Proxy' section is active, with the following settings:

- Enable:
- HTTPS Port:
- Server Certificate:



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

Redirect FQDN

HTTP Enable

HTTP Port

Redirect HTTPS

HTTPS Enable

HTTPS Port

Authenticate Client Certificates

Server Certificate

### 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 path is System > DNS & DDNS > DNS. The 'Address Record' section is active, showing a table with columns for Hostname, Domain, and IP Address. A new record is being added with Hostname empty, Domain 'fqdn2.yourdomain', and IP Address '6.6.6.6'. Below this are sections for CNAME Record, MX Record, and Domain Zone Forwarder, all currently empty. A green notification box at the bottom right says 'Some changes were made' and 'What do you want to do then?' with 'Cancel' and 'Apply' buttons.

## 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

**Criteria**

Incoming

Source Address

Destination Address

Exempt List

+ Add  Remove

<input type="checkbox"/>	Type	Object
<input type="checkbox"/>	Service	DNS

Enable Walled Garden

Walled Garden List

+ Add  **OIDC Providers**  Remove

<input type="checkbox"/>	Type	OIDC Providers
		No data

**OIDC Providers** ×

**Google**

Microsoft

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

OIDC Providers

+ Add  OIDC Providers  Remove

Type	Object
<input type="checkbox"/> Domain Name	accounts.google.com
<input type="checkbox"/> Domain Name	apis.google.com
<input type="checkbox"/> Domain Name	*client-channel.google.com
<input type="checkbox"/> Domain Name	clients*.google.com
<input type="checkbox"/> Domain Name	contacts.google.com
<input type="checkbox"/> Domain Name	*googleusercontent.com
<input type="checkbox"/> Domain Name	mail.google.com
<input type="checkbox"/> Domain Name	mail-attachment.google.com
<input type="checkbox"/> Domain Name	ogs.google.com
<input type="checkbox"/> Domain Name	play.google.com
<input type="checkbox"/> Domain Name	ssl.gstatic.com
<input type="checkbox"/> Domain Name	www.gstatic.com
<input type="checkbox"/> Domain Name	oauth2.googleapis.com
<input type="checkbox"/> Domain Name	accounts.google.com.*
<input type="checkbox"/> Domain Name	fonts.gstatic.com
<input type="checkbox"/> 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

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

Portal Type

Internal

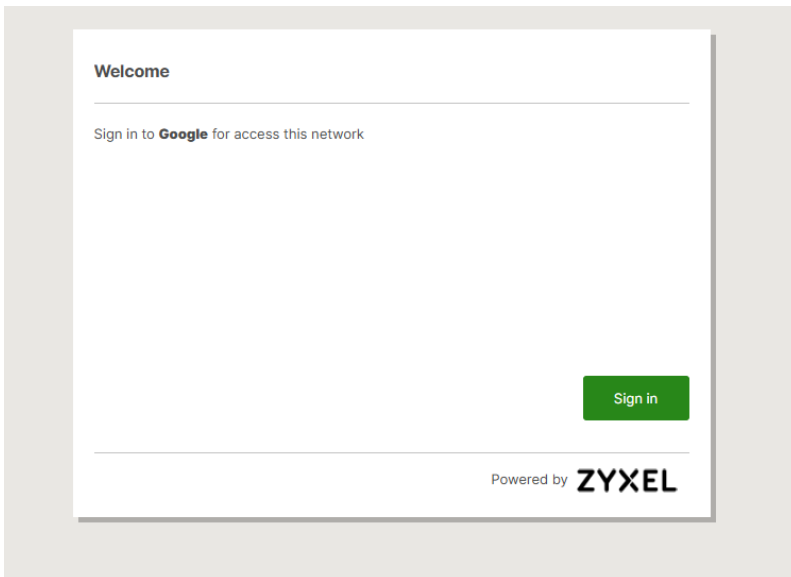
External

URL

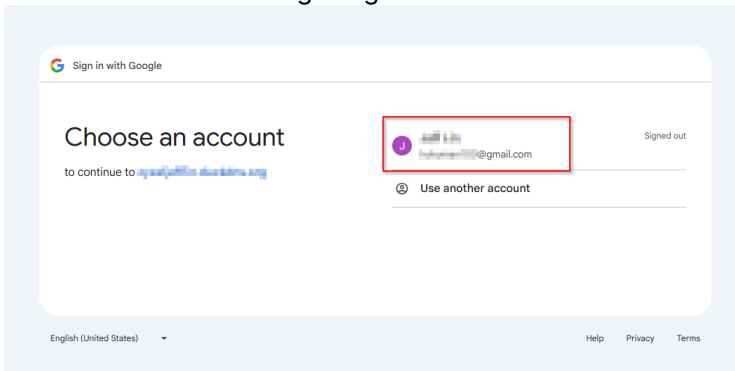
## Verification- Test User Login

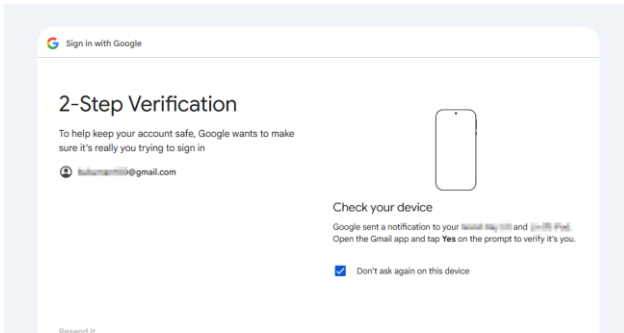
Verify that the Captive Portal correctly redirects unauthenticated users to Google Workspace/Cloud and grants access after successful authentication.

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

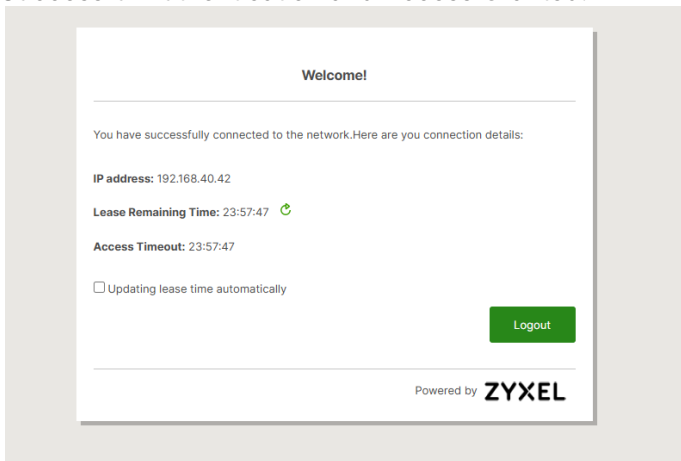


3. Confirm redirect to Google login





4. Successful Authentication and Access Granted.



Internet access is successful.



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

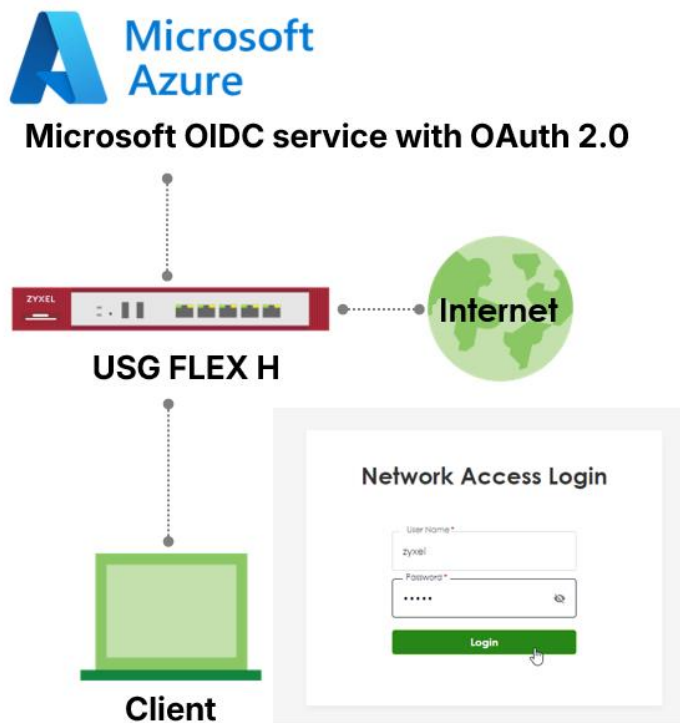
Network Status > Login Users > Login Users

Force Log Out

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1								
2								
3								
4	redacted@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' page for a Captive Portal. The breadcrumb navigation is 'Captive Portal > Authentication Policy > Settings'. The page is divided into 'Policy' and 'Settings' tabs, with 'Settings' selected. Under 'Server Settings', the following fields are visible:

Server Address	<input type="text" value="6.6.6.6"/>
Redirect FQDN	<input type="text" value="portal.company.com"/>
HTTP	Enable <input checked="" type="checkbox"/>
HTTP Port	<input type="text" value="1080"/>
Redirect HTTPS	<input type="checkbox"/>
HTTPS	Enable <input checked="" type="checkbox"/>
HTTPS Port	<input type="text" value="1443"/>
Authenticate Client Certificates	<input type="checkbox"/>
Server Certificate	<input type="text" value="portal.company.com"/>

## 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 resolve to the WAN IP of your firewall.

← User & Authentication > User Authentication > Advanced >

AAA Server      Two-factor Authentication      **Advanced**


---

**Authentication Proxy**

Enable

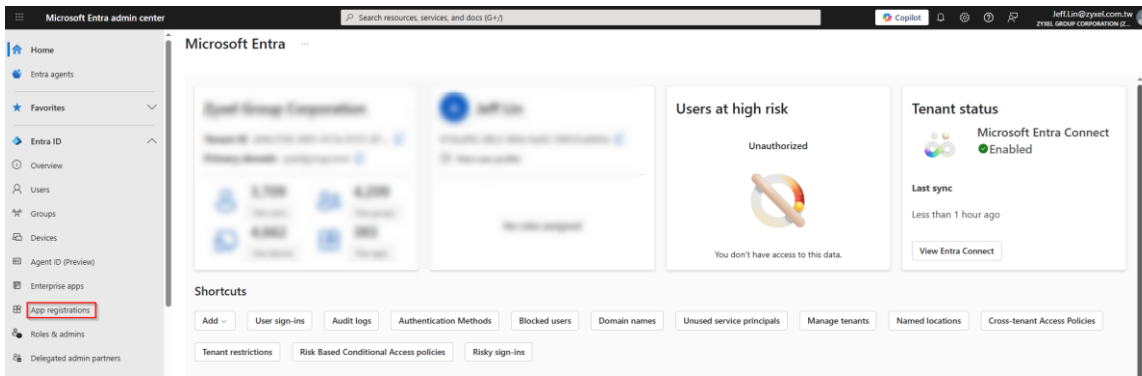
HTTPS Port

Server Certificate

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

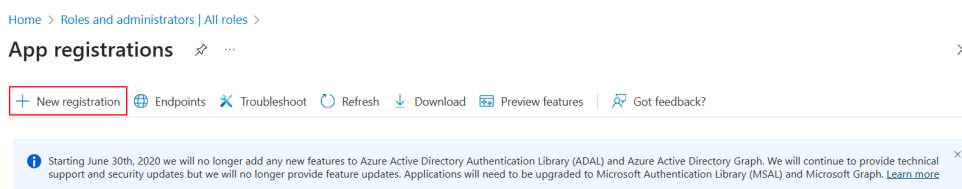
## Microsoft Entra ID

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



The screenshot shows the Microsoft Entra admin center interface. In the left-hand navigation pane, the 'App registrations' option is highlighted with a red box. The main content area displays various dashboard tiles for user management and system status.

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



The screenshot shows the 'App registrations' page in the Microsoft Entra admin center. The '+ New registration' button is highlighted with a red box. Below the button, there are links for 'Endpoints', 'Troubleshoot', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. A notification banner at the bottom states: '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'.

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	Client credentials	: 0 certificate_1_secret
Application (client) ID	: [REDACTED]	Redirect URIs	: <a href="#">Add a Redirect URI</a>
Object ID	: [REDACTED]	Application ID URI	: <a href="#">Add an Application ID URI</a>
Directory (tenant) ID	: [REDACTED]	Managed application in L...	: <a href="#">Captive-Portal</a>

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

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

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
New client secret			

No client secrets have been created for this application.

**Add a client secret**

Description:

Expires:

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? →

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
USGFlex2004P	6/28/2026	<span style="border: 1px solid red; padding: 2px;">[Redacted Value]</span>	[Redacted ID]

## 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) 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 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

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

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 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/[REDACTED]/v2.0

Client ID: [REDACTED]

Client Secret: [REDACTED]

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	: <a href="#">Captive-Portal</a>	Client credentials	: <a href="#">0 certificate_1 secret</a>
Application (client) ID	: <a href="#">XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</a>	Redirect URIs	: <a href="#">Add a Redirect URI</a>
Object ID	: <a href="#">XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</a>	Application ID URI	: <a href="#">Add an Application ID URI</a>
Directory (tenant) ID	: <a href="#">XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</a>	Managed application in l...	: <a href="#">Captive-Portal</a>

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

 <b>Web</b> Build, host, and deploy a web server application. .NET, Java, Python <a href="#">Select →</a>	 <b>Single-page application</b> Configure browser client applications and progressive web applications. Javascript. <a href="#">Select →</a>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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:

**Advanced Settings** ▾

**Configuration Validation**

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

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]5083fad1b10adc815177
- rh: [redacted]9feRWmF6OM8ODCn7x1Dh6Vp23TTIU4sAZJUAA.
- sub: [redacted]ha6V6KD7kjgCu2bdoyI9HKDg
- tid: [redacted]7de456985e8
- uti: [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).

The screenshot shows the configuration page for the Authentication Proxy. The breadcrumb navigation is 'User & Authentication > User Authentication > Advanced'. There are three tabs: 'AAA Server', 'Two-factor Authentication', and 'Advanced'. The 'Advanced' tab is selected. 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

### 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 path is System > DNS & DDNS > DNS. The 'Address Record' section is active, showing a table with columns for Hostname, Domain, and IP Address. The Domain field contains 'fqdn2.yourdomain' and the IP Address field contains '6.6.6.6'. Below this, there are sections for CNAME Record, MX Record, and Domain Zone Forwarder, all of which are currently empty. A green notification box at the bottom right indicates '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
<input type="checkbox"/> Service	DNS

Enable Walled Garden

Walled Garden List

Type	Object
<input checked="" type="checkbox"/> 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  
URL

**OIDC Providers** [X]

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

<input type="checkbox"/>	Type	Object
<input type="checkbox"/>	Domain Name	*.aadcdn.msftauth.net
<input type="checkbox"/>	Domain Name	*.aadcdn.msftauthimages.net
<input type="checkbox"/>	Domain Name	*.aadcdn.msauthimages.net
<input type="checkbox"/>	Domain Name	*.logincdn.msftauth.net
<input type="checkbox"/>	Domain Name	*.msauth.net
<input type="checkbox"/>	Domain Name	*.aadcdn.microsoftonline-p.com
<input type="checkbox"/>	Domain Name	*.microsoftonline-p.com
<input type="checkbox"/>	Domain Name	aadcdn.msftauth.net
<input type="checkbox"/>	Domain Name	aadcdn.msftauthimages.net
<input type="checkbox"/>	Domain Name	aadcdn.msauthimages.net
<input type="checkbox"/>	Domain Name	logincdn.msftauth.net
<input type="checkbox"/>	Domain Name	msauth.net
<input type="checkbox"/>	Domain Name	aadcdn.microsoftonline-p.com
<input type="checkbox"/>	Domain Name	microsoftonline-p.com
<input type="checkbox"/>	Domain Name	login.microsoftonline.com
<input type="checkbox"/>	Domain Name	login.live.com
<input type="checkbox"/>	Domain Name	autologon.microsoftazuread-ss0.com
<input type="checkbox"/>	Domain Name	graph.microsoft.com
<input type="checkbox"/>	Domain Name	login.microsoft.com
<input type="checkbox"/>	Domain Name	sts.windows.net
<input type="checkbox"/>	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

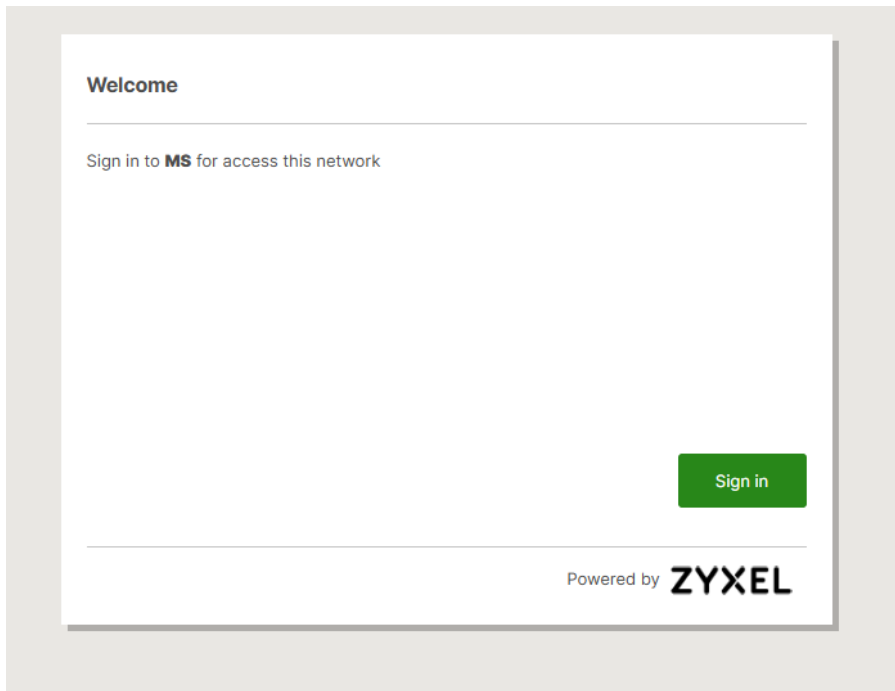
External

URL

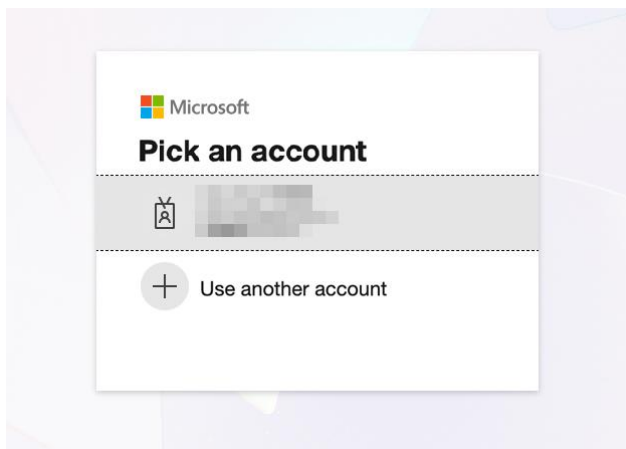
## Verification- Test User Login

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

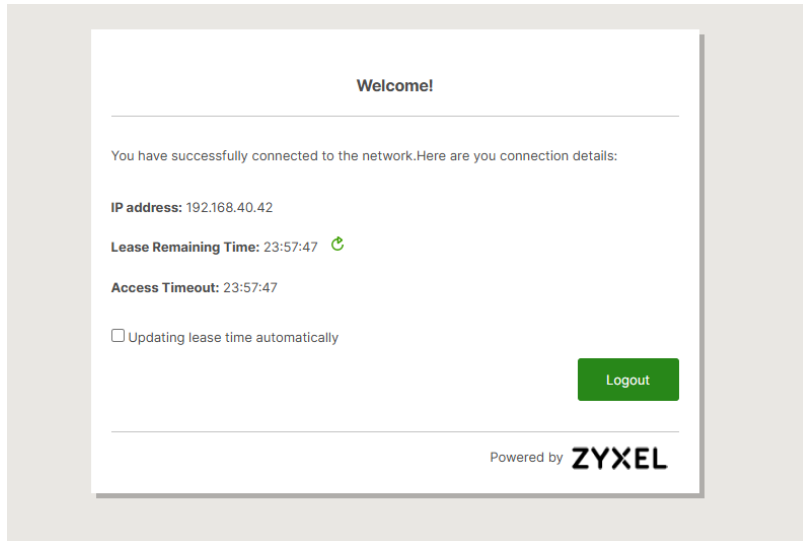
6. Connect a client device
7. Open a browser, display the Captive Portal page, and then click Sign in



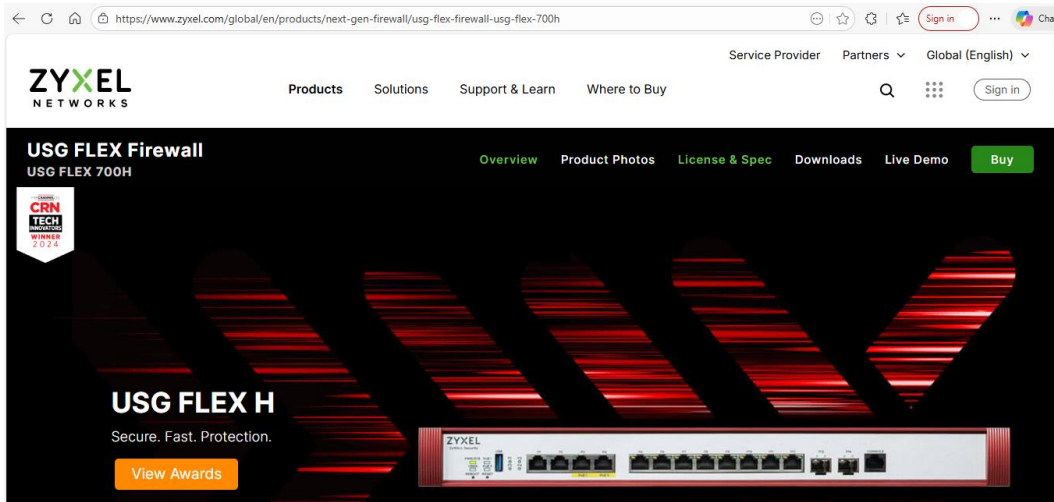
8. Confirm redirect to Microsoft login



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

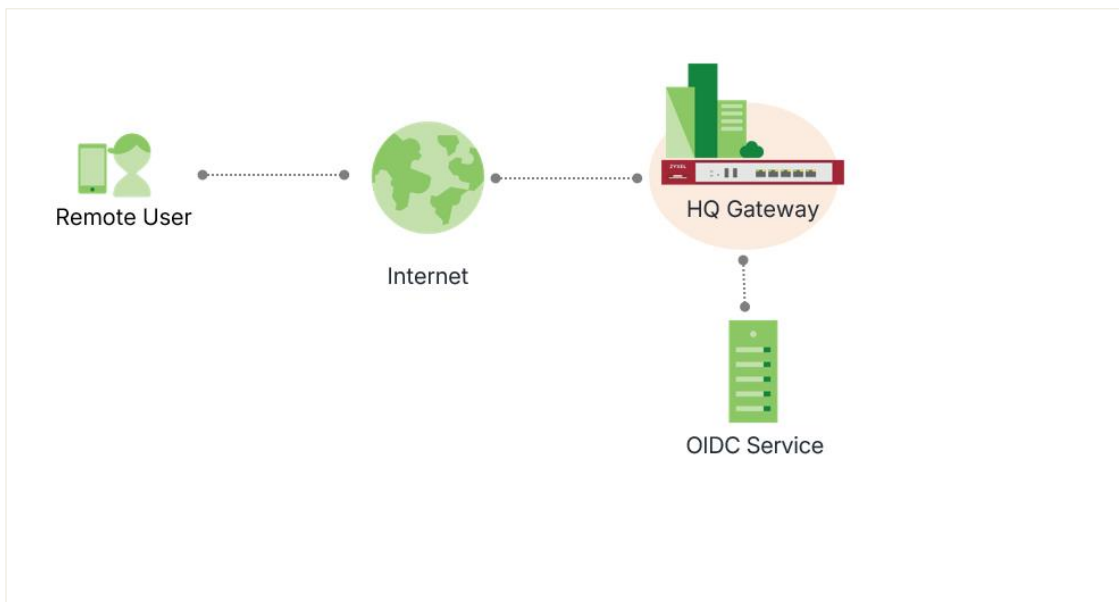
Network Status > Login Users > Login Users

Force Log Out

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1	admin	admin	192.168.40.200	0:07:00	http/https	0.0.0.0	23:25:16	admin(admin)
2	admin	admin	192.168.40.200	0:00:04	http/https	0.0.0.0	23:25:16	admin(admin)
3	admin	admin	192.168.40.200	0:00:04	http/https	0.0.0.0	23:25:16	admin(admin)
4	admin	admin	192.168.40.200	1:00:04	http/https	0.0.0.0	1 day, 0:00:00	admin(admin)
5	ext-user(oidc-users)	user	192.168.40.200	0:00:07	captiva 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	captiva 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.



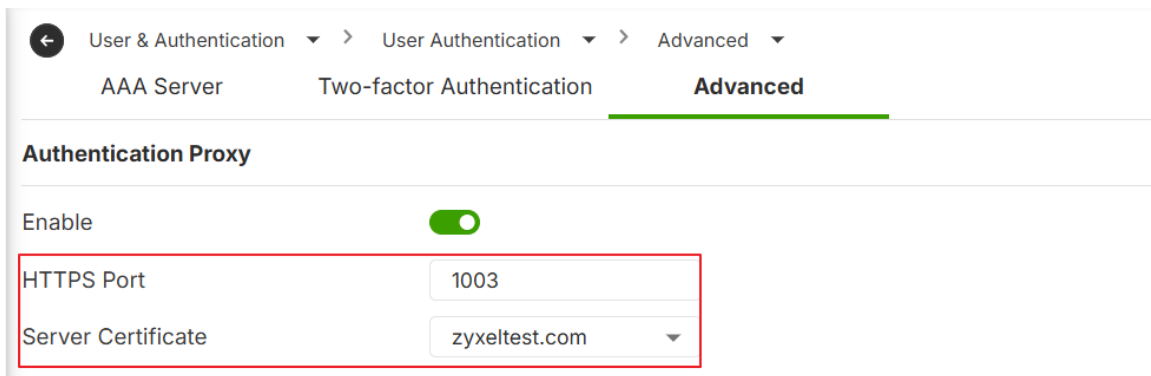
## Before You Begin

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.

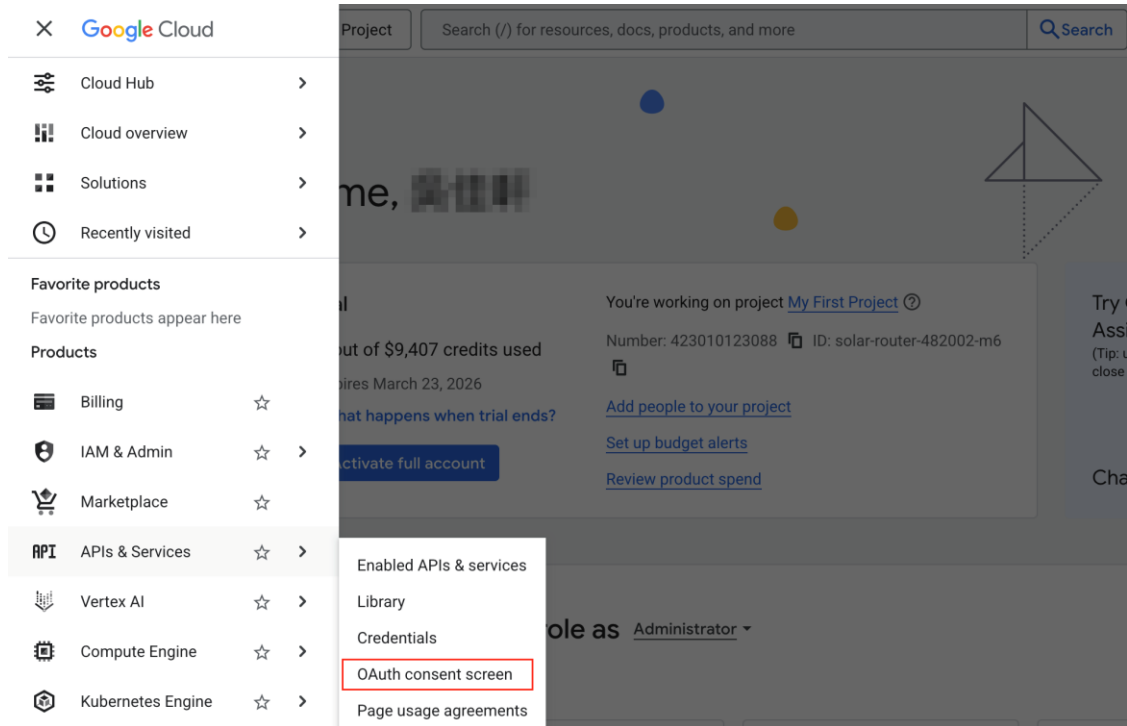


The screenshot shows the ZyWALL configuration interface for the Authentication Proxy section. The breadcrumb navigation is "User & Authentication > User Authentication > Advanced". The "Advanced" tab is selected. Under the "Authentication Proxy" heading, the "Enable" toggle is turned on. Below this, there are two input fields: "HTTPS Port" with the value "1003" and "Server Certificate" with the value "zyxeltest.com". A red rectangular box highlights these two fields.

 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 | Project configuration

Branding  
Audience  
Clients  
Data Access  
Verification Center  
Settings

### 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

Project configuration

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

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.

4. Enter Contact Information and Create

The image displays two sequential screenshots of the Zyxel Project configuration interface. Both screenshots feature a left-hand navigation menu with the following items: Overview (selected), Branding, Audience, Clients, Data Access, Verification Center, and Settings. The main content area is titled 'Project configuration'.

**Top Screenshot:** The 'Contact Information' step (3) is active. It includes a checkbox for 'App Information', 'Audience', and 'Contact Information'. A text input field labeled 'Email addresses \*' contains the email address '1@gmail.com'. Below the field, a note states: 'These email addresses are for Google to notify you about any changes to your project.' A 'Next' button is visible below the note.

**Bottom Screenshot:** The 'Finish' step (4) is now highlighted with a blue border. The 'App Information', 'Audience', and 'Contact Information' steps are marked as completed with checkmarks. 'Finish' is also marked with a checkmark. 'Create' and 'Cancel' buttons are located at the bottom of the configuration area.

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

Overview

OAuth Overview

Metrics

You haven't configured any OAuth clients for this project yet. [Create OAuth client](#)

Project Checkup

No project health recommendations found for your project. [Learn more about OAuth 2.0 Policies](#)

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

Overview

Branding

Audience

**Clients**

Data Access

Verification Center

Settings

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type \*  
Web application

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.

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

## 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.

← Client ID for Web application
🗑️ Delete

---

**Name \***

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.

**i** 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**

<b>Client ID</b>	423010123088-6fmsdladvpodb721ajma0phofkdhmd.apps.googleusercontent.com
<b>Creation date</b>	December 22, 2025, 12:42:17 PM GMT+8
<b>Last used date</b>	December 21, 2025 (Note: this data could be delayed by a day or more.)

**i** 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](#)

<b>Client secret</b>	****vMu
<b>Creation date</b>	December 22, 2025, 12:42:17 PM GMT+8

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

Name \*   
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.

**i** 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 \*

[+ 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.)

**i** 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 **\*\*\*\*\*vMu**

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

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.

6. You should see "OIDC Authentication Successful."

## OIDC Authentication Test

### OIDC Authentication Successful (Verified)

**Username:** ██████@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

Secondary Server

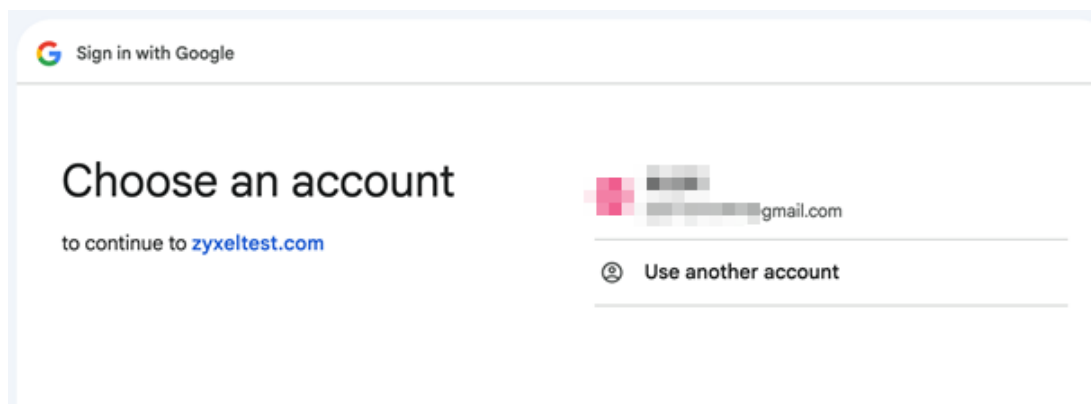
User  ⓘ

**Advanced Settings** ▾

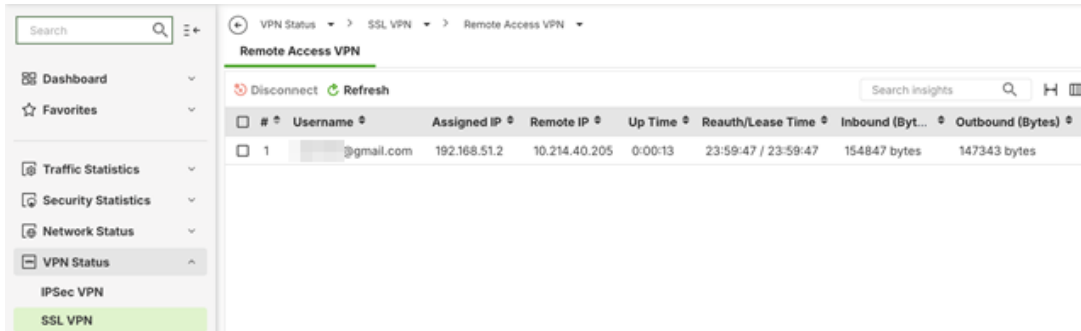
## Verification

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



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

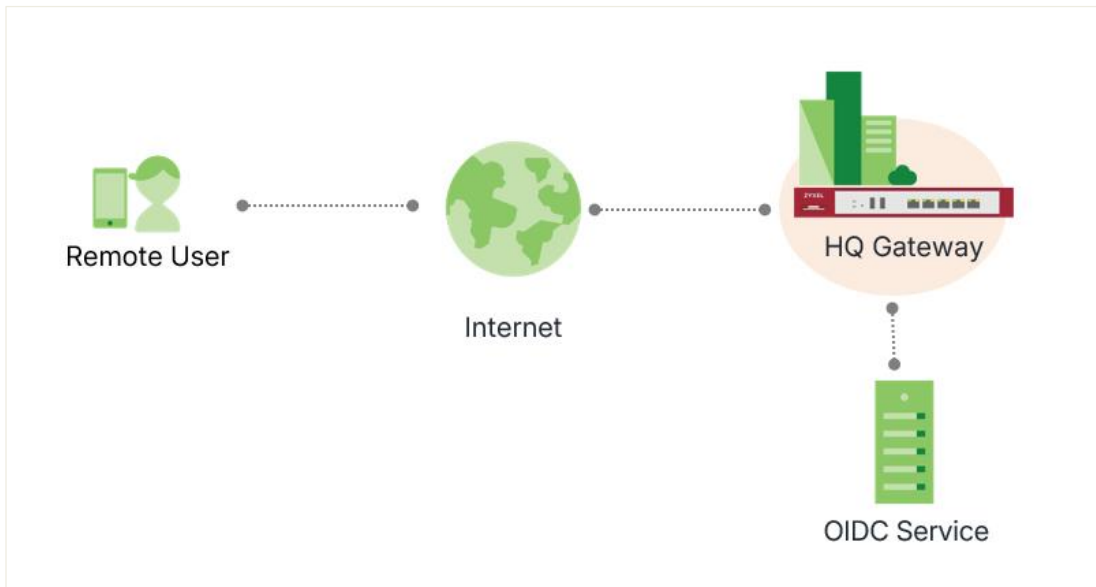


The screenshot shows the ZyXel management interface for Remote Access VPN. The breadcrumb navigation is VPN Status > SSL VPN > Remote Access VPN. The page title is Remote Access VPN. There are 'Disconnect' and 'Refresh' buttons. A search bar for insights is present. A table lists active VPN sessions with columns for ID, Username, Assigned IP, Remote IP, Up Time, Reauth/Lease Time, Inbound (Bytes), and Outbound (Bytes). One session is listed with ID 1, a username ending in @gmail.com, assigned IP 192.168.51.2, remote IP 10.214.40.205, up time 0:00:13, and reauth/lease times of 23:59:47 / 23:59:47. Inbound and outbound traffic are 154847 bytes and 147343 bytes respectively.

#	Username	Assigned IP	Remote IP	Up Time	Reauth/Lease Time	Inbound (Byt...	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

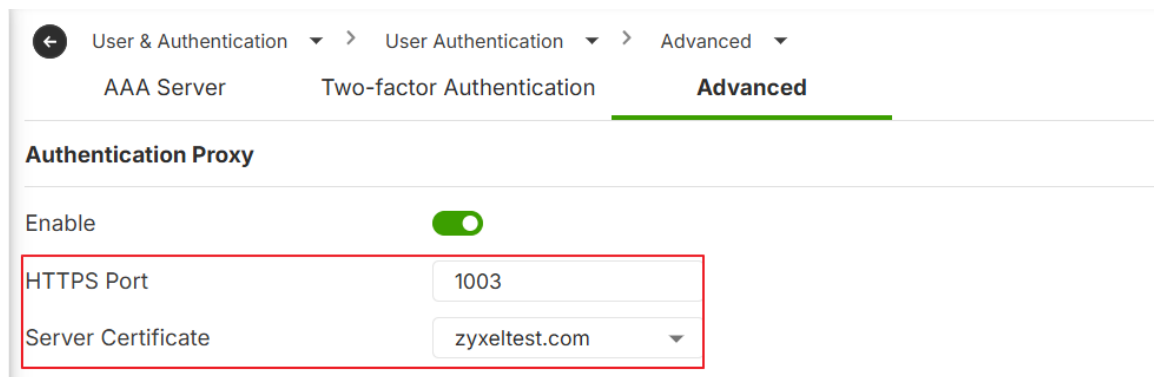
Before configuring the firewall, you must complete the required setup.

- 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.

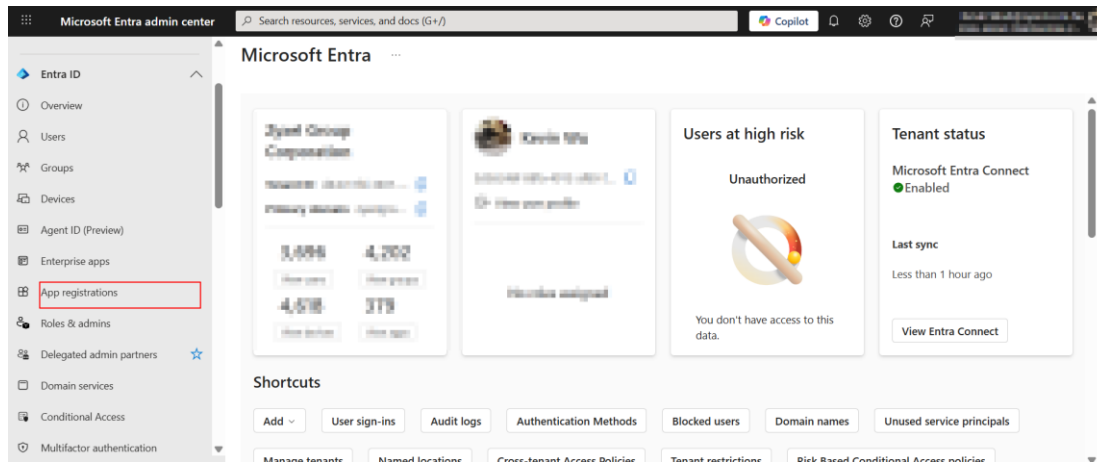


The screenshot shows the ZyWALL configuration interface for the Authentication Proxy feature. The breadcrumb navigation is "User & Authentication > User Authentication > Advanced". The "Advanced" tab is selected. Under the "Authentication Proxy" section, the "Enable" toggle is turned on. Below this, there are two input fields: "HTTPS Port" with the value "1003" and "Server Certificate" with the value "zyxeltest.com". A red rectangular box highlights these two fields.

 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

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
<a href="#">Microsoft Graph (5)</a>				

### 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
<a href="#">Microsoft Graph (5)</a>				
email	Delegated	View users' email address	No	<input checked="" type="checkbox"/> Granted for Zyxel Group... <a href="#">...</a>
offline_access	Delegated	Maintain access to data you have give...	No	<input checked="" type="checkbox"/> Granted for Zyxel Group... <a href="#">...</a>
openid	Delegated	Sign users in	No	<input checked="" type="checkbox"/> Granted for Zyxel Group... <a href="#">...</a>
profile	Delegated	View users' basic profile	No	<input checked="" type="checkbox"/> Granted for Zyxel Group... <a href="#">...</a>
User.Read	Delegated	Sign in and read user profile	No	<input checked="" type="checkbox"/> Granted for Zyxel Group... <a href="#">...</a>

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

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.			

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

Search << Got 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	Copy to clipboard	et ID
FLEXH	6/15/2026	[Redacted Value]	[Copy]	[ID]

 **Note: You must copy the secret immediately** because Microsoft Entra Portal hides the secret once the page reloads.

## Create OIDC AAA Server

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

OIDC Server ⓘ

+ Add Edit Remove Reference

Search insights 🔍

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

The screenshot shows the 'SSLVPN-Auth' application configuration page in the Azure AD portal. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (Branding & properties, Authentication (Preview), Certificates & secrets, Token configuration, API permissions), and a search bar. The main content area is titled 'Essentials' and lists several application properties: Display name (SSLVPN-Auth), Application (client) ID (highlighted with a red box), Object ID (highlighted with a red box), Directory (tenant) ID (highlighted with a red box), 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), and Managed application in local directory (SSLVPN-Auth). A feedback banner at the top right asks for input on the Microsoft identity platform.


## 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:

Client ID:

Client Secret:

Redirect Address:  (IP or FQDN)

Redirect URI:  

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

^ Essentials

Display name <a href="#">SSLVPN-Auth</a>	Client credentials <a href="#">Add a certificate or secret</a>
Application (client) ID [REDACTED]	<b>Redirect URIs</b> <a href="#">Add a Redirect URI</a>
Object ID [REDACTED]	Application ID URI <a href="#">Add an Application ID URI</a>
Directory (tenant) ID [REDACTED]	Managed application in local directo <a href="#">SSLVPN-Auth</a>
Supported account types <a href="#">My organization only</a>	

## 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://zyxelttest.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://zyxelttest.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

Secondary Server

User  ⓘ


**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



Kevin.Sun@zyxel.com.tw





Use another account

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

Search

- Security Statistics
- Network Status
- VPN Status**
- IPSec VPN
- SSL VPN**
- Tailscale
- Wireless Status

VPN Status > SSL VPN > Remote Access VPN

**Remote Access VPN**

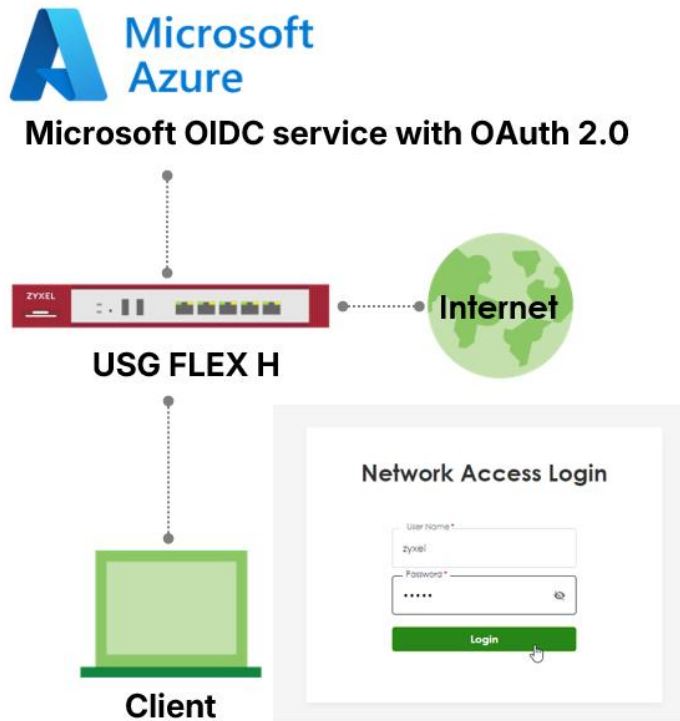
Disconnect Refresh

Search insights

#	Username	Assigned...	Remote IP	Up Time	Reauth/Lease Ti...	Inbound (Byt...	Outbound (Byt...
1	Kevin.Sun@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. On the left is a navigation pane with 'App registrations' selected. The main area shows the 'ExtGroup | Token configuration' page. Under 'Optional claims', there is a '+ Add optional claim' button and a '+ Add groups claim' button, which is highlighted with a red box. Below this is a table of existing claims.

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.

The screenshot shows the Zyxel management console interface. On the left is a navigation sidebar with categories like Home, Favorites, Entra ID, and App registrations. The main content area displays the 'ExtGroup | Token configuration' page. A modal dialog titled 'Edit groups claim' is open on the right. Inside the dialog, there is an information icon and text: 'Adding the groups claim applies to Access, ID, and SAML token types. Learn more'. Below this, a section titled 'Select group types to include in Access, ID, and SAML tokens.' contains three checkboxes: 'Security groups' (checked and highlighted with a red box), 'Directory roles', and 'All groups (includes 3 group types: security groups, directory roles, and distribution lists)'. There is also a note: 'Groups assigned to the application (recommended for large enterprise companies to avoid exceeding the limit on the number of groups a token can emit)'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

## 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".

The screenshot shows the configuration page for an AAA Server in the Zyxel management console. The breadcrumb navigation at the top reads 'User & Authentication > User Authentication > AAA Server'. The page is divided into several sections: 'Configuration' (Name: MS, Description: (Optional)), 'Server Settings' (Issuer URL, Client ID, Client Secret, Redirect Address, Redirect URI), and 'Advanced Settings' (Additional Scope: email, Login Name Attribute: email, Group Attribute: groups). The 'Group Attribute' field is highlighted with a red box. At the bottom, there is a 'Configuration Validation' section with a 'Test' button and a note: 'To validate the above settings, click Test button to login OIDC server at new tab.'



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

The screenshot shows the ZyXel management interface for 'User & Authentication'. The left sidebar has 'User & Authentication' highlighted. The main area shows 'Profile Management' for a user named 'CSO\_Security'. The 'User Type' is 'External Group User' and the 'Authentication Server' is 'MS / OIDC'. The 'Group Identifier' field is highlighted with a red box. Below, there are settings for 'Authentication Timeout Settings' (Use Default Settings selected), 'Lease Time' (1440 minutes), and '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.

The screenshot shows the ZyXel management interface for 'Captive Portal > Authentication Policy'. The 'Enable Walled Garden' toggle is turned on and highlighted with a red box. Below it, the 'Trusted Identity Provider' dropdown is set to 'Microsoft Entra ID' and is also highlighted with a red box. The 'Criteria' section shows 'Incoming' as 'LAN', 'Source Address' as 'any', and 'Destination Address' as 'any'. There is an 'Exempt List' table with columns for 'Type' and 'Object', currently showing 'Service' and 'DNS'.

Select Sign-in Method to OIDC server.

The screenshot shows the ZyXel Captive Portal configuration interface. On the left is a navigation menu with categories like Traffic Statistics, Security Statistics, Network Status, VPN Status, Wireless Status, Licensing, Network, VPN, Security Policy, Captive Portal, and Maintenance. The main area is titled 'Captive Portal > Authentication Policy'. Under 'Sign-in Method', there are three radio button options: 'Click-to-continue', 'Sign-on With', and 'Internal'. The 'Sign-on With' option is selected, and its dropdown menu is open, showing 'OIDC /MS' as the selected item. A red rectangular box highlights the 'Sign-on With' radio button and the 'OIDC /MS' dropdown selection. Below this, there are options for 'Portal Type' (Internal/External) and a 'URL' input field.

## Verification

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

Network Status > Login Users.

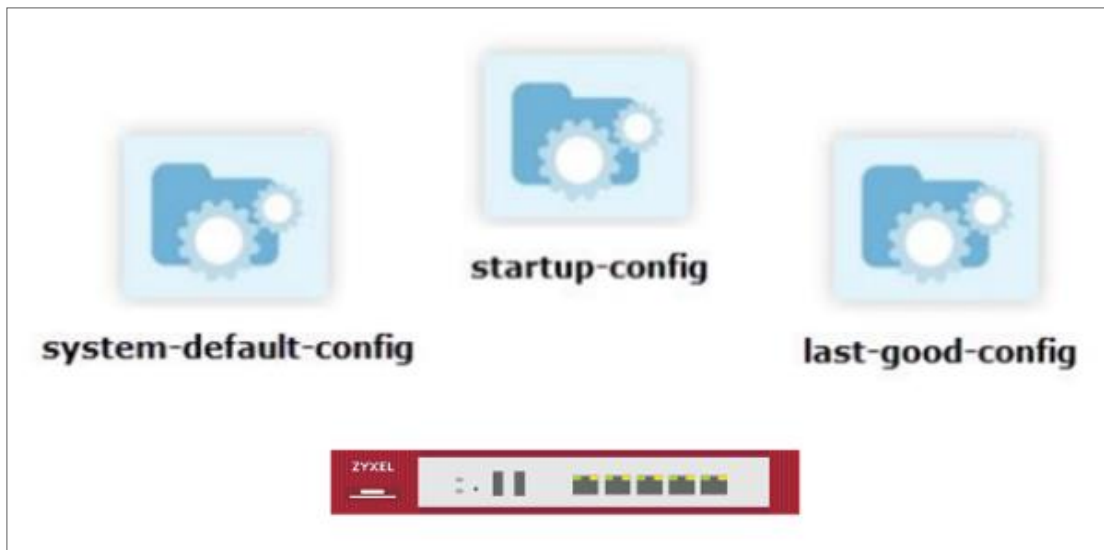
The screenshot shows the 'Login Users' page in the ZyXel management interface. It features a table with columns: #, User ID, Role, From, Login Time, Type, Tunnel IP, Lease Time, and User Info. There are two rows of data. The second row shows a user with the ID 'ext-group-user-ES0\_Security' in the User Info column, which is highlighted with a red box. The table also includes a 'Force Log Out' button and a search bar for 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-ES0_Security ext-user(oidc-users)

## 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.

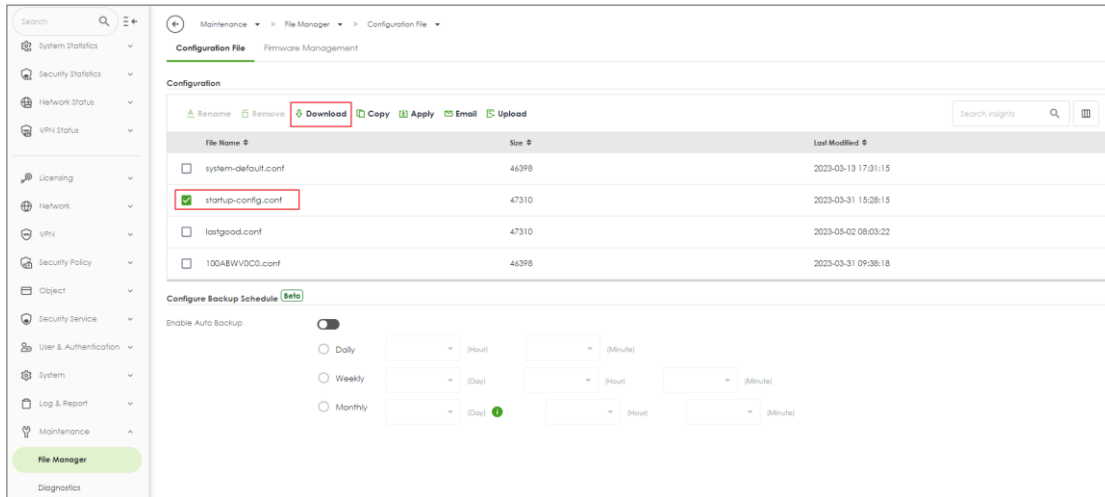
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

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".



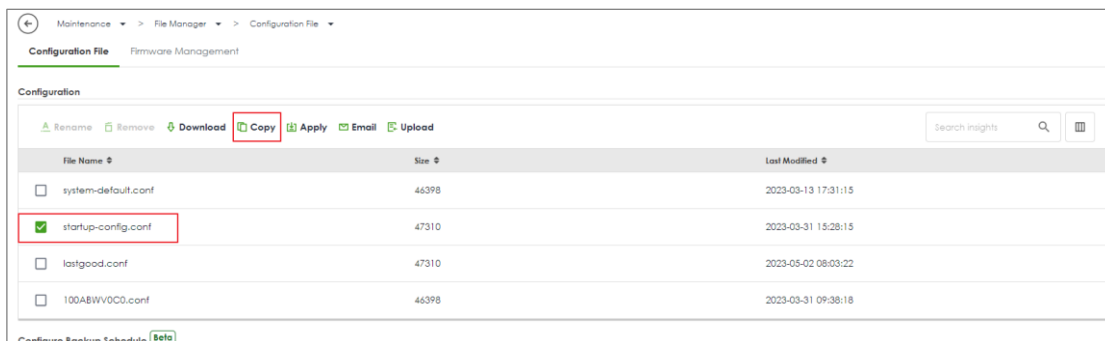
The screenshot shows the ZyXel File Manager interface. The breadcrumb path is Maintenance > File Manager > Configuration File. The page title is Configuration File. Below the title, there are action buttons: Rename, Remove, Download, Copy, Apply, Email, and Upload. The Download button is highlighted with a red box. Below the buttons is a table with columns File Name, Size, and Last Modified. The table contains four rows: system-default.conf, startup-config.conf, lastgood.conf, and 100ABWV0C0.conf. The startup-config.conf row is selected with a green checkmark and highlighted with a red box. Below the table is a section for Configure Backup Schedule (Beta) with radio buttons for Daily, Weekly, and Monthly, and dropdown menus for hours and minutes.

File Name	Size	Last Modified
system-default.conf	46398	2023-03-13 17:31:15
startup-config.conf	47310	2023-03-31 15:28:15
lastgood.conf	47310	2023-05-02 08:03:22
100ABWV0C0.conf	46398	2023-03-31 09:38:18

## Copy the Configuration Files

### Maintenance > File Manager > Configuration File

Select the file and click "Copy".

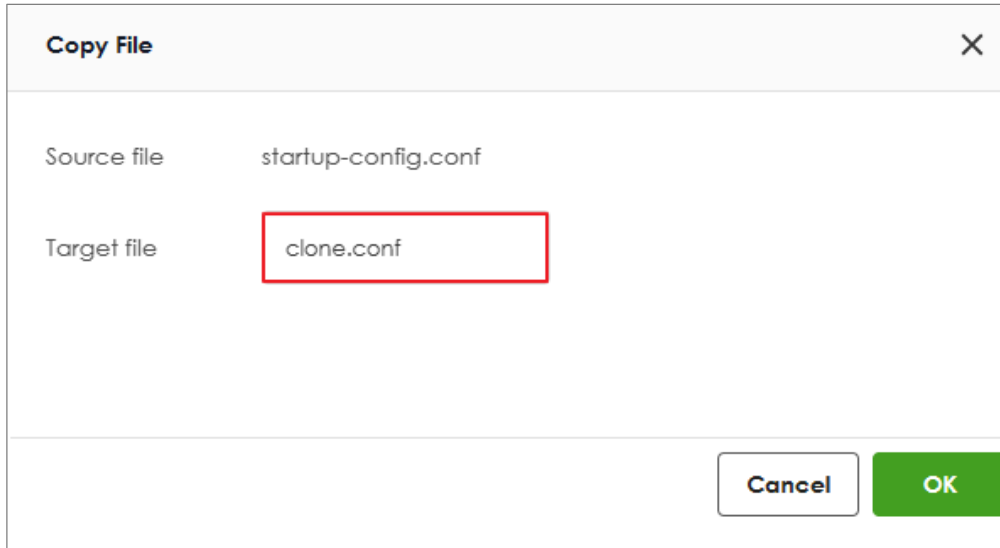


The screenshot shows the ZyXel File Manager interface. The breadcrumb path is Maintenance > File Manager > Configuration File. The page title is Configuration File. Below the title, there are action buttons: Rename, Remove, Download, Copy, Apply, Email, and Upload. The Copy button is highlighted with a red box. Below the buttons is a table with columns File Name, Size, and Last Modified. The table contains four rows: system-default.conf, startup-config.conf, lastgood.conf, and 100ABWV0C0.conf. The startup-config.conf row is selected with a green checkmark and highlighted with a red box. Below the table is a section for Configure Backup Schedule (Beta) with radio buttons for Daily, Weekly, and Monthly, and dropdown menus for hours and minutes.

File Name	Size	Last Modified
system-default.conf	46398	2023-03-13 17:31:15
startup-config.conf	47310	2023-03-31 15:28:15
lastgood.conf	47310	2023-05-02 08:03:22
100ABWV0C0.conf	46398	2023-03-31 09:38:18

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

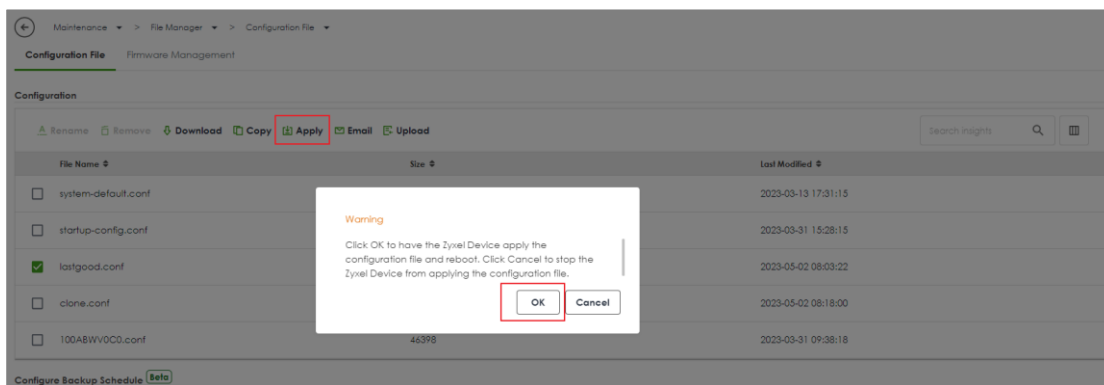
The file as format: [a-zA-Z0-9~\_.-]{1,63}.conf



## Apply the Configuration Files

### Maintenance > File Manager > Configuration File

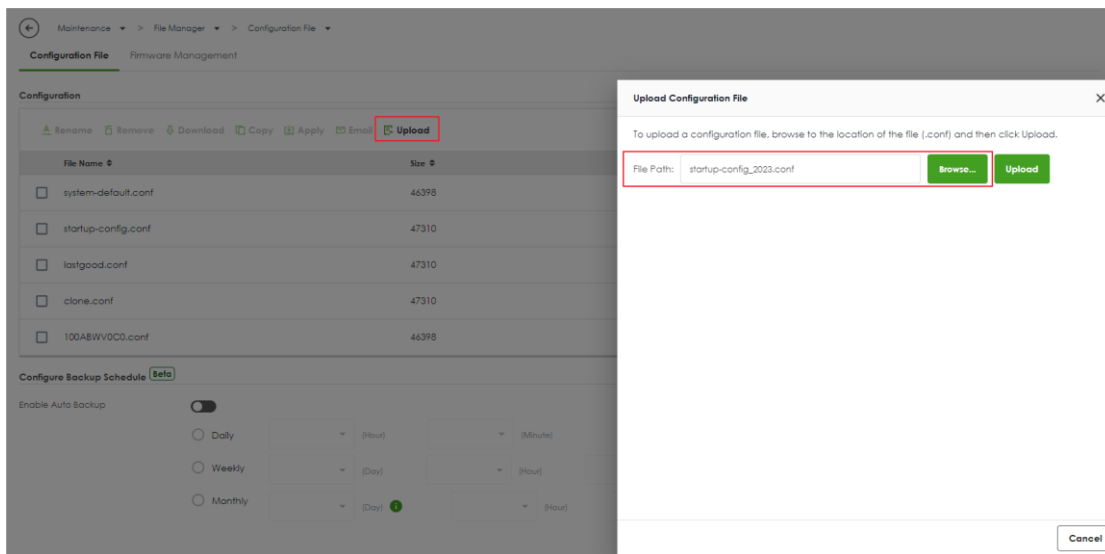
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when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

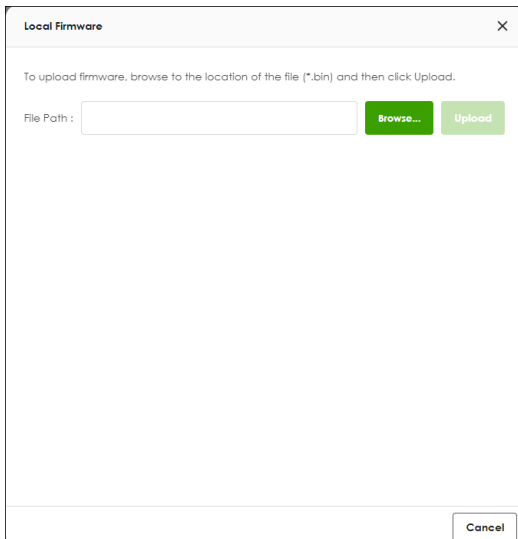
### Local Firmware Upgrade

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) portal.  
(<https://portal.myzyxel.com/my/firmwares>)



Status	Model	Version	Release Date	Action
Running	USG FLEX 200H	V1.10(A&WV.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.

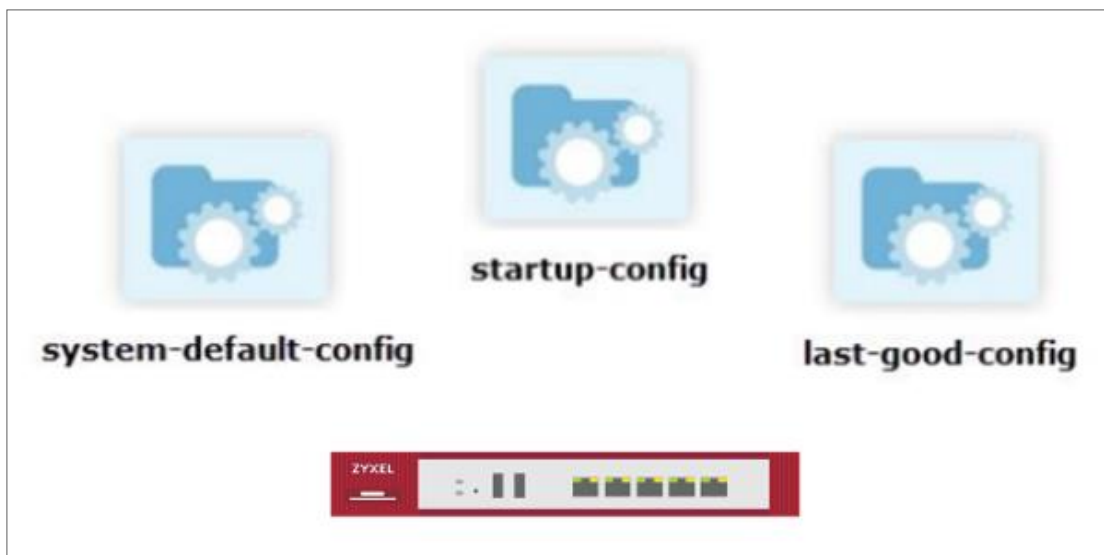
Furthermore, the "Auto Update" feature can be activated to automatically download firmware to your firewall first and reboot your device within a specified time frame.


**Cloud Firmware Information**

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

## How to set up configuration file backup rotation

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



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

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

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

Go to Configuration Backup Schedule section and enable "Enable Auto Backup".

Maintenance > Firmware/File Manager > Configuration File

**Configuration File** Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

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

**Configure Backup Schedule**

Enable Auto Backup

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

Backup Rotation 5 (1-50)

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

Maintenance > Firmware/File Manager > Configuration File

**Configuration File** Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

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

**Configure Backup Schedule**

Enable Auto Backup

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

Backup Rotation 5 (1-50)

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

Maintenance > Firmware/File Manager > Configuration File

**Configuration File** Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

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

Configure Backup Schedule

Enable Auto Backup

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

Backup Rotation 5 (1-50)

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

## Verification

### Maintenance > File Manager > Configuration File

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

Maintenance > Firmware/File Manager > Configuration File

**Configuration File** Firmware Management

Configuration

Rename Remove Download Copy Apply Email Upload Test

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

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

System							
APC							
AP							
Category System Clear Log Export Refresh 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:  [Outgoing SMTP Server Name or IP Address]

Port:  [1-65535]

TLS Security:

STARTTLS:

Authenticate Server:

SMTP Authentication:

User Name:

Password:

Retype:

**Mail Server Test**

Mail To:  [Email Address]

Send From:  [Email Address]

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

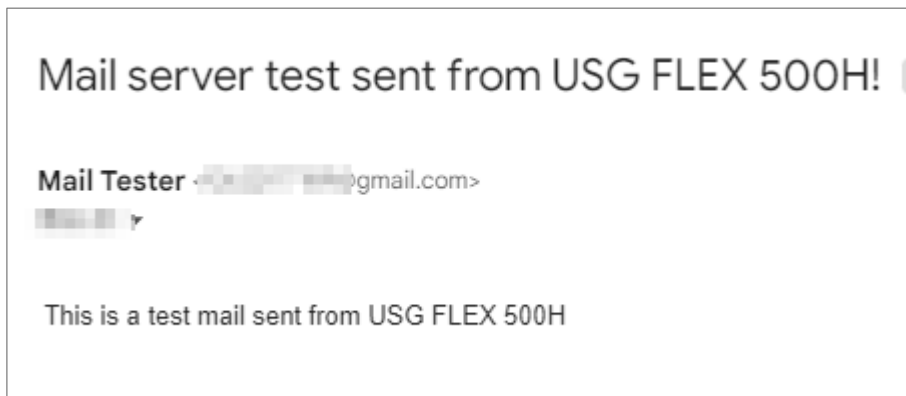
**Mail Server Test**

Mail To  (Email Address)

Send From  (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

Append system name  Append date time

Email from

Email to  (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  (Hour)  (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: [redacted]@gmail.com

Email to: [redacted]@gmail.com (Email Address)

[redacted] (Email Address)

[redacted] (Email Address)

[redacted] (Email Address)

[redacted] (Email Address)

**Send Report Now**

f [redacted]@gmail.com 下午3:34

ZYXEL NETWORKS

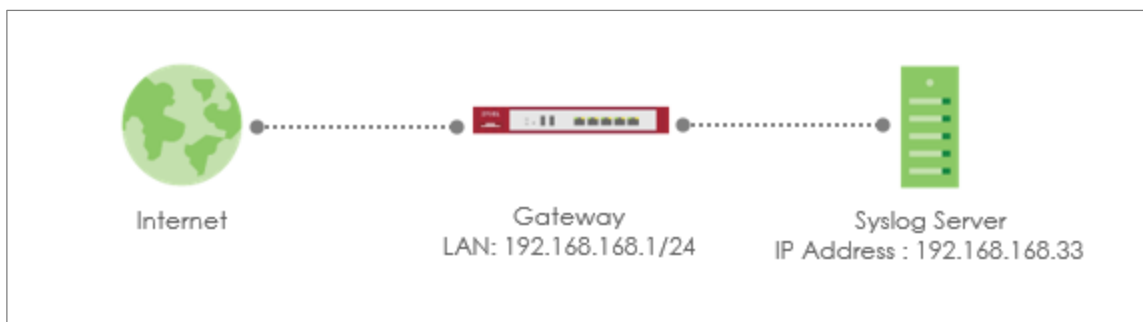
**General**


Model Name:	USG FLEX 500H
Firmware Version:	V1.10(A2H.0)07s1   2023-08-17 15:35:54
MAC Address Range:	[redacted]
System Uptime:	10 days, 22:37:53
System Name:	usgflex500h

**System Resource Usage**

## How to Setup and Send Logs to a Syslog Server

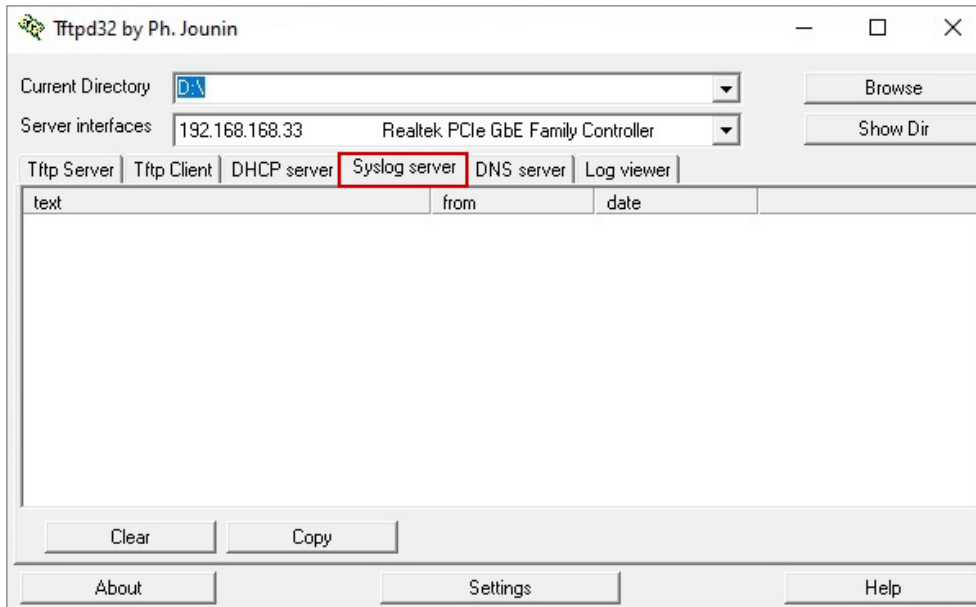
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system 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	System Log			USB Storage			Remote Server 1			Remote Server 2			Count
	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	
	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	158
> Authenticate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	9
> Security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	13
> Security Service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	6
> VPN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> License	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	130



## 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	
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	3
> Authenticate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	2
▼ Security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
Security Policy Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
DoS Prevention	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> Security Service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> VPN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
> License	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	0

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



**System Log**

Log Consolidation

Consolidation Interval  (10 Seconds - 600 Seconds)

**USB Storage**

Enable USB storage

Log Keep Duration

## Check the USG Log Files

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



System Log Archives in USB Storage

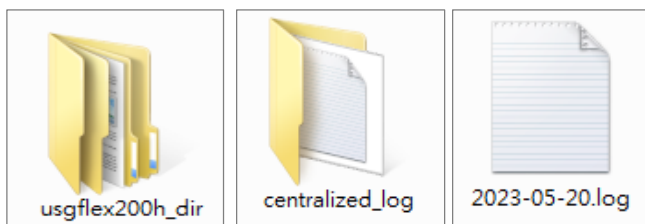
Remove  Download

<input checked="" type="checkbox"/>	File Name	Size	Modified Time
<input checked="" type="checkbox"/>	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

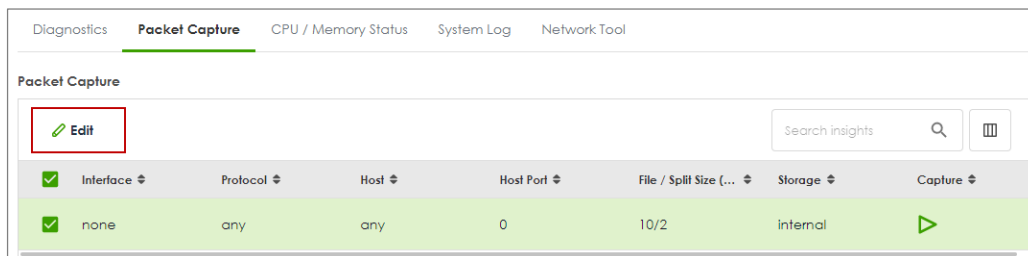
This example shows how to use the Packet Capture feature to capture network traffic going through the device's interfaces. Studying these packet captures may help you analyze network problems.



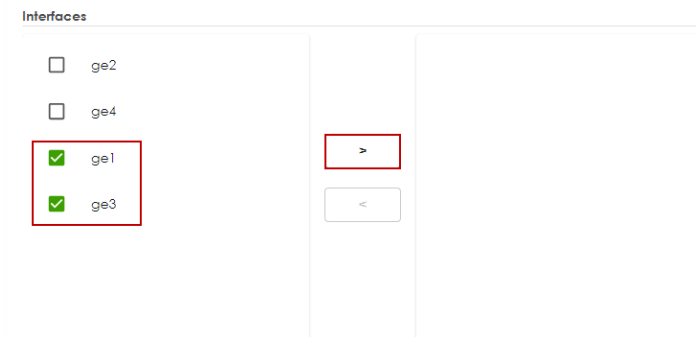
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

## 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.



- 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.

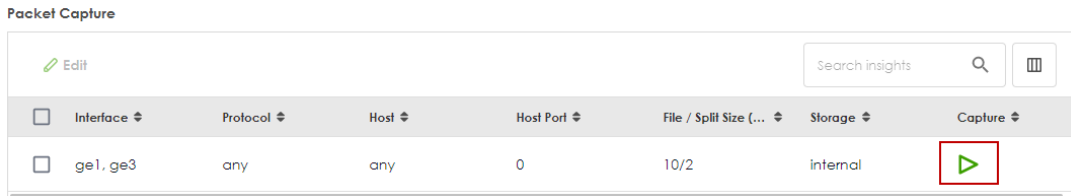
Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

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

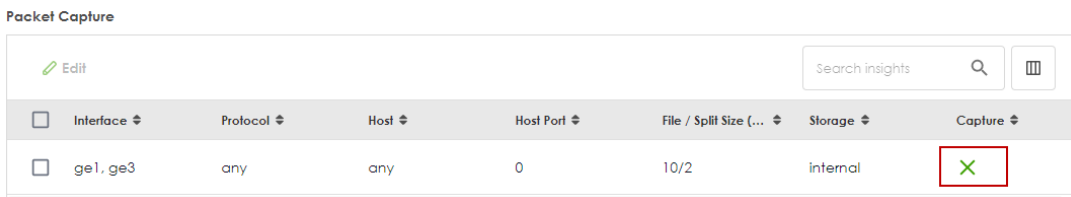
- In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".

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

9. Click the icon to start capturing packets.

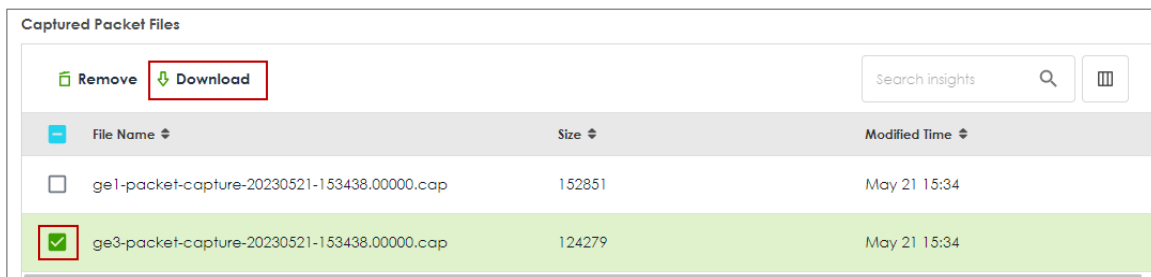


10. Click the icon to stop capturing packets.



## Download the Captured Packet Files

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



## Check Real-Time traffic using command

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

### Syntax:

cmd traffic-capture <interface name>

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

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

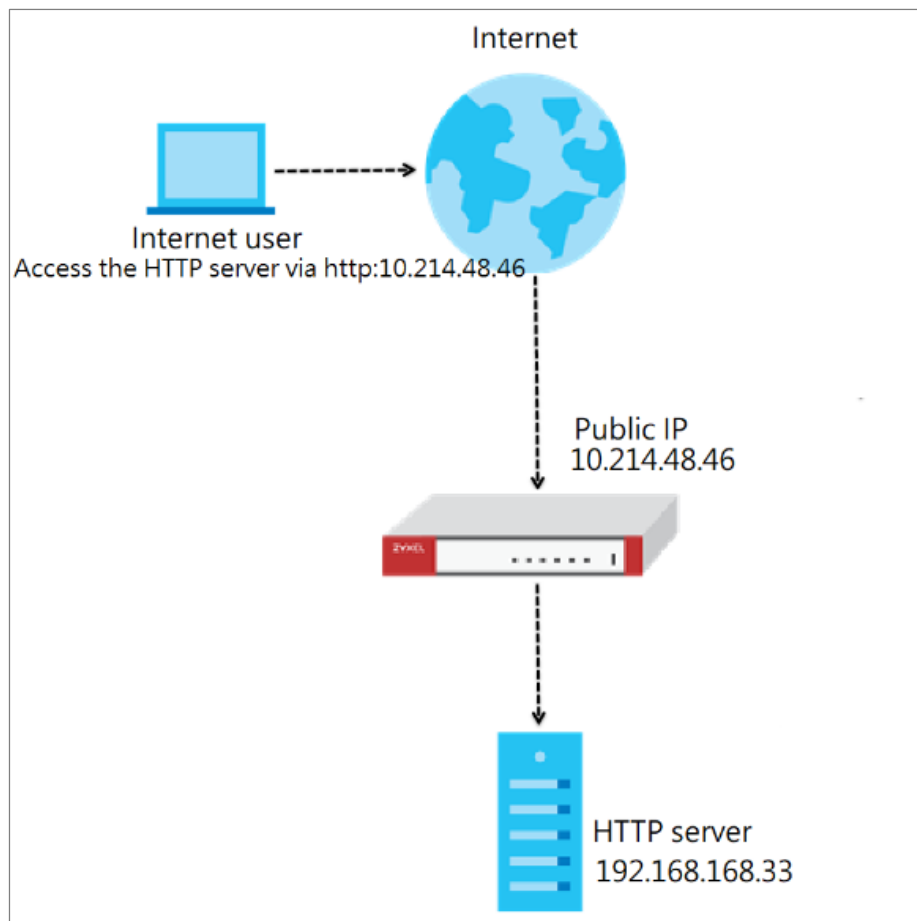
cmd traffic-capture <interface name> filter "port <port number>"

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

```
usgflex200h> cmd traffic-capture ge3 filter "src 192.168.168.33"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:07:36.738176 [REDACTED] > [REDACTED], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local.
(35)
16:07:36.738249 [REDACTED] > [REDACTED], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local.
(35)
16:07:36.739617 [REDACTED] > [REDACTED], ethertype IPv4 (0x0800),
length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.local.
(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.local.
(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

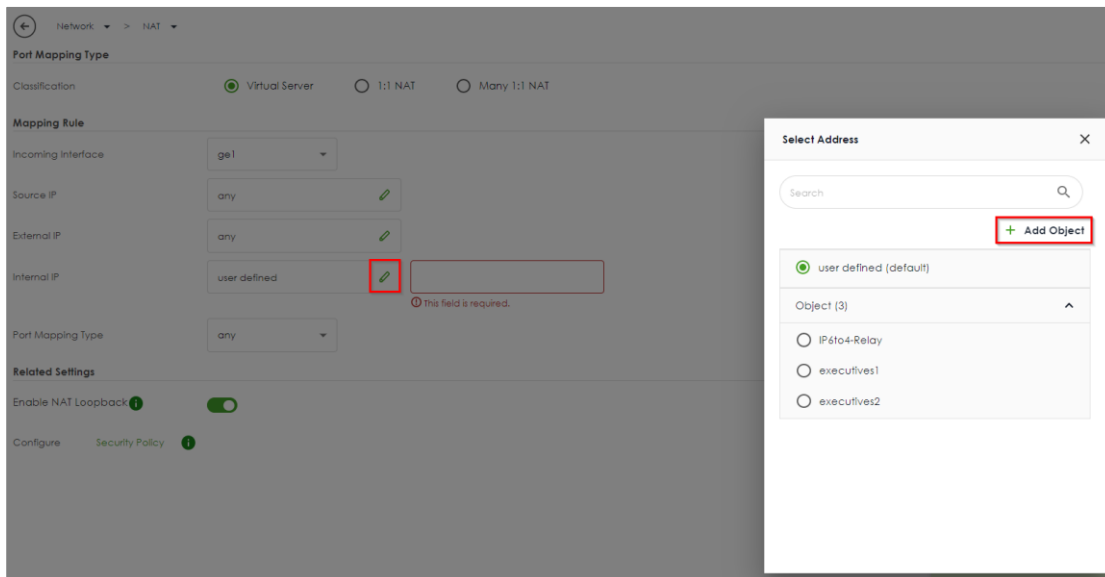
Here is an example of allowing access to the internal server behind a USG FLEX H device with network address translation (NAT). Internet users can access the server directly by its public IP address and a NAT rule will forward traffic from the internet to the local server in the intranet.



## 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.



- 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

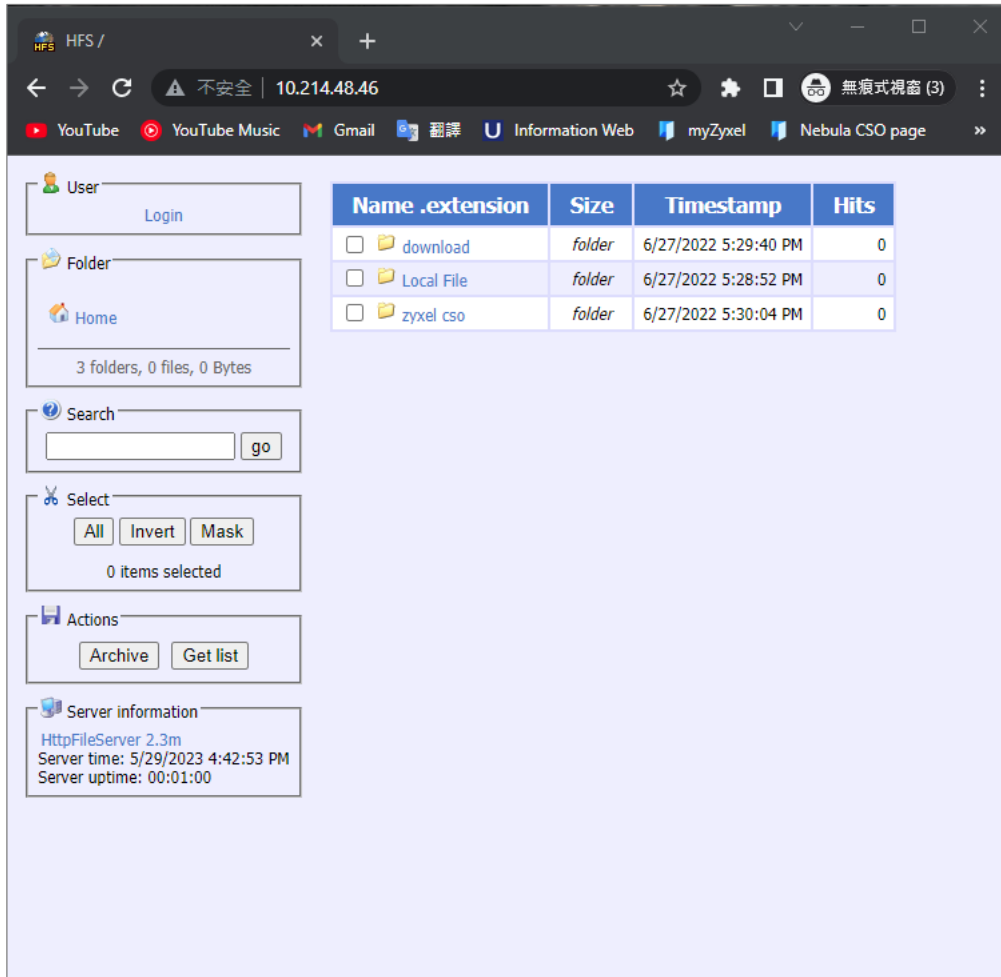
Port Mapping Type Service

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.



## How to Configure DHCP Option 60 – Vendor Class Identifier

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

### Set Up DHCP 60 on the USG FLEX H

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

The screenshot shows the configuration page for the WAN interface. The breadcrumb navigation is 'Network > Interface > External'. The 'General Settings' section shows 'Enable Interface' is turned on. The 'Interface Properties' section includes: Role (external), Interface Type (Ethernet), Interface Name (ge1), Port (p1 (ge1)), Zone (WAN), MAC Address (XXXXXXXXXX), and Description (empty). In the 'Address Assignment' section, three radio buttons are visible: 'Unassigned', 'Get Automatically (DHCP)' (which is selected and highlighted in yellow), 'Use Fixed IP Address', and '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: [Empty field]

Default SNAT:

## Test DHCP Option 60

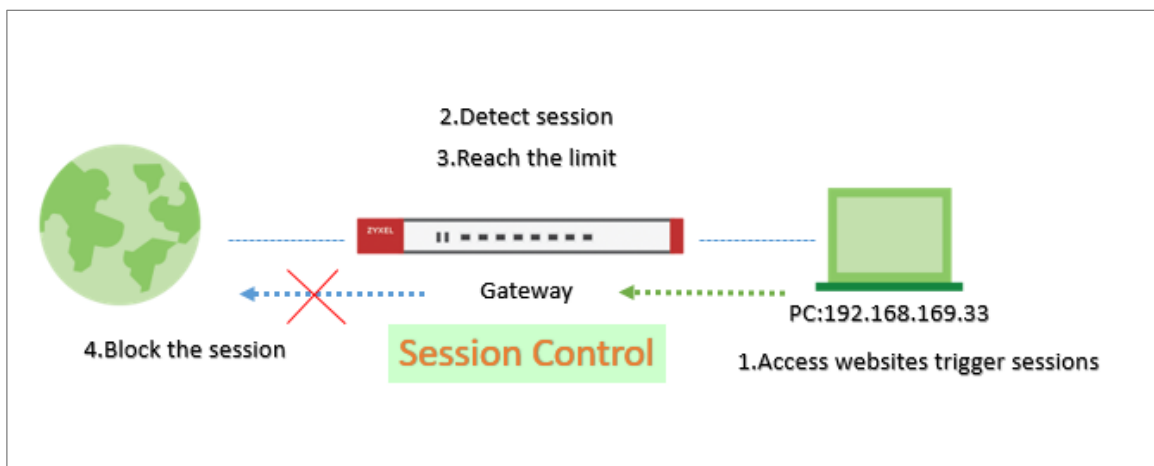
To check the functionality of DHCP Option 60, we can use packet capture software to check if option 60 string exists in the DHCP discover message that is sent from the USG FLEX H.

```

77 15.048707 0.0.0.0 255.255.255... 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
v 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
  v Option: (60) Vendor class identifier
    Length: 7
    Vendor class identifier: CSO-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
  Padding: 0000000000
  
```

## How to Configure Session Control

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



## Set Up the Session Control

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

← Security Policy > Session Control

**General Settings**

Session Control

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

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

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

Configuration

+ Add Edit Remove Active Inactive Move to Search Insights

Status	Priority	User	Source Address	Description	Limit

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

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

← Security Policy > Session Control

**General Settings**

Enable

Description

User

Source Address

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

Configuration

+ Add Edit Remove Active Inactive Move to Search Insights

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

## Test the Result

Log in as User: Zyxel

**ZYXEL**  
NETWORKS

**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**

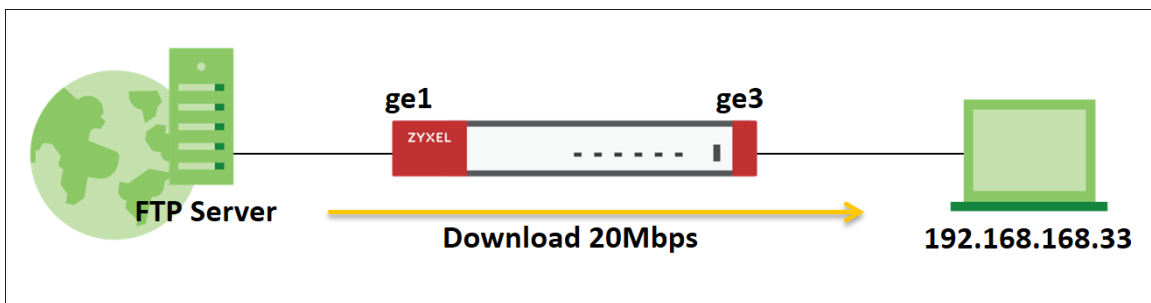
Try to access web browser to hit the session limit


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

Outgoing Interface

Source

Destination

Service Type  Service Object  Application Group

Service Object

User

Schedule

**Traffic Shaping**

Download Limit  Unlimited  Limit  Mbps

Upload Limit  Unlimited  Limit  Mbps

Priority

**Related Setting**

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

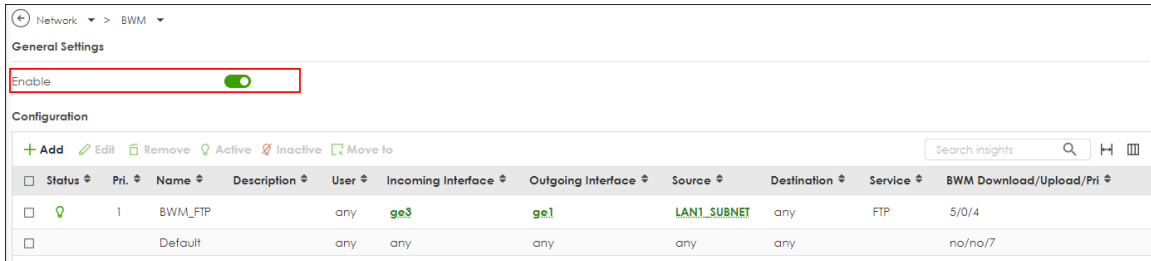
If you select the "Per-Source-IP" setting in the BWM rule, each selected IP address will have a limited bandwidth.

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



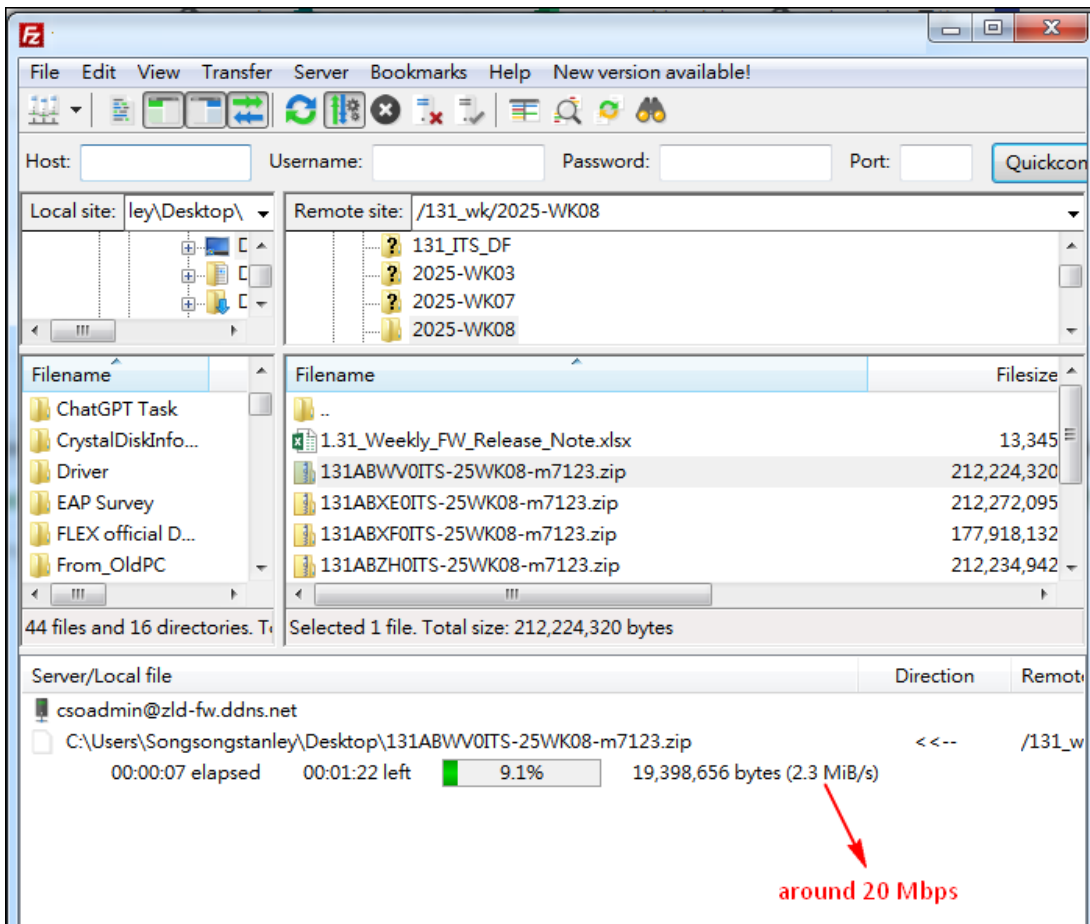
Note: If you select the "Per User" option or configure "User" as a condition, the Captive Portal service must be enabled, and the PC must be authenticated by the firewall first.

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

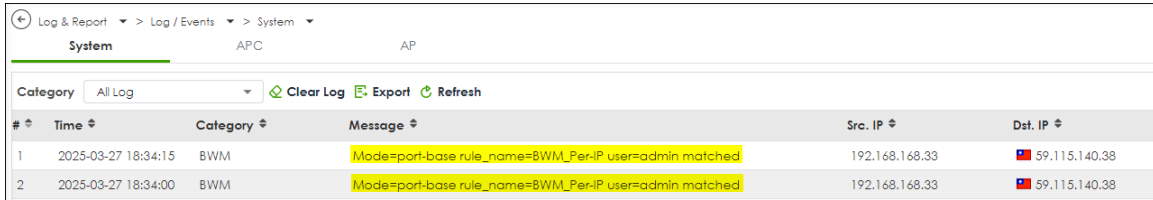


## Test the Result

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.

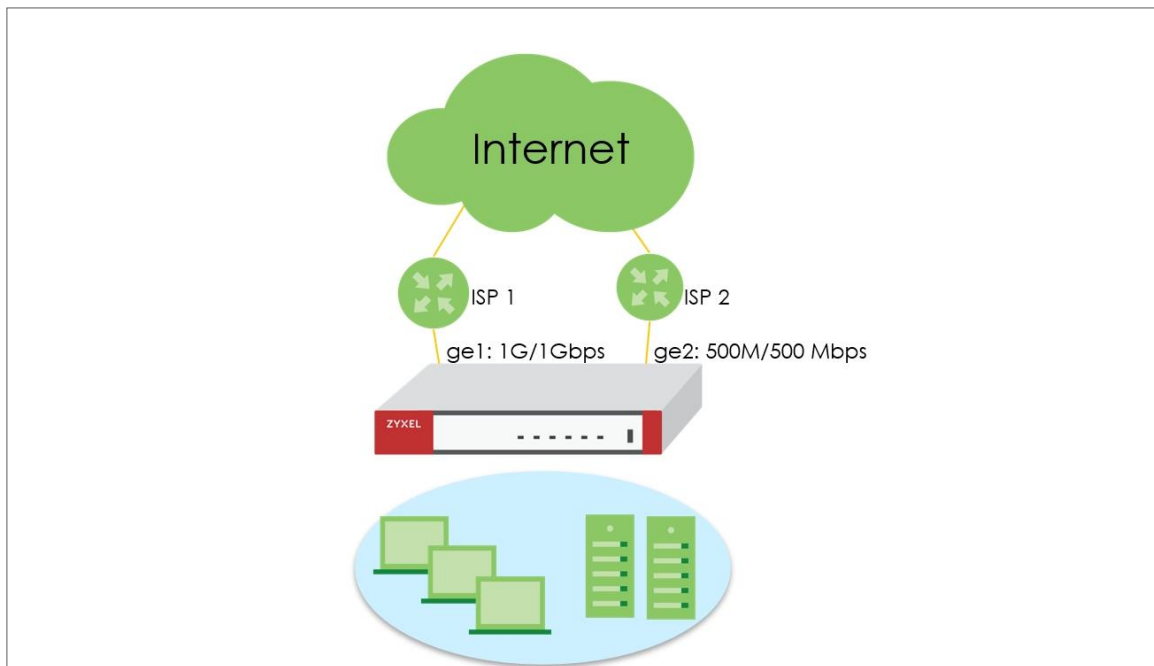


The screenshot shows the ZyXel Log & Report interface. The breadcrumb navigation is 'Log & Report > Log / Events > System'. The main heading is 'System', with sub-headings 'APC' and 'AP'. Below the heading, there is a 'Category' dropdown set to 'All Log', and buttons for 'Clear Log', 'Export', and 'Refresh'. The log table has columns for '#', 'Time', 'Category', 'Message', 'Src. IP', and 'Dst. IP'. Two log entries are visible, both with the message 'Mode=port-base rule\_name=BWM\_Per-IP user=admin matched'.

#	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 2<sup>nd</sup> user-defined Trunk.

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

Algorithm: Spillover

Load Balancing Index: Outbound

Network > Interface > Trunk

**General Settings**

Name: Spillover

**Load Balancing Setting**

Algorithm: Spillover

Load Balancing Index(es): Outbound

+ Add Remove

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

+ Add Remove

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

Click **Apply** to save changes.

**Some changes were made**

What do you want to do then?

Cancel Apply

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

Network > Interface > Trunk

Interface   **Trunk**   Port

**Default WAN Trunk**

Trunk Selection

Default Trunk

User-Defined Trunk LLF

**User-Defined Trunk**

+ Add   Edit   Remove   Reference   Search insights

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

**Default Trunk**

Edit   Search

Some changes were made  
What do you want to do then?  
Cancel   **Apply**

## Test the Result

### Spillover

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

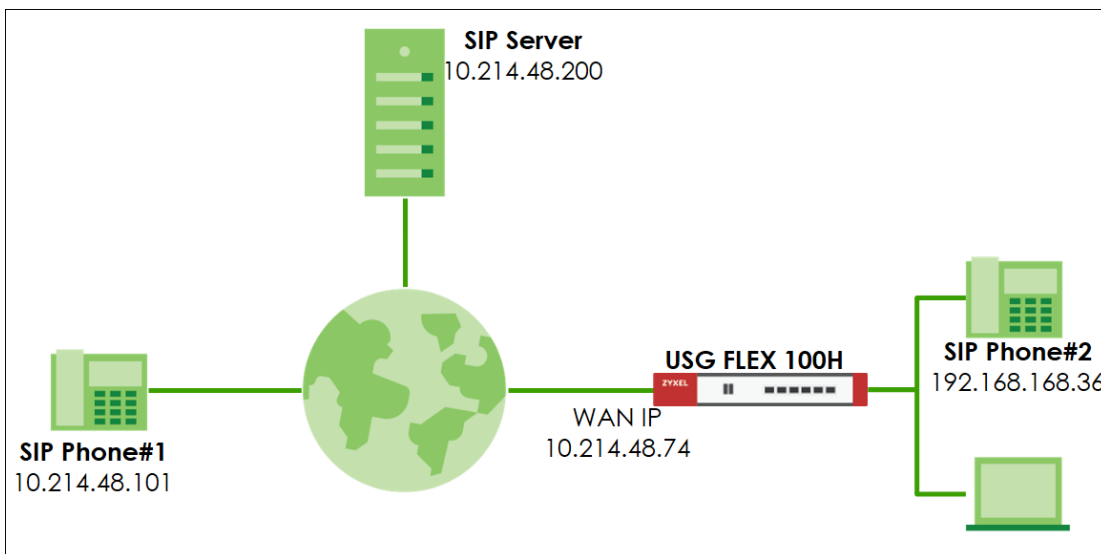
### Least Load First

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

## How Does SIP 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)

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)

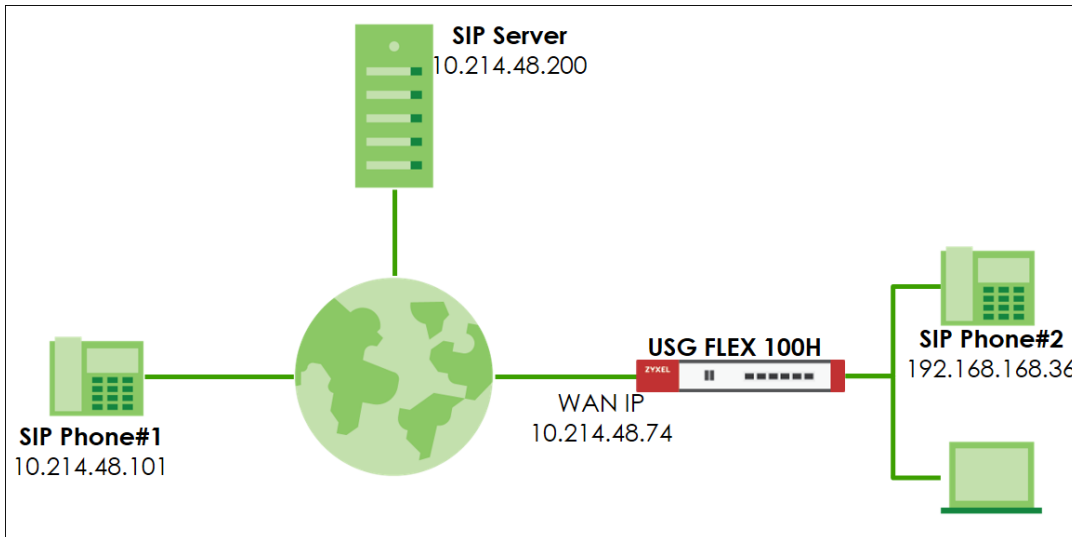
You can configure Media(RTP) and Signaling(SIP) timeout for your SIP phone, it could keep the sessions on firewall to prevent lost incoming phone call due to session expired.

**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 i**

Enable  ←

SIP Signaling Port

+ Add - Remove

Port ↓

5060

**SIP Inactivity Timeout**

Media Inactivity Timeout  seconds

Signaling Inactivity Timeout  seconds

Restrict Peer to Peer Media Connection  i

Restrict Peer to Peer Signaling Connection

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
RTP session

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

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

usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>

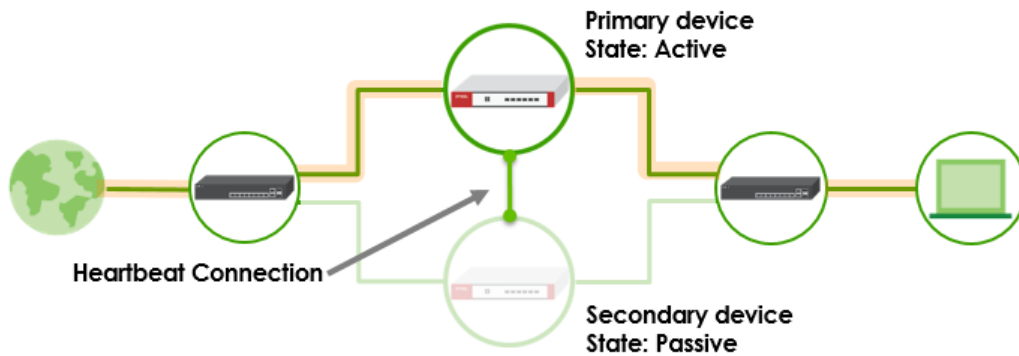
```


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

```
usgflex100h> show conntracks | match "192.168.168.36"
udp      17 2999 src=192.168.168.36 dst=10.214.48.200 sport=10002 dport=10254 packets=9513 bytes=1902600
src=10.214.48.200 dst=10.214.48.74 sport=10254 dport=10002 packets=18665 bytes=3733000 [ASSURED] mark=0 helper=RTP use=1
RTP Session
udp      17 2995 src=192.168.168.36 dst=10.214.48.200 sport=10003 dport=10255 packets=36 bytes=3312
src=10.214.48.200 dst=10.214.48.74 sport=10255 dport=1025 packets=73 bytes=6716 [ASSURED] mark=0 helper=RTP use=1
SIP Session
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>
```

## 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.

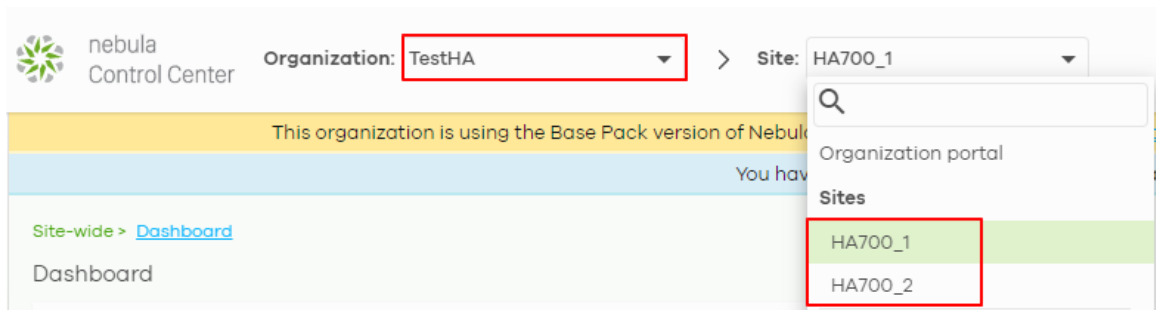


 Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.35).


## 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
<input type="checkbox"/>	ge1	WAN		10.214.48.99/255.255.255.0		Ethernet	p1	3
<input type="checkbox"/>	ge2	WAN		0.0.0.0/0.0.0.0		Ethernet	p2	1

Internal

+ Add Edit Remove Reference Active Inactive Search insights

Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input type="checkbox"/>	ge3	LAN		192.168.168.1/255.255.255.0		Ethernet	p3,p4,p5,p6	2
<input type="checkbox"/>	ge4	LAN		192.168.169.1/255.255.255.0		Ethernet	p7	2

3. Go to **System > Device HA > HA Configuration**.

- Select Primary role.
- Select HA MAC address.

If Virtual MAC Address is selected, the MAC address of each interface will be replaced as follows.

D8:EC:E5:XX:XX:1D -> D6:EC:E5:XX:XX:1D

- Configure Management IP for active and passive role. The two management IPs must be different but in the same subnet.
- Select monitor interfaces. HA failover will be triggered when monitored interface is down. Turn on **“Enable”** to enable Device HA and Apply.

HA Status	HA Configuration	HA Log
<b>General Settings</b>		
Enable	<input checked="" type="checkbox"/>	
<b>Management Configuration</b>		
Initial Role	<input checked="" type="radio"/> Primary (License Controller)	
HA MAC address		<input type="radio"/> Physical MAC address <input checked="" type="radio"/> Virtual MAC address
	<input type="radio"/> Secondary	
Active Node Management IP	<input type="text" value="10.10.10.1"/>	
Passive Node Management IP	<input type="text" value="10.10.10.2"/>	
Management IP Subnet Mask	<input type="text" value="255.255.255.0"/>	
<b>Monitor Interface</b>		
Member	<input type="text" value="ge3"/>	
Failover on Monitored Interface Link Down		<input checked="" type="checkbox"/>
Failover on Monitored Connectivity Check Failure		<input type="checkbox"/>

## Configuration on the secondary device

1. Make sure the secondary device is reset to default settings. Follow the wizard to register it to Nebula and it to the same organization as the primary device.
2. After the secondary device is registered to Nebula successfully, remove wan connection from the secondary device and login to the device via lan interface to configure HA.
3. Make sure the heartbeat port is not assigned to any interface. In this example, P8 is the heartbeat port on USG FLEX 200H. **Remove** P8 from interface ge4.


General Settings	
Enable Interface	<input checked="" type="checkbox"/>
Interface Properties	
Role	internal
Interface Type	Ethernet
Interface Name	ge4
Port	<input type="text" value="p7 ( ge4 )"/> <input checked="" type="checkbox"/> <input type="text" value="p8 ( ge4 )"/> <input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>	
Management Configuration		
Initial Role	<input type="radio"/> Primary (License Controller) <input checked="" type="radio"/> Secondary	
	HA MAC address	<input type="radio"/> Physical MAC address <input checked="" type="radio"/> Virtual MAC address
Active Node Management IP	<input type="text"/>	
Passive Node Management IP	<input type="text"/>	
Management IP Subnet Mask	<input type="text"/>	

## 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.

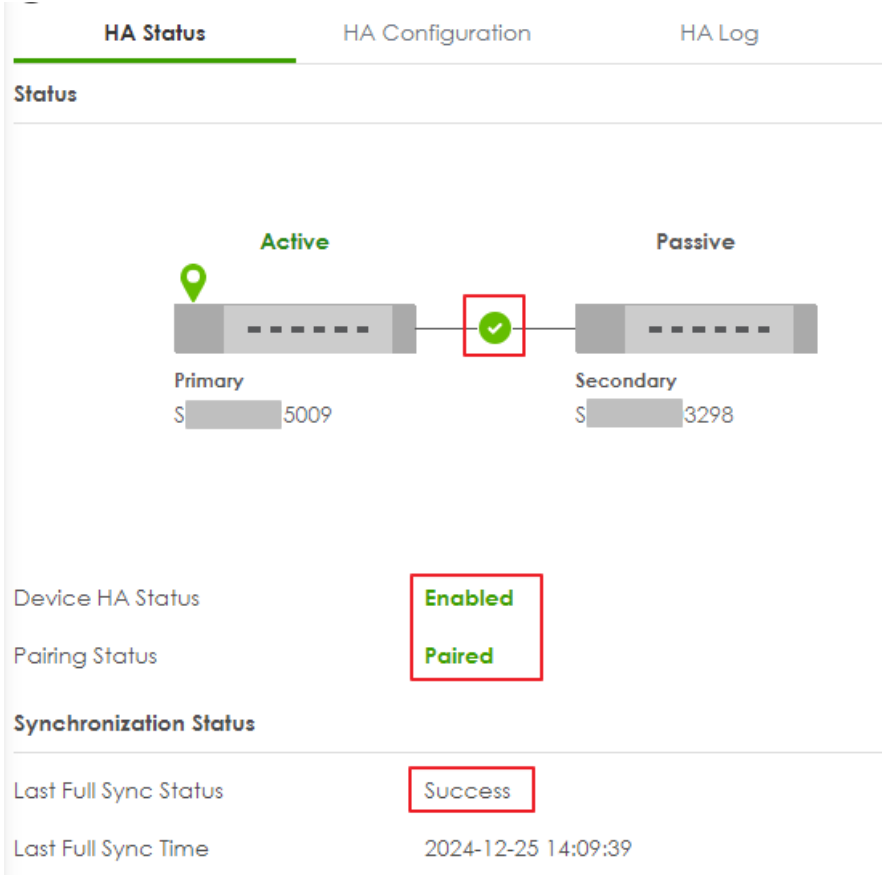
 Note: The heartbeat port of the primary and secondary device must be connected directly to each other (not through a switch).

## 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



The screenshot displays the HA Status page with the following details:

- Active Device:** Primary (Serial: S 5009)
- Passive Device:** Secondary (Serial: 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 Pairing Status is not "Paired", check what the error message is and resolve the error. In this example, the error is "Device firmware mismatch". Check the firmware version on primary and secondary again and make sure firmware version on both devices are identical.

System > Device HA > HA Status


HA Status | HA Configuration | HA Log

Status



Device HA Status: **Enabled**

Pairing Status: Device firmware or model mismatch detected

 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 Status | **HA Configuration** | HA Log

**General Settings**

Enable:


**Management Configuration**

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: gel 

Fallover on Monitored Interface Link Down:

Fallover on Monitored Connectivity Check Failure:

## HA Synchronization

- Full Synchronization: Full Sync will be performed under the following conditions. You can also use [SYS LED](#) on the passive device to check the status of HA synchronization.
  - After device reboot
  - After firmware update
  - After turning off Pause Device HA
  - After heartbeat connection is restored
  - After performing CLI on active device to manually force a full synchronization  
*usgflex200h> cmd device-ha force-sync full*
- Incremental Synchronization: This happens automatically when changes are made to the active firewall. The updates are synced to the passive firewall within 5 seconds. It is important to only make configuration changes on the active device.



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


## Connect the network cables to the secondary device

Once the devices have been properly synchronized, connect all network cables to wan and lan interfaces of the secondary devices.

## Test HA Failover

1. In this example, ge1 is the monitored interface. Unplug the Ethernet cable of ge1 interface from the primary device to trigger HA failover.

**Monitor Interface**

Member ge1 

Failover on Monitored Interface Link Down

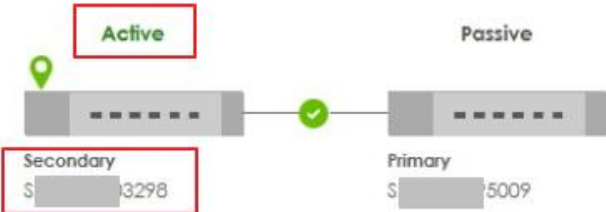
Failover on Monitored Connectivity Check Failure

2. Check HA Status and HA log by accessing Active Node Management IP <https://10.10.10.1>. In HA Status, the secondary device becomes Active role.

**Active Node**

System > Device HA > HA Status

HA Status | HA Configuration | HA Log



Device HA Status: **Enabled**

Pairing Status: **Paired**

**Synchronization Status**

Last Full Sync Status: Success

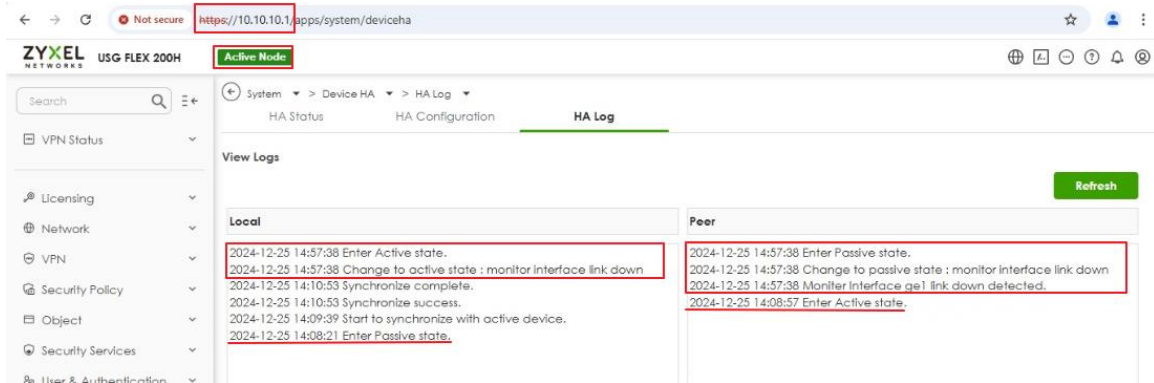
Last Full Sync Time: 2024-12-25 14:10:53

**Failover Status**

Failover Reason: Monitor interface link down

Last Failover Time: 2024-12-25 14:57:38

In HA Log, the secondary device (Local) changes the state from Passive to Active.



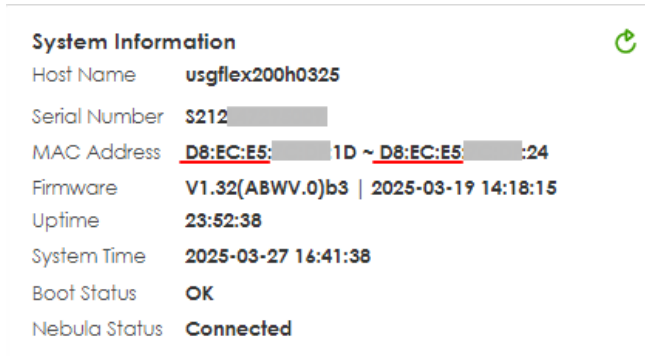
- To prevent excessive failover flapping, the firewall includes a mechanism. By default, the Device HA failover count limit is 5. When this failover count reaches limitation, failover will be stopped. The failover count automatically resets every 5 days. You can use the command to check the failover count.

***usgflex200h> show state vrf main device-ha summary***

## Check Virtual MAC Address

### Active Device

On Dashboard > System Information, MAC address is the physical MAC address.














In Network > Interface, it shows the Virtual MAC address.

Interface Properties	
Role	external
Interface Type	Ethernet
Interface Name	ge1
Port	p1 ( ge1 )
Zone	WAN
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <u>d6:ec:e5:</u> [redacted] 1d <input type="radio"/> Overwrite Default MAC Address auto1

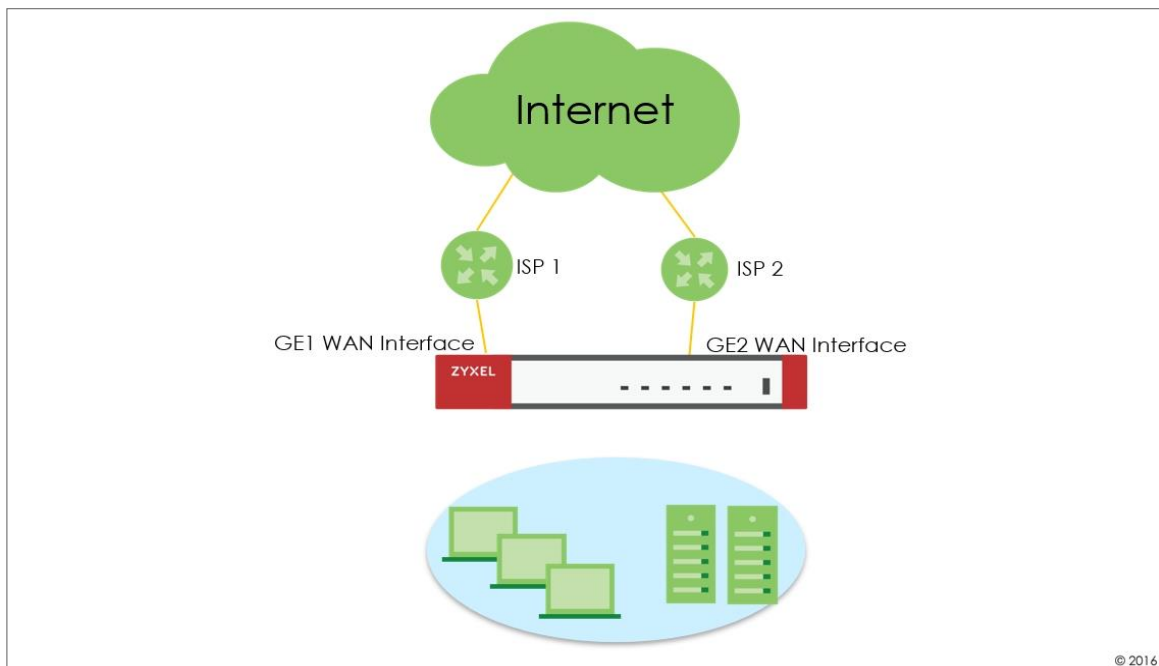
Interface Properties	
Role	internal
Interface Type	Ethernet
Interface Name	ge3
Port	p3 ( ge3 ) p4 ( ge3 ) p5 ( ge3 ) p6 ( ge3 )
Zone	LAN
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <u>d6:ec:e5:</u> [redacted] 1f <input type="radio"/> Overwrite Default MAC Address auto3


## SYS LED Status

State	SYS LED on Active Device	SYS LED on Passive Device
Pairing in Progress	Alternating Green on: 500ms, Red on: 500ms  	Green Solid 
Pairing fail	Red Blinking (1sec) 	Green Solid 
Sync. in Progress	Green Solid 	Amber Blinking (500ms) 
Sync. Completed	Green Solid 	Amber Solid 
Active Node Running	Green Solid 	Amber Solid 

## How to check Packet Flow Explorer

The Packet Flow Explorer is a powerful tool for analyzing and understanding routing-related issues. When used correctly, it offers a basic overview of your firewall's configuration without requiring an in-depth examination. This example demonstrates how to check the routing and SNAT status using the Packet Flow Explorer.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.31).

## Scenario and Requirement

1. Dual WAN interfaces are in the default WRR mode, and both WANs are active.

Name	Default										
<b>Load Balancing Setting</b>											
Algorithm	wrr										
<table border="1"> <thead> <tr> <th>Interface</th> <th>Mode</th> <th>Parameter</th> </tr> </thead> <tbody> <tr> <td>ge1</td> <td>Active</td> <td>1</td> </tr> <tr> <td>ge2</td> <td>Active</td> <td>1</td> </tr> </tbody> </table>			Interface	Mode	Parameter	ge1	Active	1	ge2	Active	1
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		<b>Static Route</b>			
<b>Configuration</b>					
<span>+ Add</span> <span>Edit</span> <span>Remove</span> <span>Refresh</span>					
<input type="text" value="Search insights"/>					
Status	Name	Destination	Next Hop	Description	Metric
<input type="checkbox"/>	Google_DNS	8.8.8.8/32	ge2		0

3. A policy route is configured to route all internet traffic through the GE1 WAN interface when source is LAN1 subnet.

Policy Route		Static Route											
<b>Configuration</b>													
<span>+ Add</span> <span>Edit</span> <span>Remove</span> <span>Active</span> <span>Inactive</span> <span>Move to</span> <span>Refresh</span>													
<input type="text" value="Search insights"/>													
Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits
<input type="checkbox"/>	1	any	none	ge3	LAN1_SUBNET	any	any	any	any	ge1	preserve	outgoing-interface	0

Based on the configuration above, we expect that if a host is placed in the LAN 1 subnet, all traffic will be routed through the GE1 WAN interface, except for traffic to 8.8.8.8, which will be routed through the GE2 WAN interface.

## Verification

1. Place a host in the LAN1 subnet, then run the command **ping 8.8.8.8 -t** in the Windows Command Prompt to check for ICMP response from 8.8.8.8.

```
C:\Users\NT122546>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=9ms TTL=57
Reply from 8.8.8.8: bytes=32 time=8ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=7ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
```

The host receives ICMP response.

2. Confirm that the traffic is being sent out through the GE2 WAN interface, as per the static route configuration.

Type the command **cmd traffic-capture ge2 filter "host 8.8.8.8"** to capture packets on the GE2 WAN interface and verify that the traffic is being sent out through the GE2 WAN interface.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
█
```

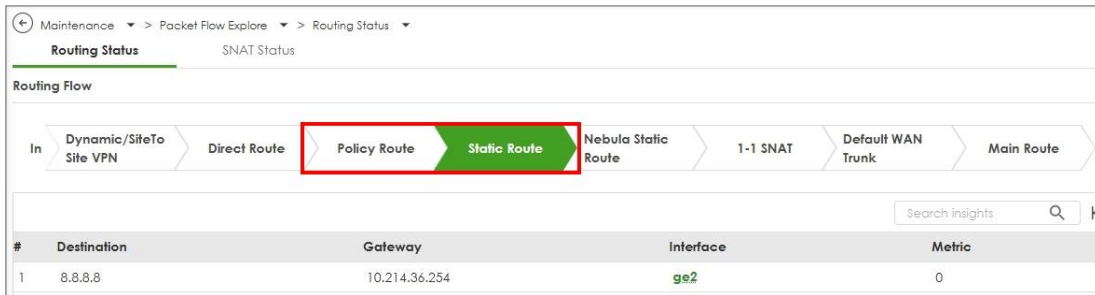
We're unable to see packets to 8.8.8.8. Let's capture the packets on the GE1 WAN interface instead.

**cmd traffic-capture ge1 filter "host 8.8.8.8"**

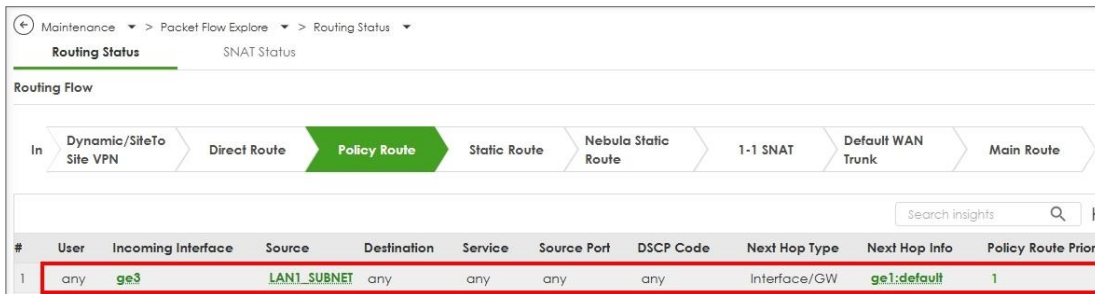
```
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:59:42.856370 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34317, length 74
09:59:42.862565 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34317, length 74
09:59:43.869372 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34318, length 74
09:59:43.874648 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34318, length 74
09:59:44.882064 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34319, length 74
09:59:44.886659 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34319, length 74
09:59:45.895564 d8:ec:e5:7c:df:dd > d2:ec:32:78:al:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34320, length 74
09:59:45.898654 d2:ec:32:78:al:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34320, length 74
```

Traffic to 8.8.8.8 is being sent out through the GE1 WAN interface, indicating that the static route is not working as expected.

3. Go to **"Maintenance > Packet Flow Explorer > Routing Status"** to check for possible issues.



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.



We can 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  i

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=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.

```
usgflcx200h> 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:a1:18, 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:a1:18 > 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:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26450, len
15:51:48.751877 d2:ec:30:78:a1:18 > 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:a1:18, 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:a1:18 > 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:a1:18, 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:a1:18 > 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:a1:18, 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:a1:18 > 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:  characters. The valid characters are [a-z][A-Z]+[0-9][a-z][A-Z][\_-].

Zone:


MAC Address:  address

Ethernet  
VLAN  
Bridge  
LAG

 Note:

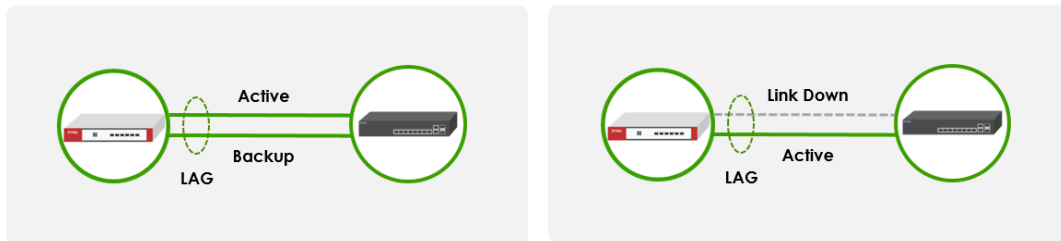
- LAG support interface Role: **External, Internal and General**
- When the interface role is external, the LAG IP address does not support PPPoE or PPPoE with a static IP

3. Select the LAG mode

Name	<input type="text" value="LAG-ge-5-6"/>
Zone	<input type="text" value="LAN"/>
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <input type="radio"/> Overwrite Default MAC Address <input type="text"/>
Description	<input type="text"/>
Address Assignment	<input type="radio"/> Unassigned <input checked="" type="radio"/> Use Fixed IP Address IP/Network Mask <input type="text" value="172.198.1.1/24"/>
Secondary IP	<div style="border: 1px solid #ccc; padding: 5px;"> <p><a href="#">+ Add</a> <a href="#">Remove</a></p> <p><input type="checkbox"/> IP/Netmask ↕</p> <p style="text-align: center;">No data</p> </div>
Members 	<input type="text" value="ge5 x ge6 x"/>
Mode	<input type="text" value="static"/> <input checked="" type="text" value="active-backup"/> (1-1000)ms <input type="text" value="lACP (802.3ad)"/>
Mii Monitoring Interval	
Primary	

## LAG mode: Active-Backup

Provides automatic link failover by keeping backup ports not transmitting traffic until the primary port experiences a link-down event.



**Mii Monitoring Interval:** Defines how frequently the system checks if a LAG member interface is active or down

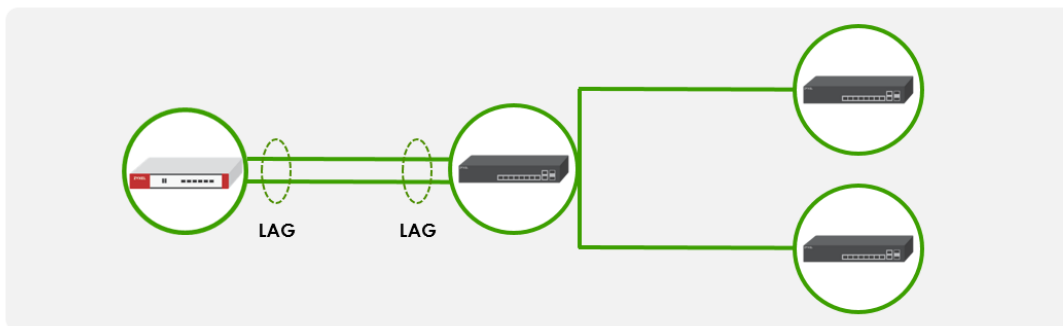
**Primary:** Allows you to specify which member interface should be preferred as the active link

Members ⓘ	ge5 x ge6 x	
Mode	active-backup	
Mii Monitoring Interval	100	(1-1000)ms
Primary	ge5	

## LAG mode: LACP (802.3ad)

Provides automatic link failover and load sharing by allowing all ports in the LAG group to transmit traffic. The LACP messages will be periodically sent.

When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall.



**Transmit Hash Policy:** Determine how outgoing traffic is distributed across the aggregated links. The default option is **src-dst-ip-mac**. Select **src-dst-ip-mac** to distribute traffic more efficiently by considering both source-destination IP and MAC.

Members <span style="color: green;">i</span>	ge5 <span style="color: green;">x</span> ge6 <span style="color: green;">x</span> <span style="float: right;">▼</span>
Mode	lacp (802.3ad) <span style="float: right;">▼</span>
Mii Monitoring Interval	100 (1-1000)ms
Transmit Hash Policy	src-dst-ip-mac <span style="float: right;">▼</span>

### 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.

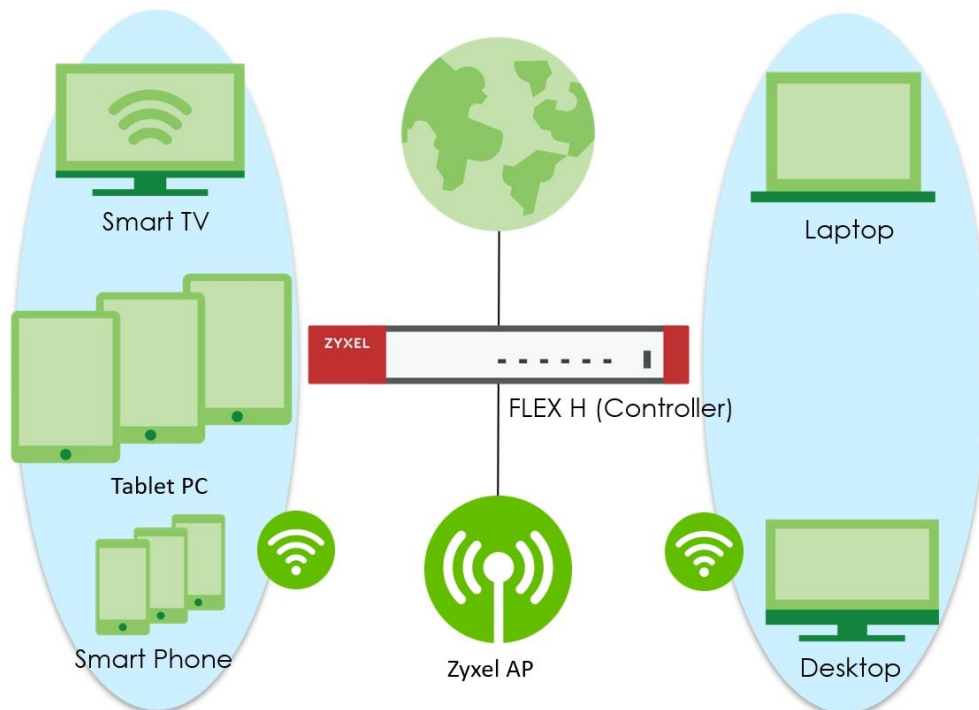
Members <span style="color: green;">i</span>	ge5 <span style="color: green;">x</span> ge6 <span style="color: green;">x</span> <span style="float: right;">▼</span>
Mode	static <span style="float: right;">▼</span>
Mii Monitoring Interval	100 (1-1000)ms
Transmit Hash Policy	src-dst-ip-mac <span style="float: right;">▼</span>


## 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

Search insights

<input checked="" type="checkbox"/> Name	IP Address
<input checked="" type="checkbox"/> AP-F4:4D:5C:9D:D8:A8	192.168.168.38

Once the actions above are completed, the AP will be listed in the Managed AP tab.

**Wireless > Access Points > AP List > Managed AP**

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**

#	Enabled	Name	WLAN Security
1	<input checked="" type="checkbox"/>	Zyxel_Wireless_Network	<input checked="" type="radio"/> Password
2	<input type="checkbox"/>	SSID2	<input checked="" type="radio"/> Open
3	<input type="checkbox"/>	SSID3	<input checked="" type="radio"/> Open
4	<input type="checkbox"/>	SSID4	<input checked="" type="radio"/> Open
5	<input type="checkbox"/>	SSID5	<input checked="" type="radio"/> Open
6	<input type="checkbox"/>	SSID6	<input checked="" type="radio"/> Open
7	<input type="checkbox"/>	SSID7	<input checked="" type="radio"/> Open
8	<input type="checkbox"/>	SSID8	<input checked="" type="radio"/> Open

## Test the Result

Go to Wireless > Access Points > AP List > Managed AP tab. You can check the list of APs currently connected, along with detailed information such as IP address, model name, current clients, MAC address, and radio information.

### Wireless > Access Points > AP List > Managed AP

Firmware Status	Status	Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	Uplink	Power Mode
Update Available	✓	AP-F44D5C9DD8A8	192.168.168.38	WBE660S	0	F4:4D:5C:9D:D8:A8	n/a	n/a	n/a	ETHERNET	Limited

Go to the Wireless > WLAN clients, you can check the list of wireless stations associated with a managed AP and the details information such as SSID Name, Security, IPv4 Address, and association time.

### Wireless > WLAN clients

MAC Address	Host Name	Connected to	AP Group	SSID	Security	IPv4 Address	Association time
E0:D0:45:6B:3F:69	NT122546-NB01	AP-F44D5C9DD8A8	default	Zyxel_Wireless_Network	WPA2-PSK	192.168.168.39	2025/03/26 17:08:11

Using a laptop to connect to SSID: Zyxel\_Wireless\_Network and type the password for authentication. Go to the Log & Report > Log / Events > APC, you will see WLAN Station Info as shown below.

### Log & Report > Log / Events > APC

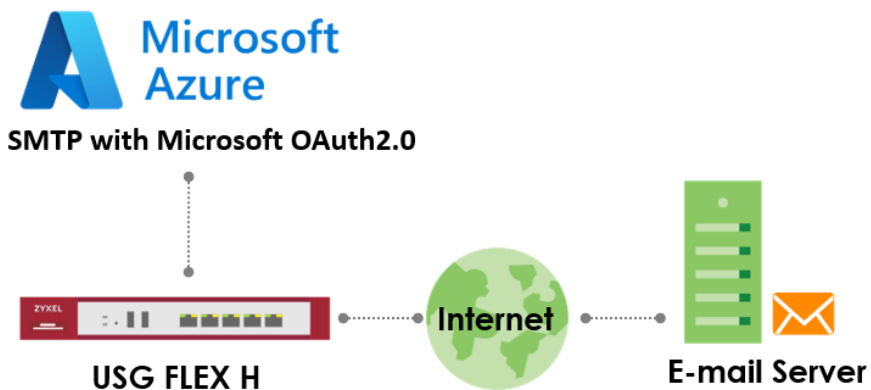
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2025-03-26 17:17:25	Wlan Station Info	STA connected. MAC:E0:D0:45:6B:3F:69, AP:AP-F44D5C9DD8A8, interface:wlan-2-1, SSID: Zyxel_Wireless_Network. Signal: -20dBm	0.0.0.0	0.0.0.0	0	


## **What Could Go Wrong?**

If you can't see AP information in the AP List, please check the number of APs connected to the USG FLEX H firewall has exceeded the maximum Managed AP number it can support. If your mobile device can't access to the Internet via AP connects to the USG FLEX H firewall, please check if the LAN outgoing security policy allow access to the Internet.

## How to set up SMTP with Microsoft OAuth2.0?

This guide explains how to configure your gateway to send emails using **SMTP with Microsoft OAuth 2.0** authentication through a Microsoft 365 account. OAuth 2.0 provides secure, token-based authentication, replacing less secure basic authentication methods. Follow these steps to register an application in Microsoft Azure and configure your gateway for SMTP.



 Note: SMTP with Microsoft OAuth 2.0 is supported on USG Flex H series. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.35).

## Prerequisites

1. A Microsoft 365 account with a licensed Exchange Online mailbox.
2. Administrative access to the Microsoft Azure Portal (<https://portal.azure.com>).
3. SMTP AUTH is enabled for the mailbox (see Step 3 below).
4. Your gateway device with SMTP configuration access (firmware version uOS1.35 or above).

## Step 1: Register an Application in Azure Portal

1. **Sign in to Azure Portal** - Navigate to <https://portal.azure.com> and sign in with an account that has administrative privileges for Microsoft Entra ID.
2. **Navigate to App Registrations** - In the left-hand menu, select **Microsoft Entra ID > App registrations > New registration**.

3. **Configure the Application** –

**Name:** Enter a descriptive name (e.g., "Gateway SMTP App").

**Supported account types:** Select **Accounts in this organizational directory only** (Single tenant) for most cases.

**Redirect URI:** The redirect URI specifies where the authorization server should send the user back after successfully authenticating to return an access token to their email account.

**Type:** Select **"Web"**.

**URI:** Enter [https://\[device fqdn or ip\]/cgi-bin/msoauth2.cgi](https://[device fqdn or ip]/cgi-bin/msoauth2.cgi). Replace [Device FQDN or IP] with the actual fully qualified domain name or IP address of an internal interface that the administrator computer can connect to. (Note: Redirect URI must begin with the scheme **https**). Finally, click **Register**.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

All services > App registrations >

## Register an application

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

SMTP

Supported account types  
Who can use this application or access this API?

Accounts in this organizational directory only (Zyxel Group Corporation only - Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://192.168.0.81/cgi-bin/msoauth2.cgi

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Register

4. **Copy Application IDs** – On the app's **Overview** page, copy the **Application (client) ID** and **Directory (tenant) ID**. These are required for your gateway configuration.

Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot

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-...-...-...-...	Redirect URIs	: 1_web_0_spa_0_public_client
Object ID	: 52960d2c-...-...-...-...	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: d44c31fd-...-...-...-...	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*****	66a6b72b-1a32-4d18-a932-b0d8a4719f12

## 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?

You are editing permission(s) to your application, users will be notified.

Granting tenant-wide consent may revoke permissions that were previously granted. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization, or app. [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
offline_access	Delegated	Maintain access to data you have given it access to
User.Read	Delegated	Sign in and read basic profile

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs 3

**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

Home > App registrations > test0616

test0616 | API permissions

Search Refresh Got feedback?

You are editing permission(s) to your application, users will be notified.

Granting tenant-wide consent may revoke permissions that were previously granted. [Learn more](#)

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization, or app. [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
offline_access	Delegated	Maintain access to data you have given it access to
User.Read	Delegated	Sign in and read basic profile

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs 3

**Microsoft Graph**  
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

**Delegated permissions** 4  
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 5

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 app. [Learn more](#)

Permission

**OpenId permissions (1)** 6

offline\_access Maintain access to data you have given it access to

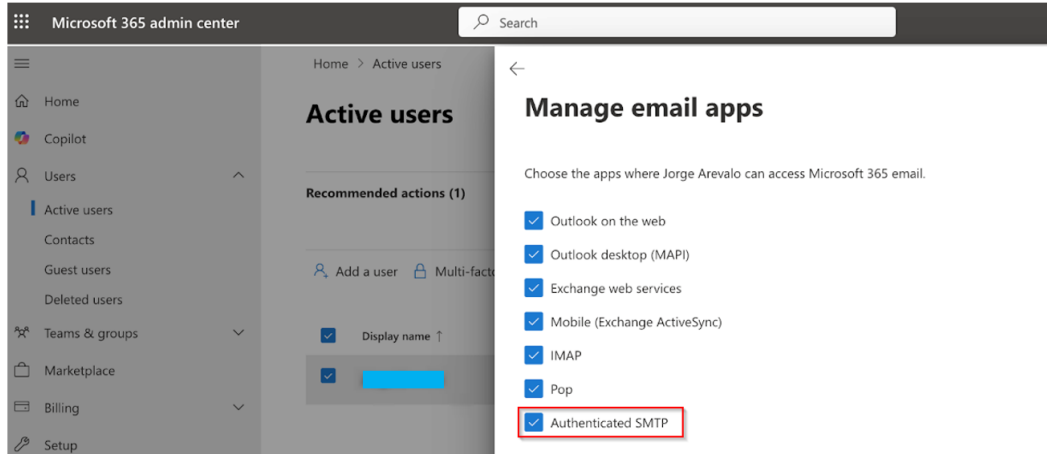
To view and manage consented permissions for individual users, click on the user's name in the table below.

**Add permissions** Discard 7

### 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.

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 breadcrumb trail is 'System > Notification > Mail Server'. The page title is 'Mail Server' with a sub-tab 'Alert'. Under 'General Settings', the 'Mail Server' field is 'smtp.office365.com' (Outgoing SMTP Server Name or IP Address), 'Port' is '587' (1-65535), 'TLS Security' is enabled, 'STARTTLS' is enabled, and 'Authenticate Server' is disabled. The 'Authentication Method' is set to 'Microsoft OAuth2.0', with a link 'How to set up SMTP with Microsoft OAuth2.0'. The 'Sender Email Address' is 'jerry@zyxel.com.tw', 'Client ID' is '27cba1b2-fad2-4c0a-9ee7-8f3d44336a82', 'Client Secret' is masked with dots, and 'Tenant ID' is 'd44c31fd-3401-e17a-f1e7-d70e4b789a6d'. The 'Token Status' is 'No token available – click "Get New Token"'. There are 'Get New Token' and 'Refresh Token Status' buttons. Below, the 'Default Sender and Recipient' section has a 'Recipient' field 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](mailto: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.

The screenshot shows the 'Mail Server' configuration page in the Zyxel web interface. The 'Authentication Method' is set to 'Microsoft OAuth2.0'. The 'Token Status' is 'No token available - click "Get New Token"'. Two buttons, 'Get New Token' and 'Refresh Token Status', are highlighted with a red box. Below the configuration, there is a 'Default Sender and Recipient' section with a 'Recipient' field and a 'Send Test Email' button.

## Verify the SMTP with Microsoft OAuth2.0 function

1. Ensure token is successfully acquired.

This screenshot shows the same configuration page as above, but the 'Token Status' is now 'Valid', which is highlighted with a red box. The 'Get New Token' and 'Refresh Token Status' buttons are still visible below the status.

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.

#	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.

**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:

[+ Add](#)

[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 > [View Details](#)

j@zyxel.com.tw  
帳號名 - j@zyxel.com

**General**

Model Name: USG FLEX 200HP  
 Firmware Version: V1.35(ABXE.0j4 | 2025-06-25 06:26:12  
 MAC Address Range: 08:00:27:00:00:00-08:00:27:00:00:00  
 System Uptime: 2 days, 7:06:20  
 System Name: usgflex200hp

**Licensing**

[License Status](#)

[Signature Status](#)

**License 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:

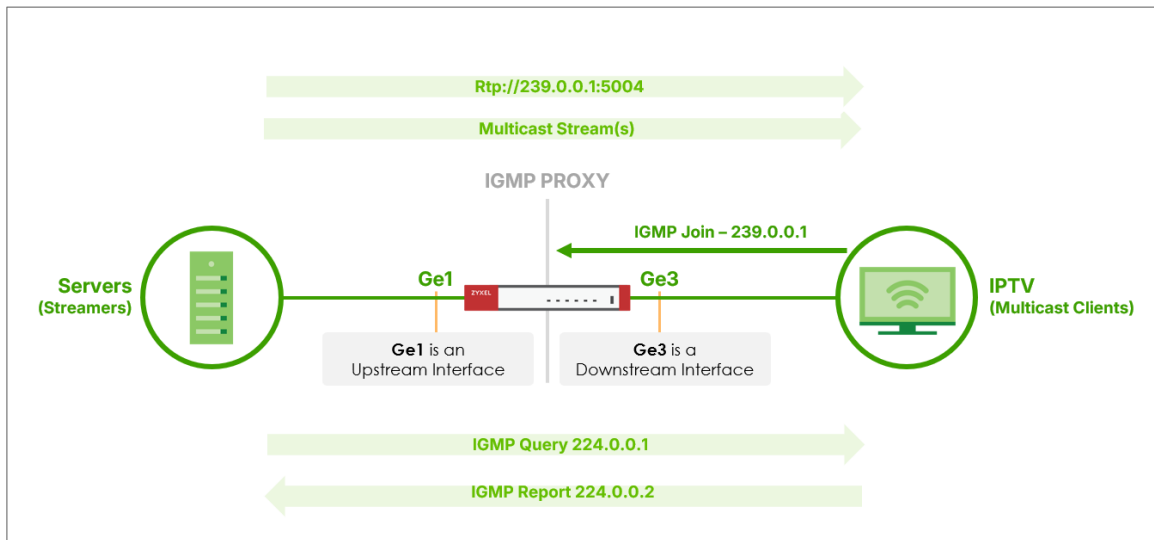
- o Verify all steps were completed correctly
- o Check Microsoft Entra ID audit logs for authentication errors
- o Contact your system administrator for Azure access issues
- o Refer to Microsoft's official OAuth 2.0 documentation


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.

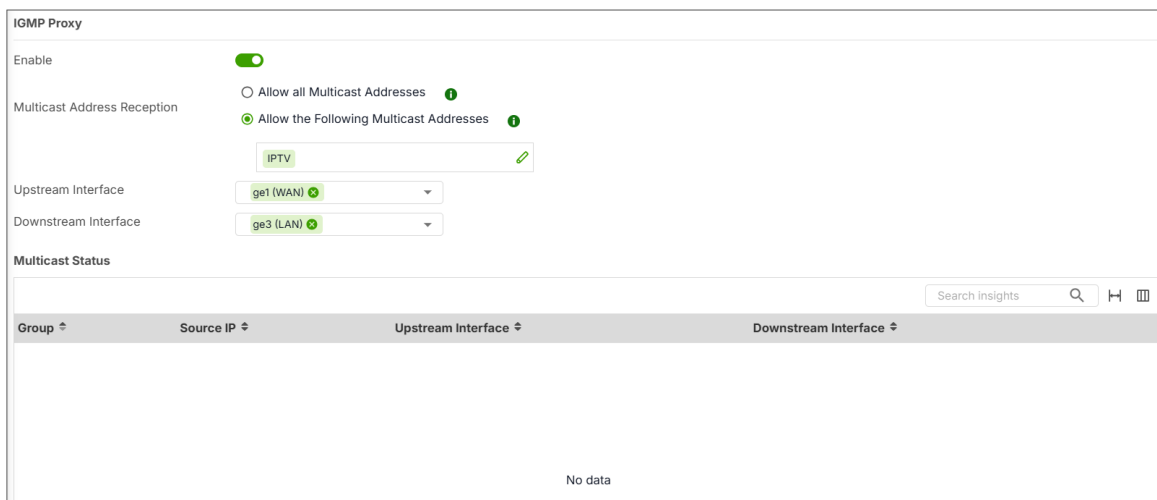


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.36).

## Enable the IGMP Proxy for Downstream and Upstream Interface

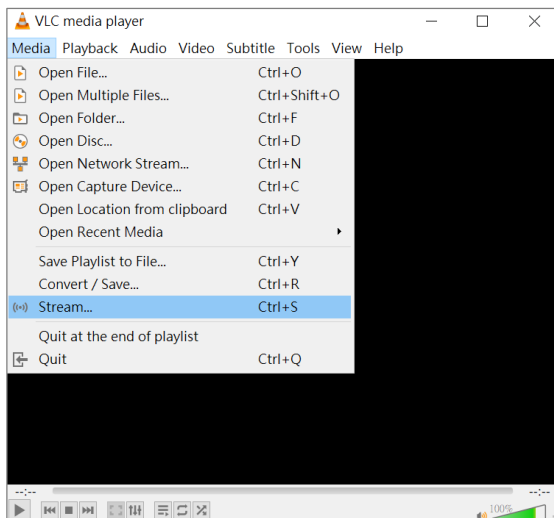
Go to "Network > Multicast" and enable IGMP Proxy. Select "Allow the Following Multicast Addresses". Create an address object for the IPTV client, and select this client.

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.

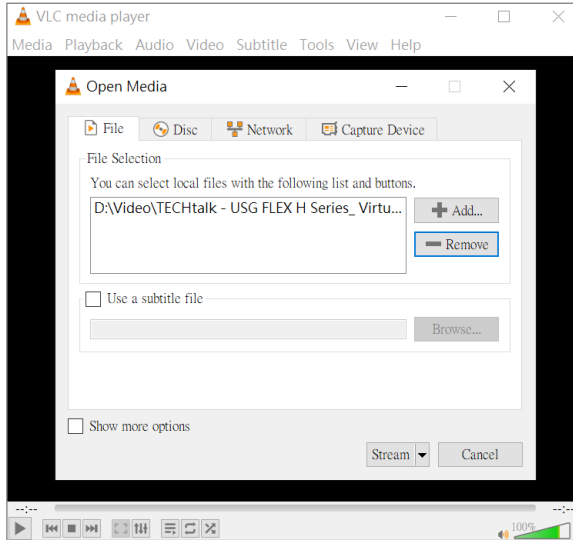


## Set Up Streamer Server Using VLC software

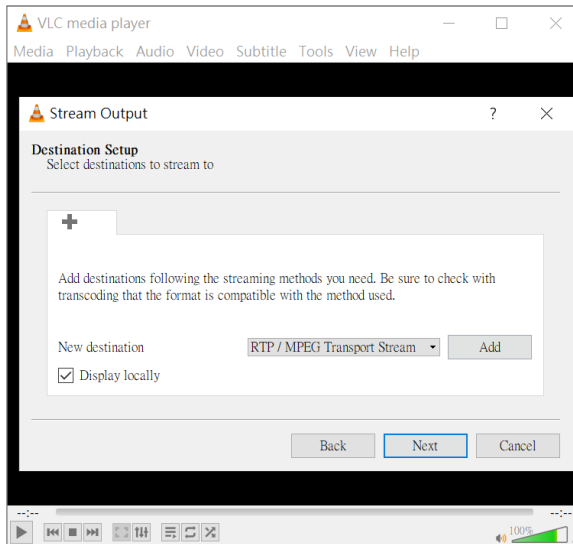
Open Medial Player, and Select "Stream"



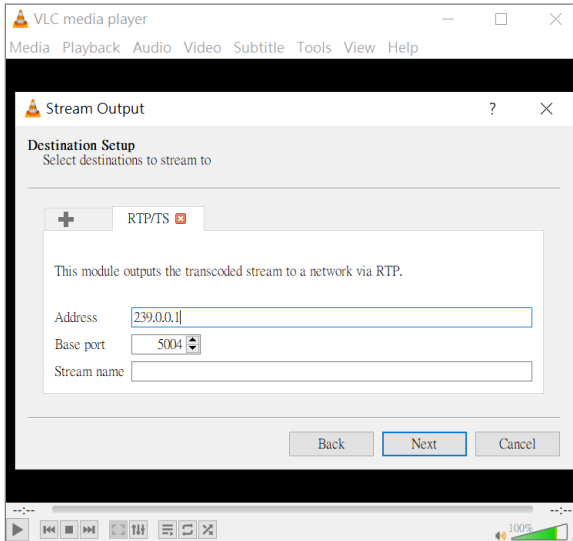
Add a video file and click on "Stream" button.



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

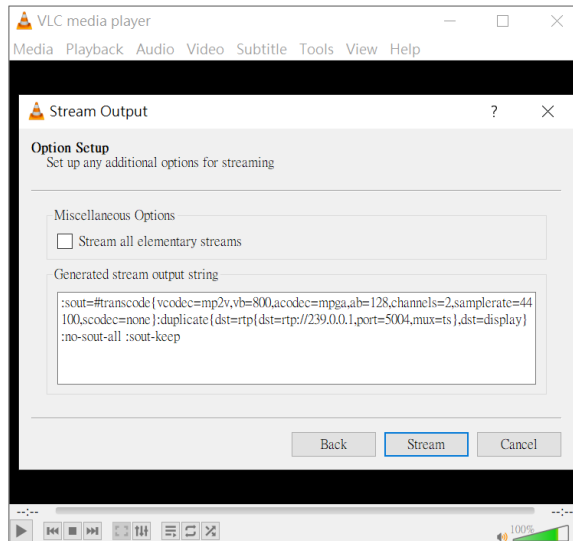


Configure IP address and port number of IGMP group.



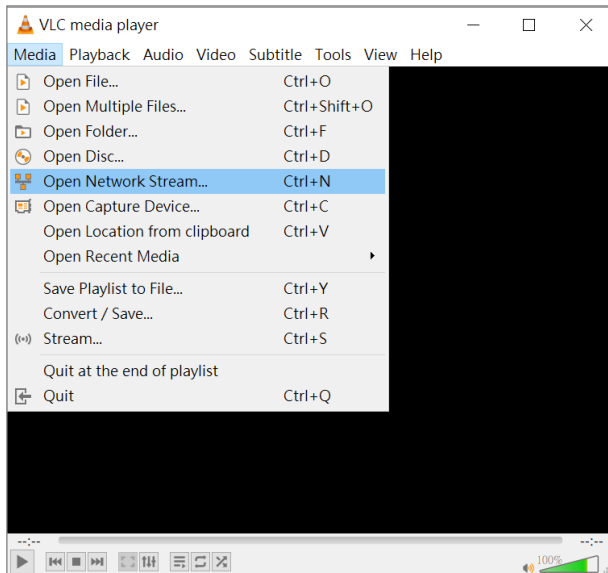
Click Next to complete the setup process

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

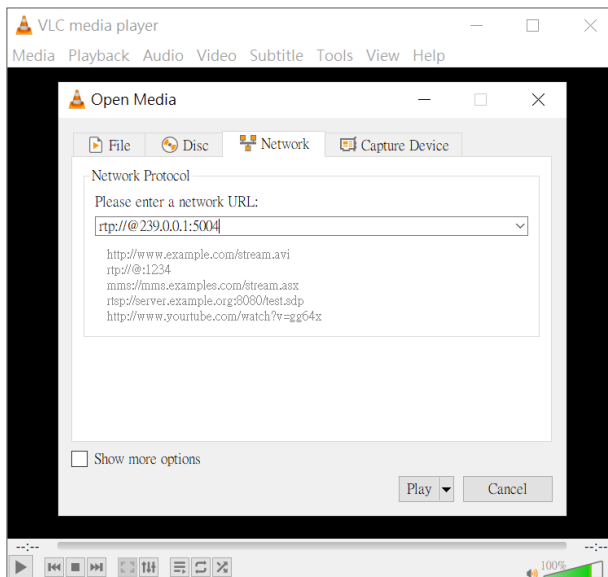


## Set Up Player Client Using VLC software

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

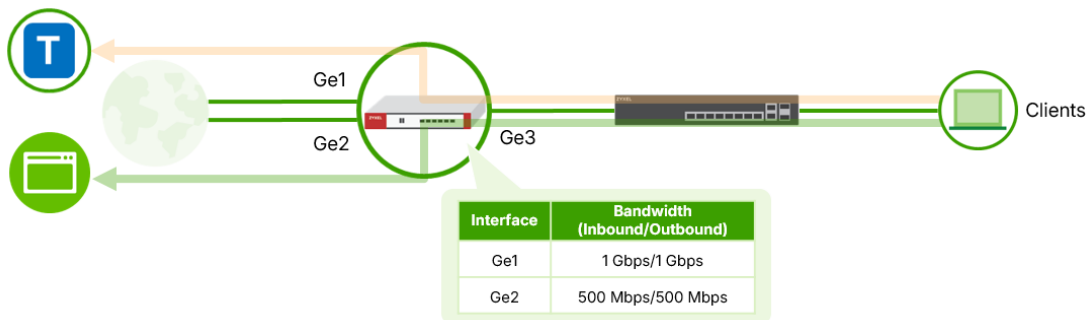
After IPTV client join the multicast group, we can monitor the status on Multicast table.

IGMP Proxy			
Enable	<input checked="" type="checkbox"/>		
Multicast Address Reception	<input type="radio"/> Allow all Multicast Addresses ⓘ <input checked="" type="radio"/> Allow the Following Multicast Addresses ⓘ		
	<input type="text" value="IPTV"/> ⓘ		
Upstream Interface	<input type="text" value="ge1 (WAN)"/> ⓘ		
Downstream Interface	<input type="text" value="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** ▾

- 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

Source Port

**Next Hop**

---

Type

Interface

**DSCP Marking**

---

DSCP Marking

**Address Translation**

---

SNAT Address

## 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												Static Route	
Configuration													
+ Add Edit Remove Active Inactive Move to Refresh <span style="float: right;">Search insights</span>													
Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits
<input type="checkbox"/>	1	any	none	ge3	LANL_SUBNET	any	any	Microsoft teams, Teamspeak v2 + 1	any	ge1	preserve	outgoing-interface	59

## Chapter 6- Nebula

### How to Set Up Nebula site-to-site VPN on the USG FLEX H?

This example shows how to use Nebula VPN to establish Site to Site VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Site-to-Site VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



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

## Set Up the Site-to-Site VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Site-to-Site VPN topology.

### USG FLEX/ATP site

The screenshot shows the Nebula Control Center interface for configuring Site-to-Site VPN on a USG FLEX/ATP site. The breadcrumb trail is Site-wide > Configure > Firewall > Site-to-Site VPN. The configuration is for Site: ATP200.

**Site-to-Site VPN**

- Primary interface: wan1
- Secondary interface: wan2

**Local networks**

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

**Nebula VPN**

- Enabled:
- VPN Area: Default
- VPN topology: Split tunnel (send only site-to-site traffic over the VPN)
  - 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: [Organization Name] > Site: USG Flex 200HP

Site-wide > Configure > Firewall > Site-to-Site VPN

Site-to-Site VPN

Primary interface: **ge1\_ppp**

Secondary interface: **ge2**

Name	Subnet	Use VPN
ge3	192.168.168/24	<input checked="" type="checkbox"/>
ge4	192.168.169/24	<input type="checkbox"/>

Nebula VPN

Enabled:

VPN Area: Default

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

Area communication:

NAT traversal:  None  Custom NAT traversal: IP

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: [Organization Name] > 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: [Organization Name] > 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

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.0/24	connected	109.38 KB	109.38 KB	679	2025-01-07 14:48:19

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.


The screenshot shows the ZyXel USG FLEX 200HP Web-GUI interface. The breadcrumb navigation is VPN Status > IPsec VPN > Site to Site VPN. The page title is 'Site to Site VPN' with a sub-header 'Remote Access VPN'. There are 'Disconnect' and 'Refresh' buttons. A table displays the VPN connections, with the 'Nebula VPN' entry highlighted in red. The table has columns for Name, Remote Gateway, Remote ID, My Address, Policy Route, Uptime, Rekey, Inbound (Bytes), and Outbound (Bytes).

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BCP11802	111.243.11.11	5182L372000	59.115.11.11	0.0.0.0 <-> 0.0.0.0	2544	24987	2623 (157.38K bytes)	2600 (156K bytes)

## 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

The screenshot shows the Nebula Control Center interface for configuring Site-to-Site VPN. The page is titled "Site-to-Site VPN" and includes the following configuration sections:

- Primary interface:** ge1\_PPP
- Secondary interface:** ge2
- Local networks:**

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>
- Nebula VPN:**
  - Enabled:
  - VPN Area: Default
  - VPN topology: Split tunnel (send only site-to-site traffic over the VPN) / Hub-and-Spoke
  - Hubs (peers connect to):
 

SiteName
1 USG Flex 200HP

At the bottom, there is a note: "Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestration](#) 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

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.770/24	<input type="checkbox"/>

Nebula VPN

Enabled:   
VPN Area: Default  
VPN topology: Split tunnel (send only site-to-site traffic over the VPN)  
Hub-and-Spoke  
Hubs (peers connect to):  
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: 192.168.168/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.1/24	connected	91.42 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

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168.1/24	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.


The screenshot shows the ZyXel USG FLEX 200HP Web-GUI interface. The breadcrumb navigation path is VPN Status > IPsec VPN > Site to Site VPN. The main content area displays a table of Site to Site VPN connections. A red box highlights the first entry, which is the 'Nebula VPN' connection. The table has columns for Name, Remote Gateway, Remote ID, My Address, Policy Route, Uptime, Rekey, Inbound (Bytes), and Outbound (Bytes).

	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BC9911802B	111.243.	5182L3720007311	59.115.	0.0.0.0 <-> 0.0.0.0	742	25466	762 (45.72K bytes)	731 (43.86K bytes)

## How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)?

This example shows how to use Nebula VPN to establish Hub-and-Spoke VPN tunnel between USG FLEX/ATP and USG FLEX H. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



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

## Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke VPN topology and ensure that the USG FLEX H series is set as the Spoke site.

### USG FLEX/ATP site

The screenshot displays the Nebula Control Center interface for configuring Site-to-Site VPN. The breadcrumb trail is Site-wide > Configure > Firewall > Site-to-Site VPN. The page is titled "Site-to-Site VPN".

**Primary interface:** wan1

**Secondary interface:** wan2

**Local networks:**

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

**Nebula VPN:**

**Enabled:**

**VPN Area:** Default

**VPN topology:** Split tunnel (send only site-to-site traffic over the VPN)  
Hub-and-Spoke

**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

The screenshot shows the configuration page for Site-to-Site VPN in the Nebula Control Center. The page is for the 'USG Flex 200HP' site. Key configuration elements include:

- Primary interface:** ge1\_PPP
- Secondary interface:** ge2
- Local networks:** A table with columns 'Name', 'Subnet', and 'Use VPN'.
 

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>
- Nebula VPN:**
  - Enabled:
  - VPN Area: Default
  - VPN topology: Split tunnel (send only site-to-site traffic over the VPN)
  - Hub-and-Spoke: Hub-and-Spoke
  - Hubs (peers connect to):
 

SiteName
1 ATP200

At the bottom, there is a note: "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.

The screenshot shows the 'VPN connections' monitoring page for the 'ATP200' site. It displays the connection status and a table of site connectivity.

**Connection status:** This security gateway is exporting 1 subnet over the VPN: 192.168.66.0/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168.1/24	connected	26.71 KB	34.84 KB	869	2025-01-07 17:46:52

The screenshot shows the 'VPN connections' monitoring page for the 'USG Flex 200HP' site. It displays the connection status and a table of site connectivity.

**Connection status:** This security gateway is exporting 1 subnet over the VPN: 192.168.168.1/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.1/24	connected	93.05 KB	89.77 KB	439	2025-01-07 16:36:32

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

The screenshot shows the ZyXel USG FLEX 200HP Web-GUI interface. The breadcrumb navigation path is VPN Status > IPsec VPN > Site to Site VPN. The main content area displays a table of Site to Site VPN connections. A red box highlights the 'Nebula VPN' entry, which is in a connected state.

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BC9911B02B8...	111.243.2...	182L372000...	1.161.1.8...	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.



In Step 3, The Web GUI will prompt you to register your firewall.

The screenshot shows a web interface for "Device Registration". On the left, a vertical progress bar has six steps: 1. Connect To Internet (checked), 2. System Time (checked), 3. Device Registration (highlighted with a green circle and number), 4. License Summary, 5. Subnet Planning, and 6. Finish. The main content area is titled "Device Registration" and contains the following text: "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." Below this, it says "Create an Organization and Site on Nebula to be able to use SecuReporter and remote support." and "Registration Status: Incomplete". At the bottom right, there are two buttons: "Back" and "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.

The screenshot shows the Nebula Control Center (NCC) registration page. On the left, there is a sidebar with a heading "01" and two paragraphs of text. The first paragraph says: "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." The second paragraph says: "To register your USG FLEX H firewall with Nebula, please select an Organization and a Site under your authority, or create new ones." The main content area is titled "First step is to create your Organization and Site" and contains two input fields: "Organization" (a dropdown menu with "Organization name" selected) and "Site" (a text input field with "Site name" and a clear button 'x'). A green "Next" button is located below the input fields.

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.

**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?**

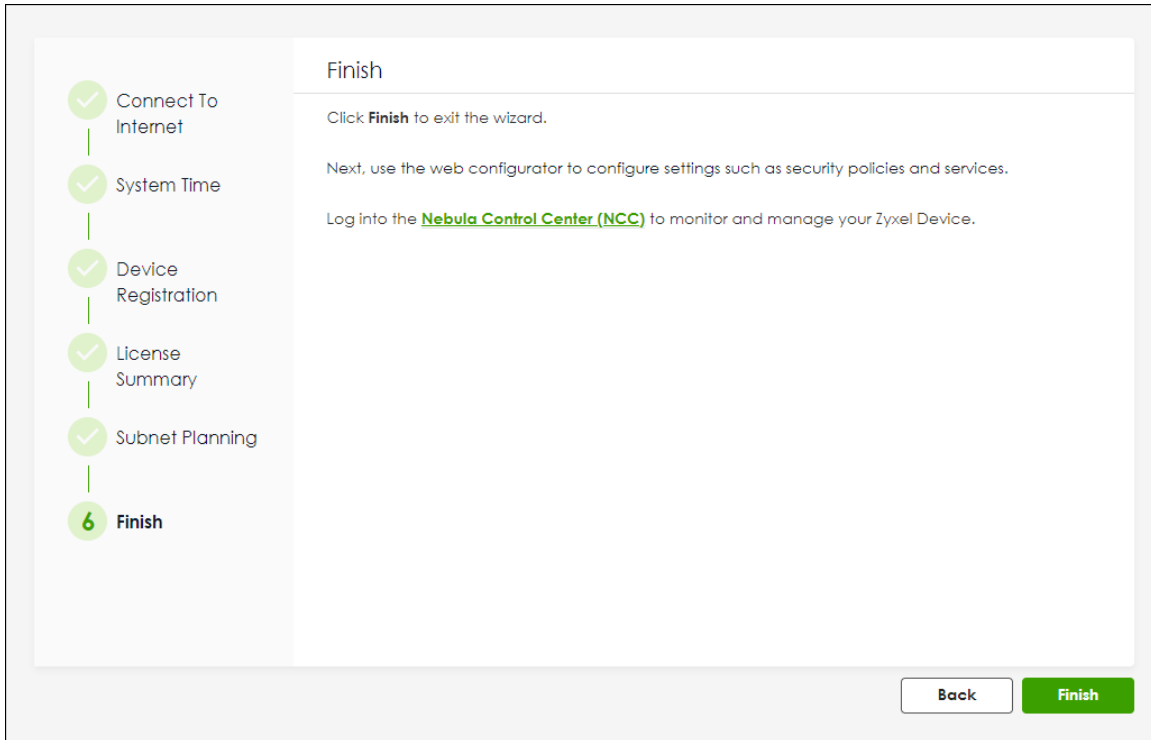
Yes, let Nebula adjust subnets of ge3/ge4.

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

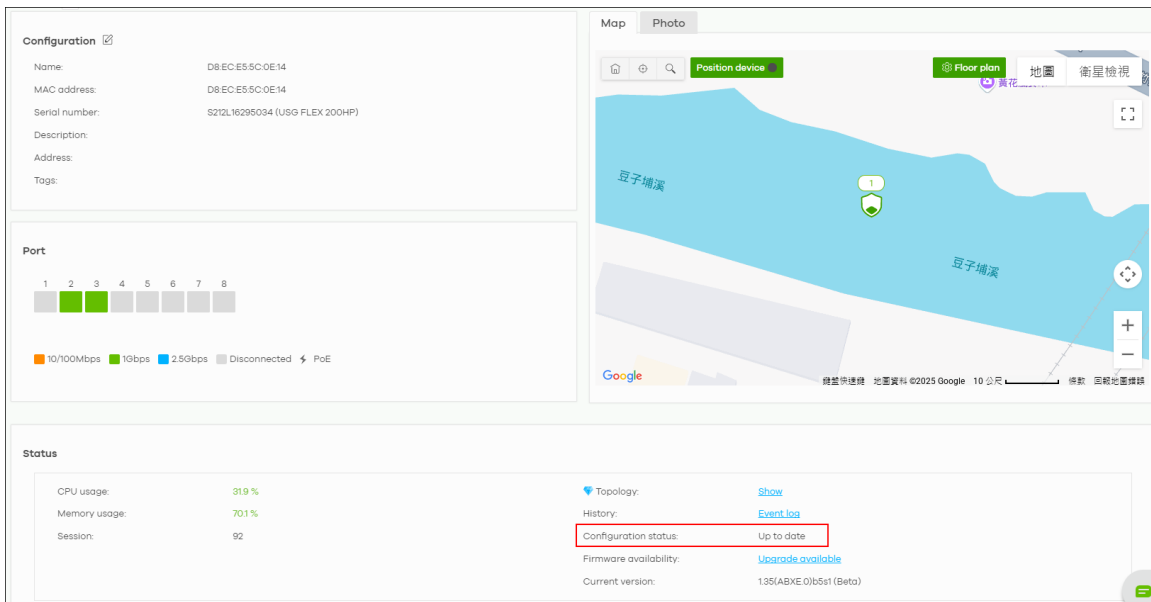
**Important notice:** In VPN scenario, connection may fail when the internal subnet of a firewall conflicts with the others. The problem happens when the firewall uses default subnets participating VPNs and you have to manually adjust internal subnets to fix the problem.

Back Next

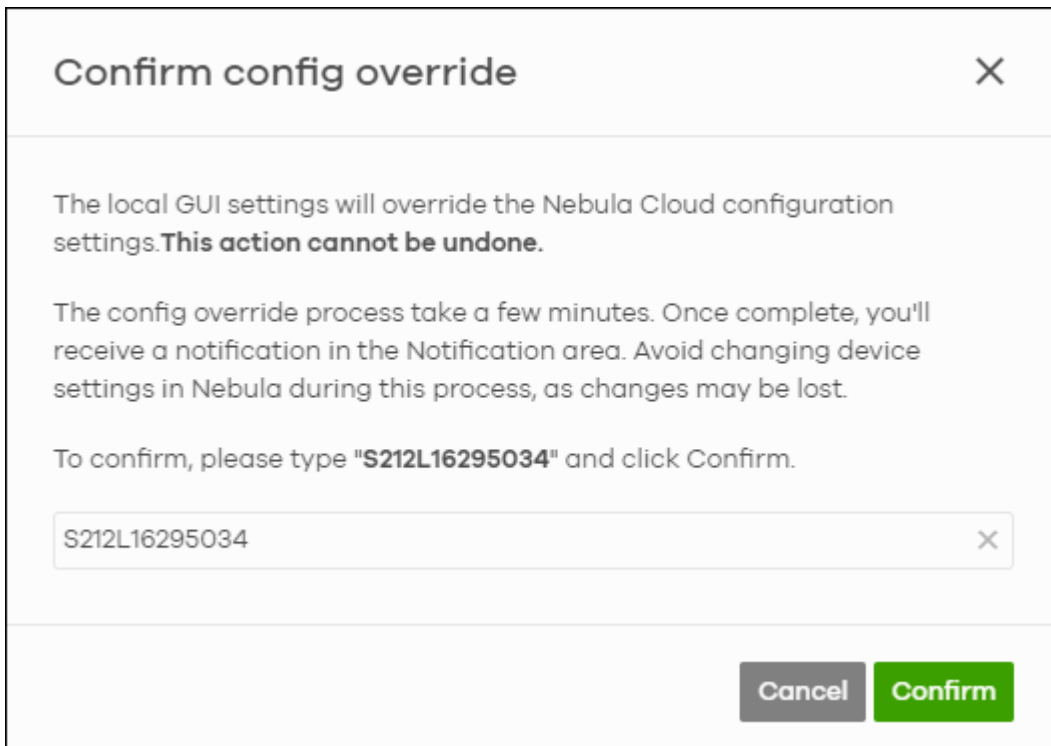
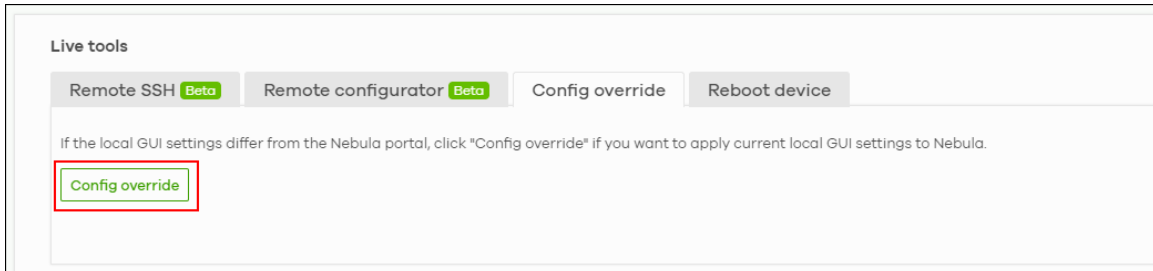
In Step 6, Click **Finish** to close the wizard from Web GUI.



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.

[Exit Wizard](#)

**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		<a href="#">View</a>	
ge2		192.168.1.55	255.255.255.0		p2	WAN		<a href="#">View</a>	
<a href="#">+Add</a>									
Internal									
Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description	Reference	
ge3		192.168.88.1	255.255.255.0		p3 p4 p5 p6	LAN		<a href="#">View</a>	
ge4		192.168.89.1	255.255.255.0		p7 p8	LAN		<a href="#">View</a>	
<a href="#">+Add</a>									


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

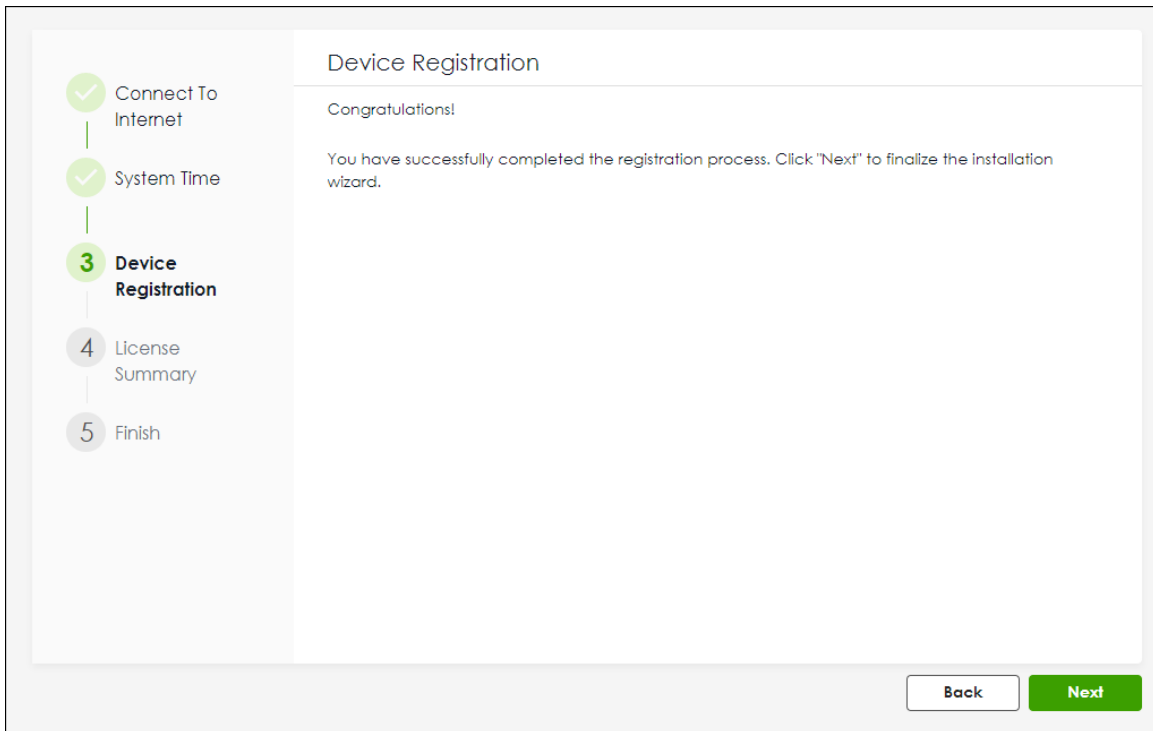
Second DNS Server: 1.1.1.1

VLAN Tag:

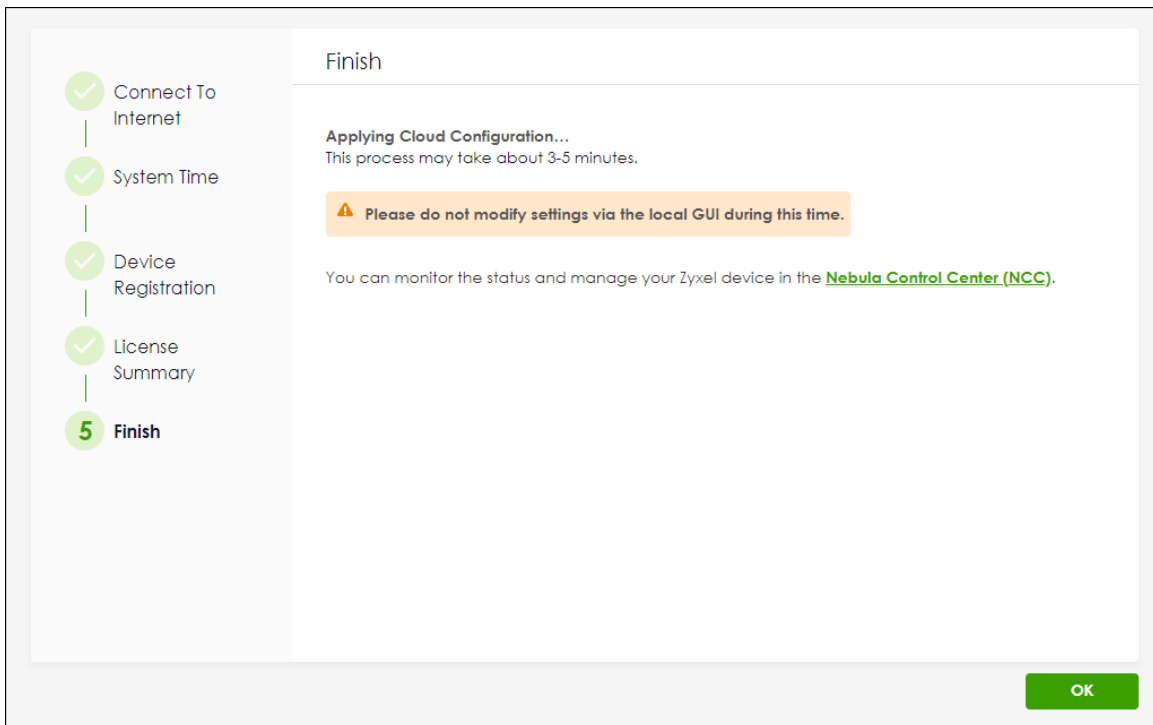
**Connection Test** ✔ Pass

**Next**

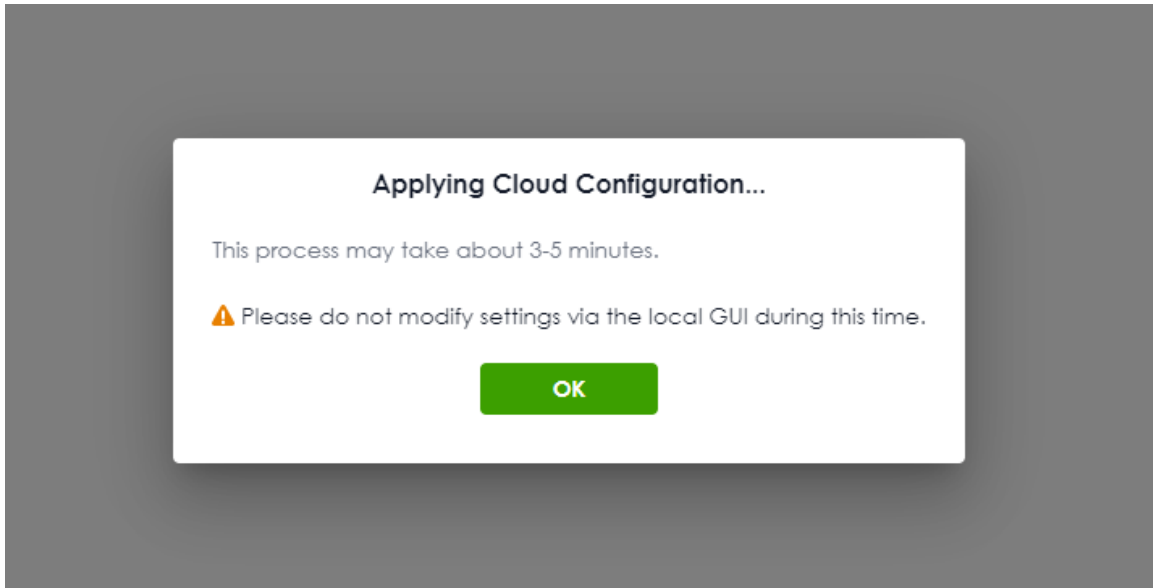
Once connected to the Internet and Nebula CC, the wizard will automatically verify the device's registration status.



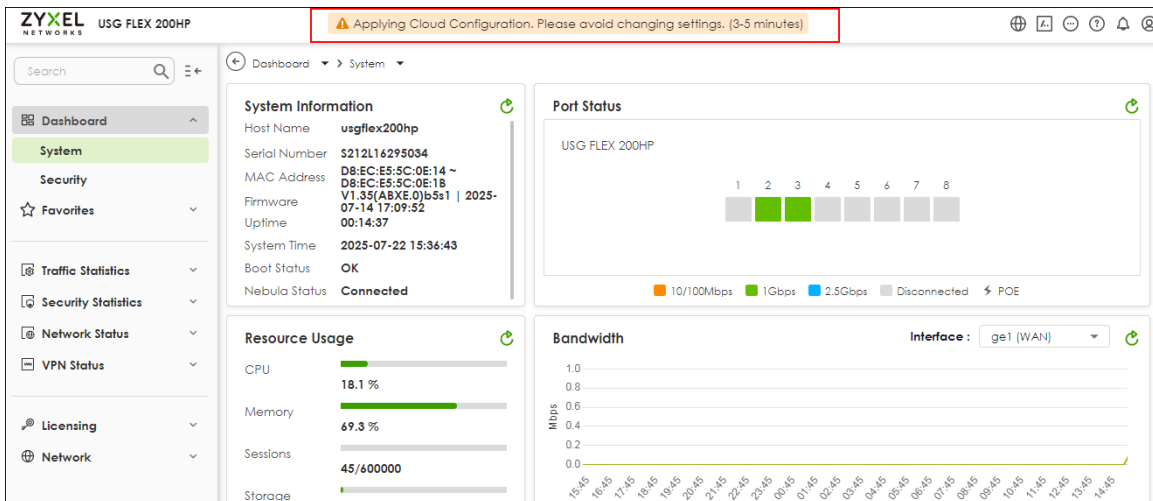
In step 5, Click **OK** to finish the wizard. Please wait 3–5 minutes for Nebula CC to provision the configuration to the firewall.



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.

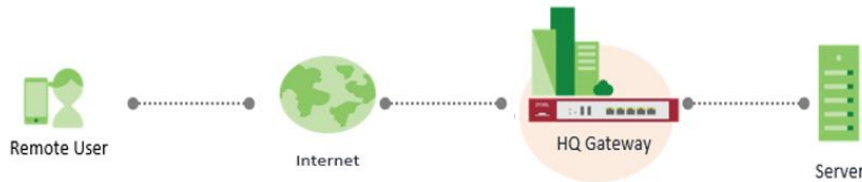
The screenshot displays the Zyxel Nebula management interface for a firewall device. It is divided into three main sections:

- Configuration:** Shows device details such as Name (D8:EC:E5:5C:0E:14), MAC address (D8:EC:E5:5C:0E:14), Serial number (S212L16295034 (USG FLEX 200HP)), Description, Address, and Tags.
- Port:** Displays a row of 8 port status indicators. Ports 1, 2, and 3 are highlighted in green, indicating they are active. A legend below shows speed options: 10/100Mbps (orange), 1Gbps (green), 2.5Gbps (blue), and Disconnected (grey), along with a PoE icon.
- Status:** Shows system health metrics: CPU usage (31.9%), Memory usage (70.1%), and Session count (92). It also includes links for Topology (Show), History (Event log), Configuration status (Up to date), Firmware availability (Upgrade available), and Current version (135(ABXE.0)b5s1 (Beta)). The 'Configuration status: Up to date' text is highlighted with a red box.

On the right side, there is a map view showing the device location on a map of '豆子埔溪' (Douzibuxi) with a 'Position device' button and a 'Floor plan' button. The map includes a search bar, a 'Position device' button, a 'Floor plan' button, and a '衛星檢視' (Satellite view) button. The map shows a blue area representing a body of water or a specific location, with a green shield icon indicating the device's location. The map is powered by Google and includes a scale bar for 10 kilometers.

## 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	<input type="text" value="Nebula assigned domain name"/>
Sign-on with	<input type="text" value="Nebula cloud authentication"/>

### Create user ✕



Account type: USER

Email:  ✕ \*

Username:  ✕

Description:  ✕

Password:  ✕ Generate

 DPPSK:   Generate


802.1X:  Allow to use WPA-Enterprise to access network

VPN Access:  Allow to use Remote VPN access

Authorized:  ▼

Expires:  Does not expire  
 Expires in:  ✕ \* minutes ▼

Login by:  ▼

 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.

The screenshot displays the ZyXel web management interface. On the left is a navigation menu with 'Configure' selected. The main area shows a 'Configure' sidebar with 'Remote access VPN' highlighted. Below this, the 'IPSec VPN Server' configuration page is shown. The 'Nebula assigned domain name' is 'nebula-68c8f3e8.d2ns-nbl.com'. A dropdown menu for 'Binding address' is open, showing options: 'ge1\_PPP', 'Auto', 'Custom IP', 'External', 'ge1', 'ge1\_PPP' (highlighted), and 'ge2'. A toggle switch for 'IPSec VPN Server' is turned on. At the bottom, there are fields for 'Type' (set to 'Nebula assigned domain name'), 'Sign-on with' (set to 'Nebula cloud authentication'), and a '+ Add account' button, along with a 'Download' button for the VPN configuration script.

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  X

DNS Server

**Security Settings**

Zone

Allowed User  X

**Phase 1 Settings**

SA Life time  X (180 - 3000000 Seconds)

Proposal

Encryption	Authentication
<input type="text" value="AES256"/>	<input type="text" value="SHA256"/>

Diffie-Hellman group  X

**Phase 2 Settings**

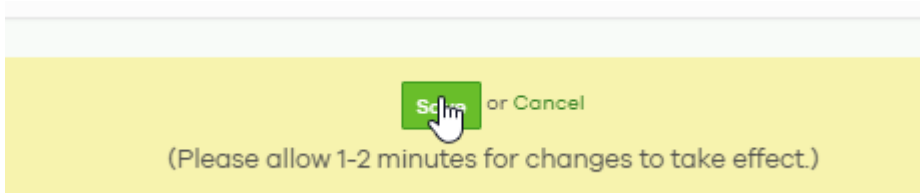
SA Life time  X (180 - 3000000 Seconds)

Proposal

Encryption	Authentication
<input type="text" value="AES256"/>	<input type="text" value="SHA256"/>

Perfect forward secrecy (PFS)  X

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.

VPN configuration script download [Download](#)

..			File folder
Android(strongSwan)	1,142	1,142	File folder
Apple	5,877	5,877	File folder
Windows	4,820	4,820	File folder
ZyxelSecuExtender	4,324	4,324	File folder

## 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.

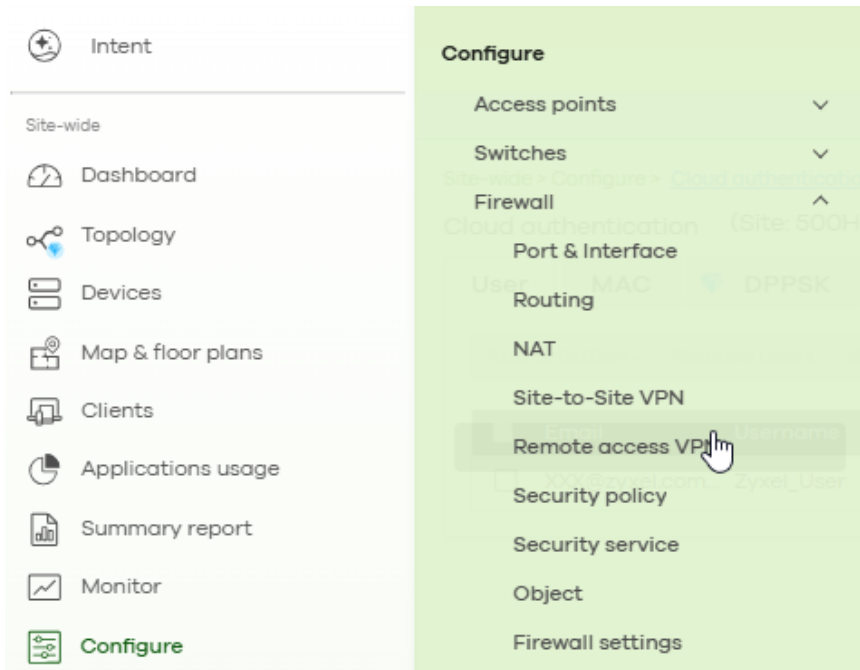
When the minimum TLS version is set to 1.3, only TLS 1.3 connections are allowed.

Minimum TLS version

1.2

1.2

1.3



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](#)

Clients will use VPN to access

**ADVANCED OPTIONS**

Internet and Local Networks (Full Tunnel)  
Auto SNAT  ⓘ

Local Networks Only (Split Tunnel)

**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



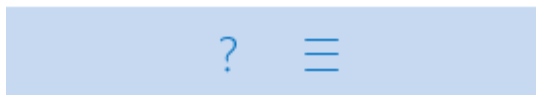
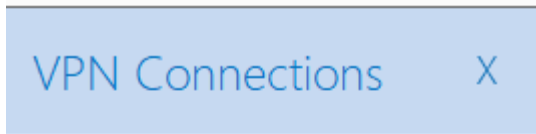


After download, will require to unzip the file

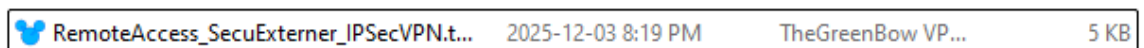
Android(strongSwan)	2025-12-01 7:01 PM	File folder
Apple	2025-12-01 7:01 PM	File folder
Windows	2025-12-01 7:01 PM	File folder
ZyxelSecuExtender	2025-12-01 7:01 PM	File folder

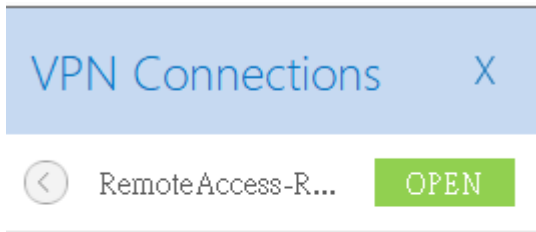
## Set Up Remote Access on SecuExtender VPN Client (Windows)

1. Launch the client

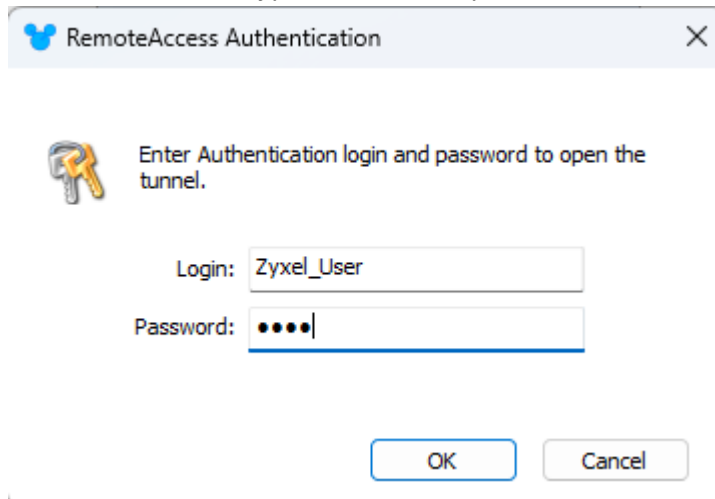


2. Double click the script file





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

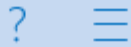


VPN Connections X



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

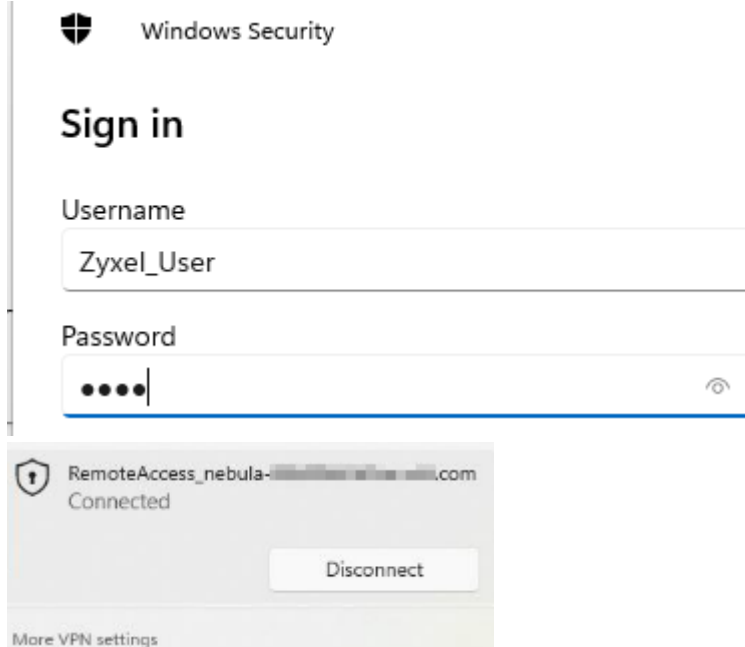
```

Requesting administrative privileges to install the IKEv2 VPN CA certificate...
"Install the IKEv2 VPN CA certificate..."
Create the RemoteAccess_nebula-10.10.10.10.com VPN connection

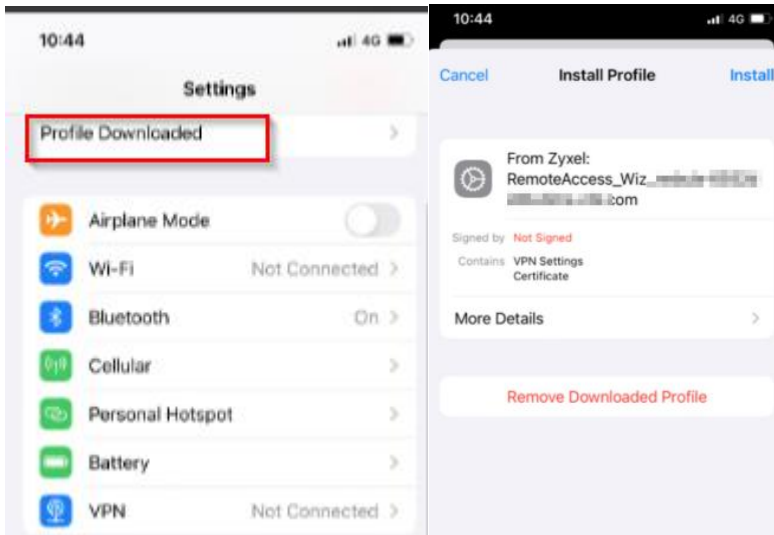
DestinationPrefix : 10.10.10.0/24
InterfaceIndex    :
InterfaceAlias    : RemoteAccess_nebula-10.10.10.10.com
AddressFamily     : IPv4
NextHop           : 0.0.0.0
Publish           : 0
RouteMetric       : 1
PolicyStore       :

Press any key to continue . . . |
  
```

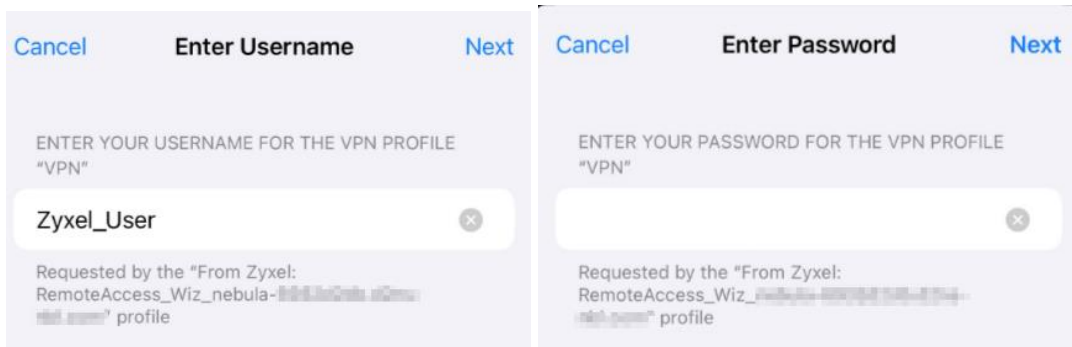
2. Connect to the VPN and enter the user name and password



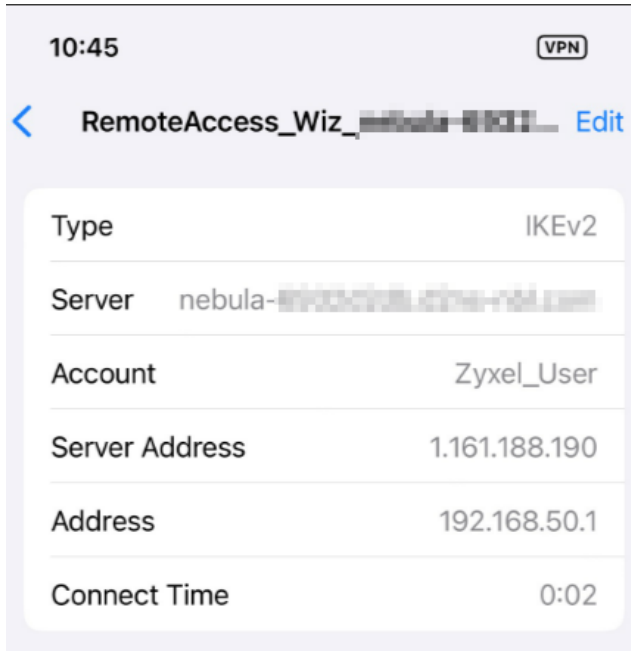




3. Enter your username and password.

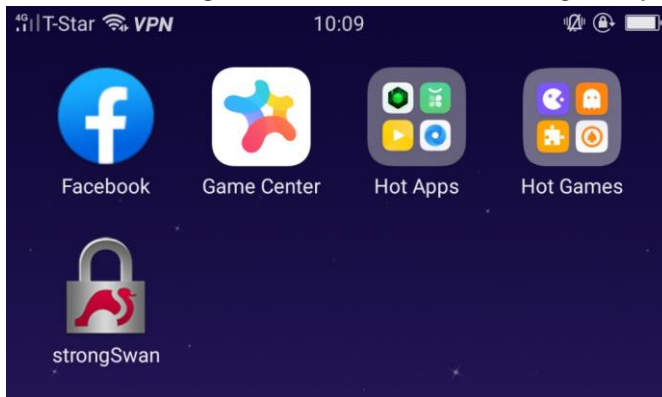


4. Connect to the VPN from the **Settings** > **VPN** menu.

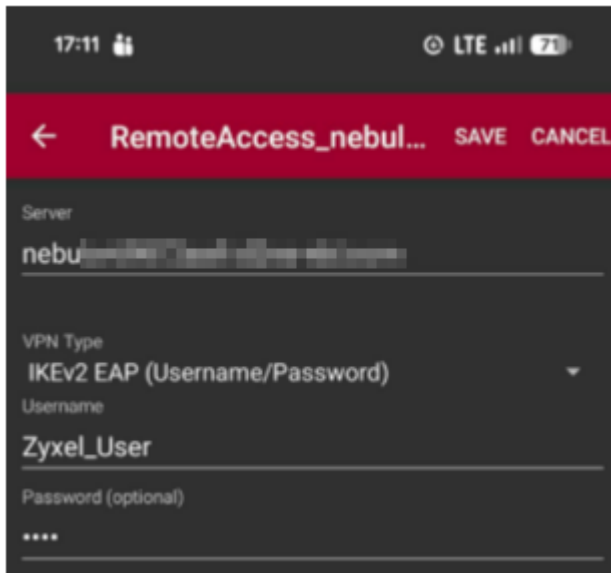


## Set Up IKEv2 VPN on Android (strongSwan App)

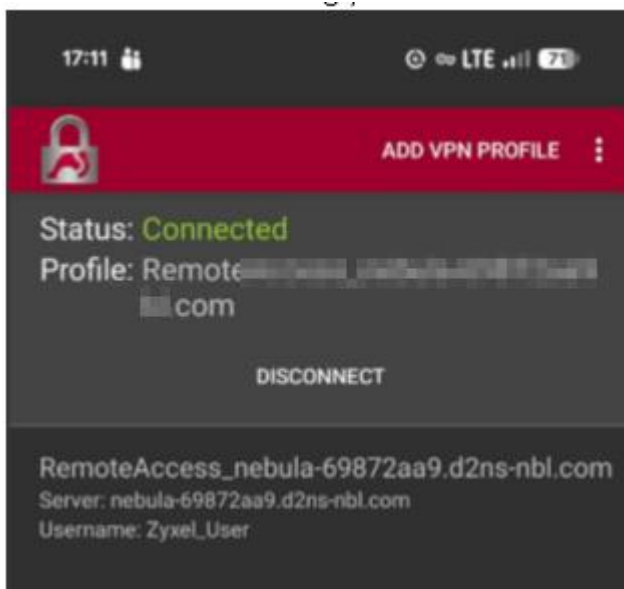
1. Install the **strongSwan VPN Client** from Google Play Store



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:

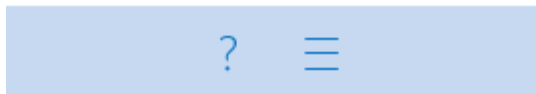
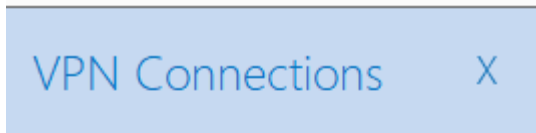
Local Networks Only (Split Tunnel)

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

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

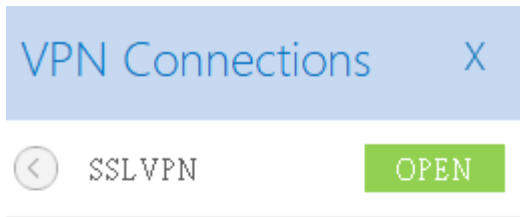
## Set Up Remote Access on SecuExtender VPN Client(Windows)

1. Launch the client

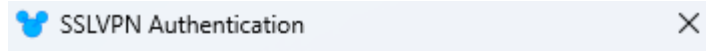


2. Double click the script file

 RemoteAccess_SecuExtender_SSLVPN.tgb	2025-12-04 7:28 AM	TheGreenBow VP...	6 KB
--------------------------------------------------------------------------------------------------------------------------	--------------------	-------------------	------



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



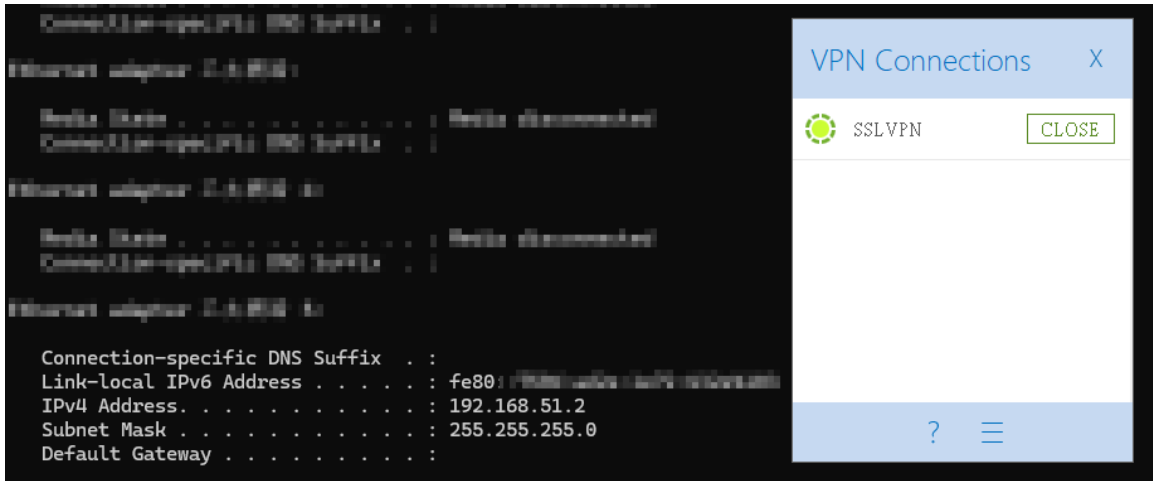
Enter Authentication login and password to open the tunnel.

Login:

Password:

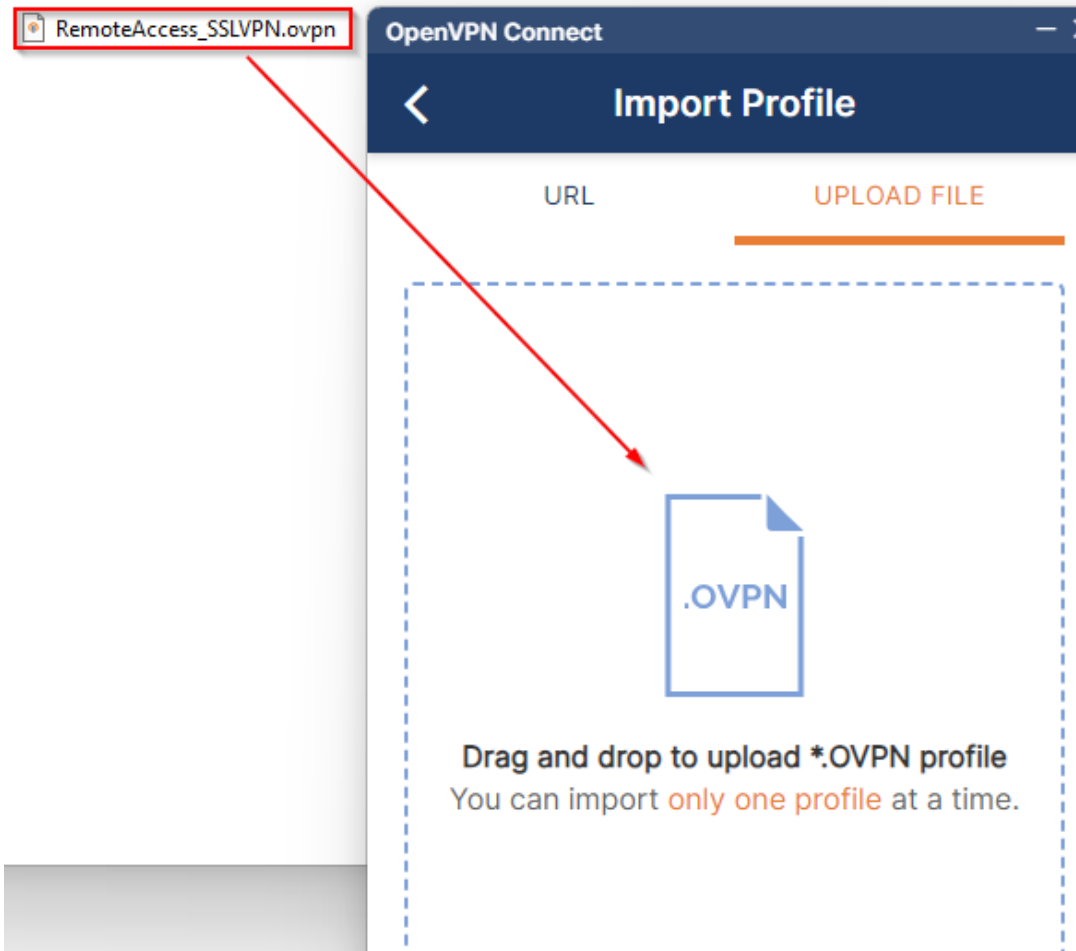
OK

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



2. Enter Username and password

OpenVPN Connect

Imported Profile

Profile Name  
nebula-XXXXXXXXXX@zyxel.com

Server Hostname  
nebula-XXXXXXXXXX@zyxel.com

Username  
Zyxel\_User

Save password

DISCONNECTED

OpenVPN Profile

nebula-XXXXXXXXXX@zyxel.com

Enter password

Profile: nebula-XXXXXXXXXX@zyxel.com

Password  
.....

OK CANCEL

3. The connection should work

The image shows a Windows Command Prompt window on the left and the OpenVPN Connect application on the right. The Command Prompt displays the following network configuration for the 'OpenVPN Connect DCO Adapter':

```
IPv4 Address . . . . . : 192.168.51.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::f3a1:ca81:f1a1:ca81%1
IPv4 Address . . . . . : 192.168.51.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter networkadapter1:

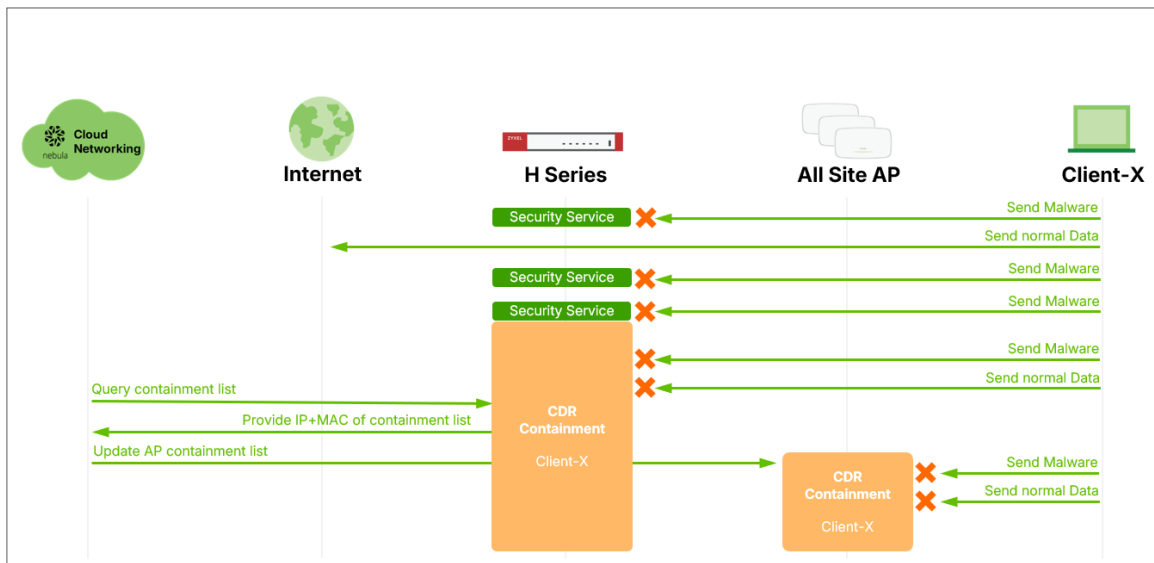
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Unknown adapter OpenVPN Connect DCO Adapter:
```

The OpenVPN Connect application on the right shows the 'Profiles' screen. The 'OpenVPN Profile' 'nebula-88000045-1234' is shown as 'CONNECTED' with a green toggle switch. Below this, there is a 'DISCONNECTED' section with a downward arrow. The 'CONNECTION STATS' section shows a data transfer rate of 92.9KB/s and a graph of activity. At the bottom, it displays 'BYTES IN 4.63 KB/S' with a downward arrow and 'BYTES OUT 771 B/S' with an upward arrow and a plus sign icon. The 'DURATION' and 'PACKET RECEIVED' fields are also visible.

## 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 <input type="text"/>	30 <input type="text"/>	Block
IDP	Vulnerability exploit detected	100 <input type="text"/>	30 <input type="text"/>	Block
Web Threats	Connections to malicious web sites detected	30 <input type="text"/>	30 <input type="text"/>	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

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

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

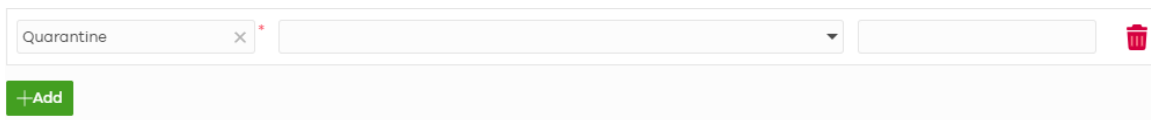
xxxx@zyxel.com.tw ⓘ

## 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 configuration window with a list of objects. The first object is named 'Quarantine' and has a red 'x' icon next to it. Below the list is a green '+Add' button.

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	<input type="text" value="quarantine"/>
Description	<input type="text"/>
Type	<input type="text" value="VLAN"/>
Member type	<input type="text" value="Port"/>
Members	<input type="text" value="p4"/>
Zone	<input type="text" value="Quarantine"/>
VLAN ID	<input type="text" value="101"/> (1 - 4094)
Priority (8021P)	<input type="text"/> (0 - 7)
Address assignment	<input type="text" value="Static"/>
IPv4 address/Network Mask	<input type="text" value="192.168.101.1/24"/>
Secondary IP	<input type="text"/>

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
<span style="background-color: #008000; color: white; padding: 2px 5px; border-radius: 3px;">+Add</span>			

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.

#	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\_CS0

Site : ██████████

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:██████████  
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.

The screenshot shows the 'Event log' interface in the ZyXel management console. The breadcrumb path is 'Site-wide > Monitor > Firewall > Event log'. The search filters are set to 'Keyword: Any', 'Category: CDR', and 'Time: 2026-05-07 16:51'. The results show 1 match in 45 event logs. The log entry is as follows:

Time	Category	Source IP	Source port	Destination IP	Destination p...	Detail
2026-05-07 16:38:18	CDR					client:192.168.168.38 user:- fromge3 security event.Web Threats threshold2 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