ZYXEL NETWORKS

www.zyxel.com

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

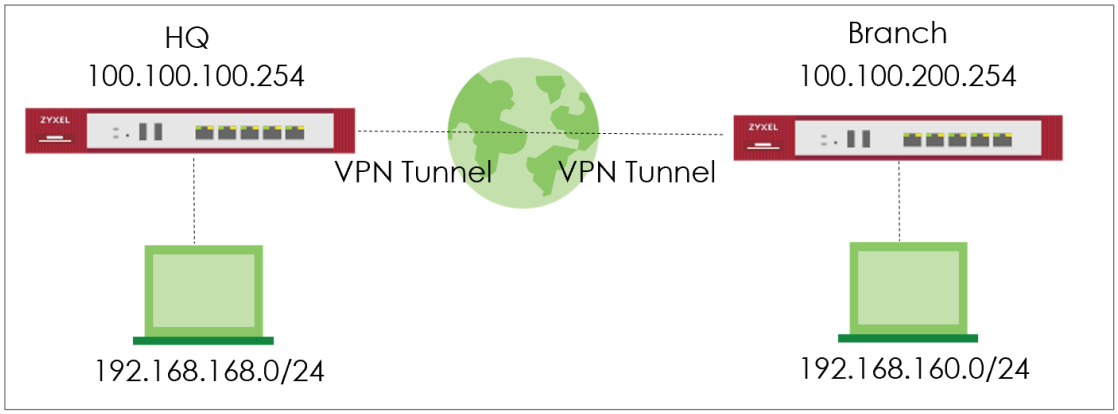
Apr. 2026

Table of Content

Chapter 1- VPN

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

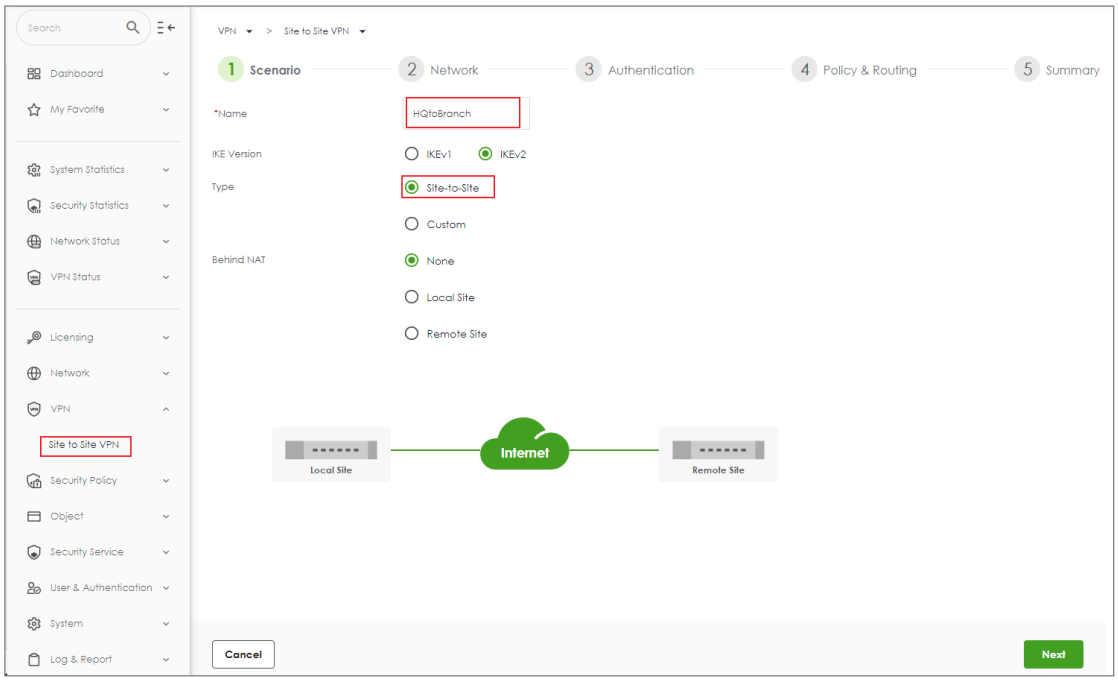
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

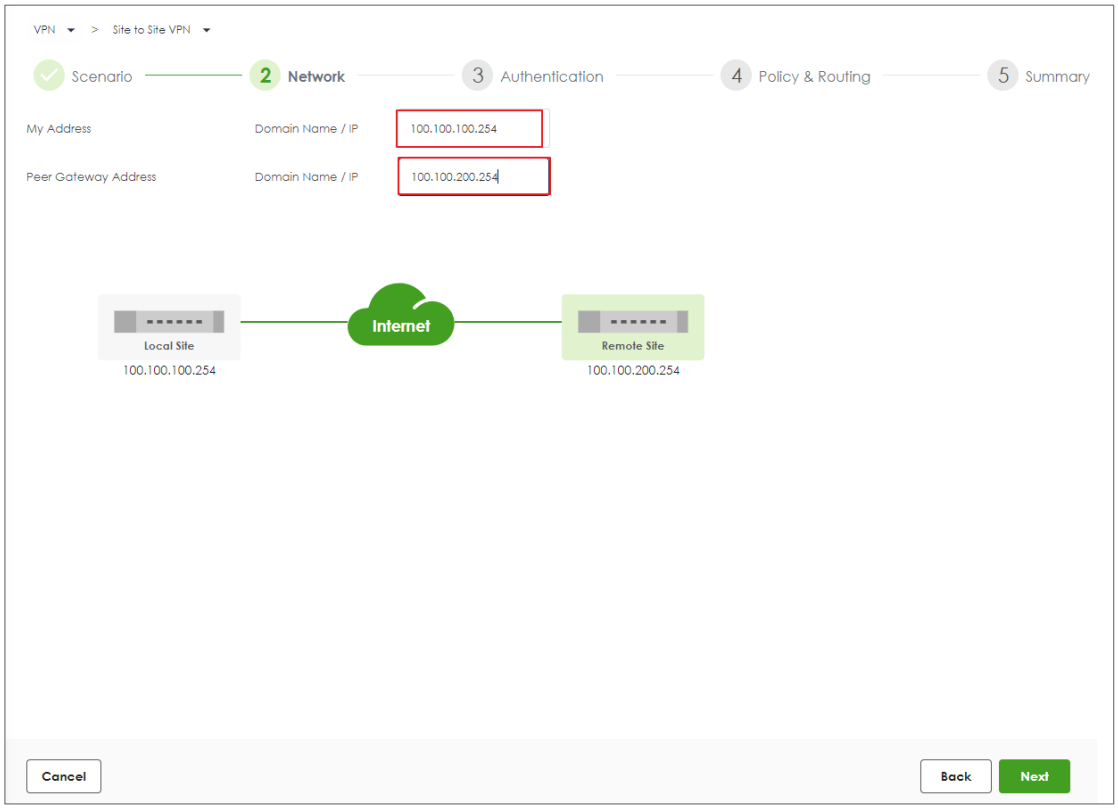
VPN > Site to Site VPN > Scenario

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



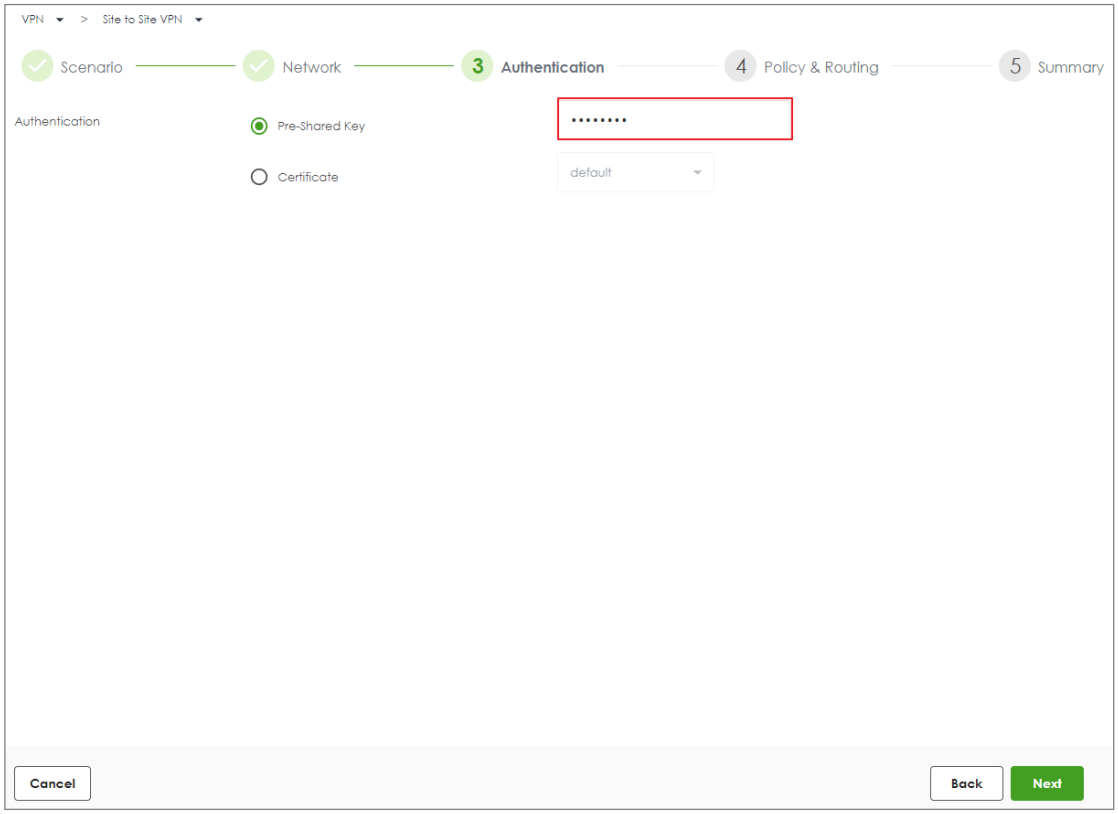
VPN > Site to Site VPN > Scenario > Network

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



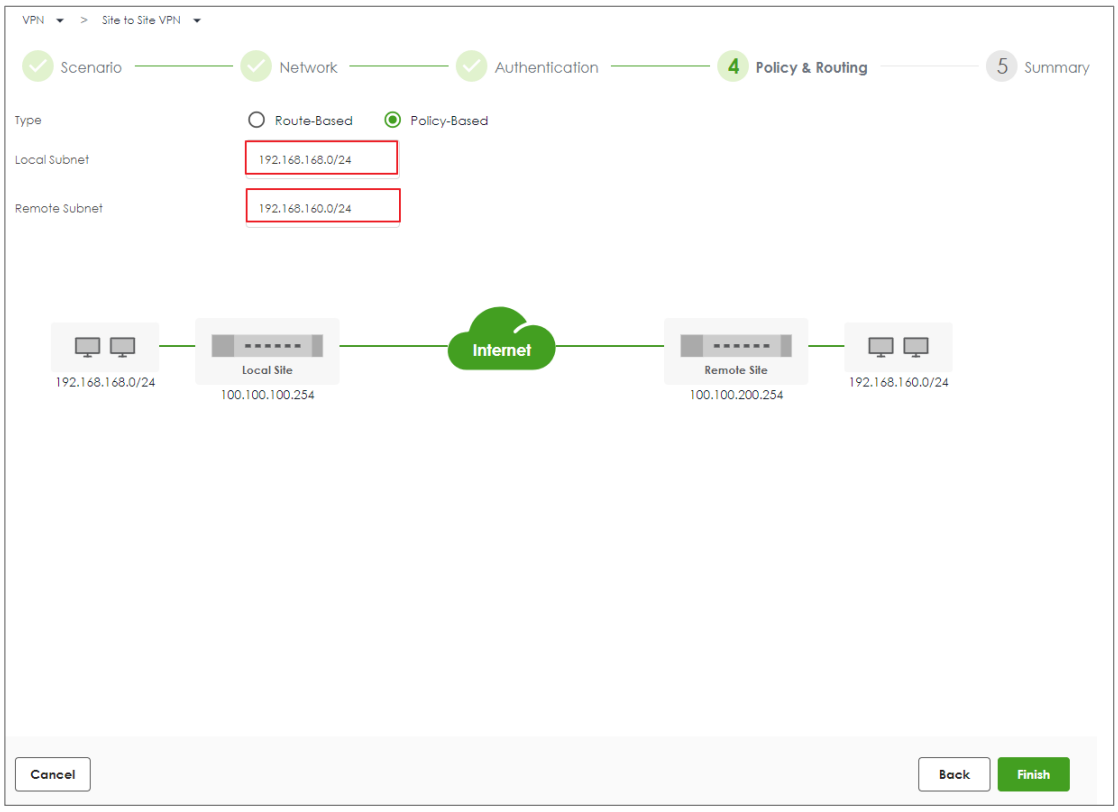
VPN > Site to Site VPN > Scenario > Network > Authentication

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



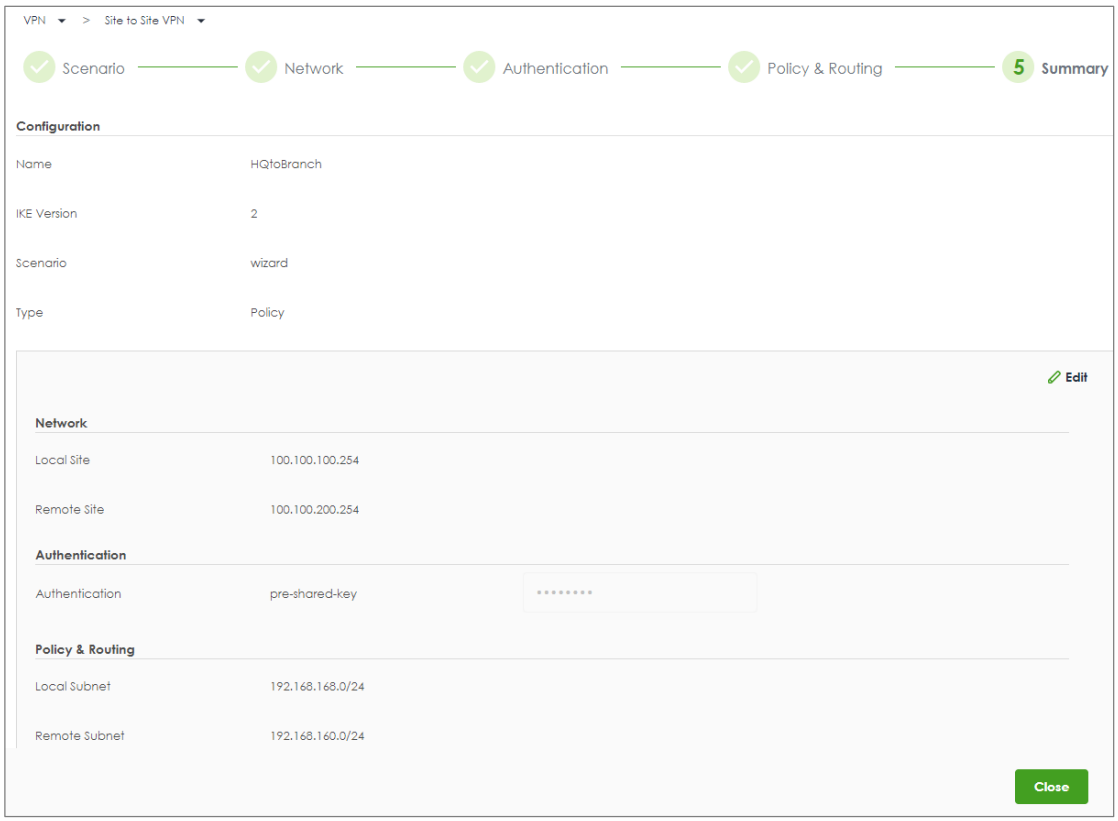
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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.



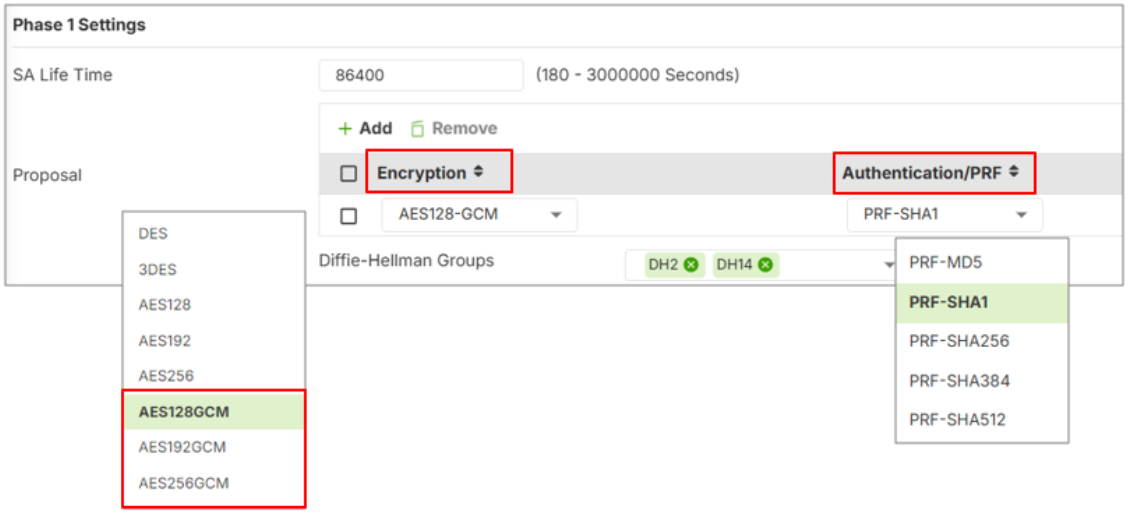
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

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

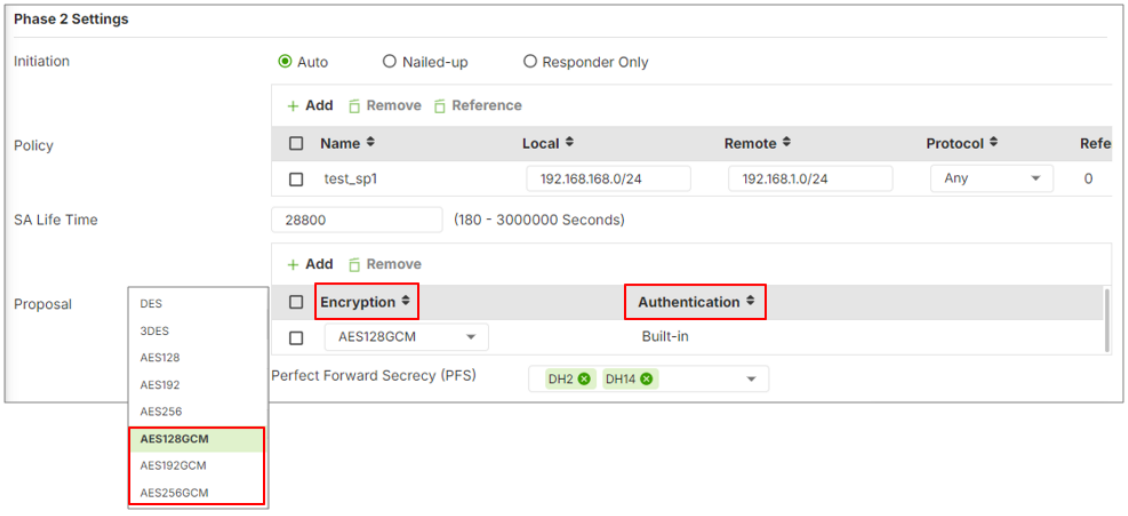


Note: Beginning with uOS 1.37, IKEv2 supports AES-GCM encryption.

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



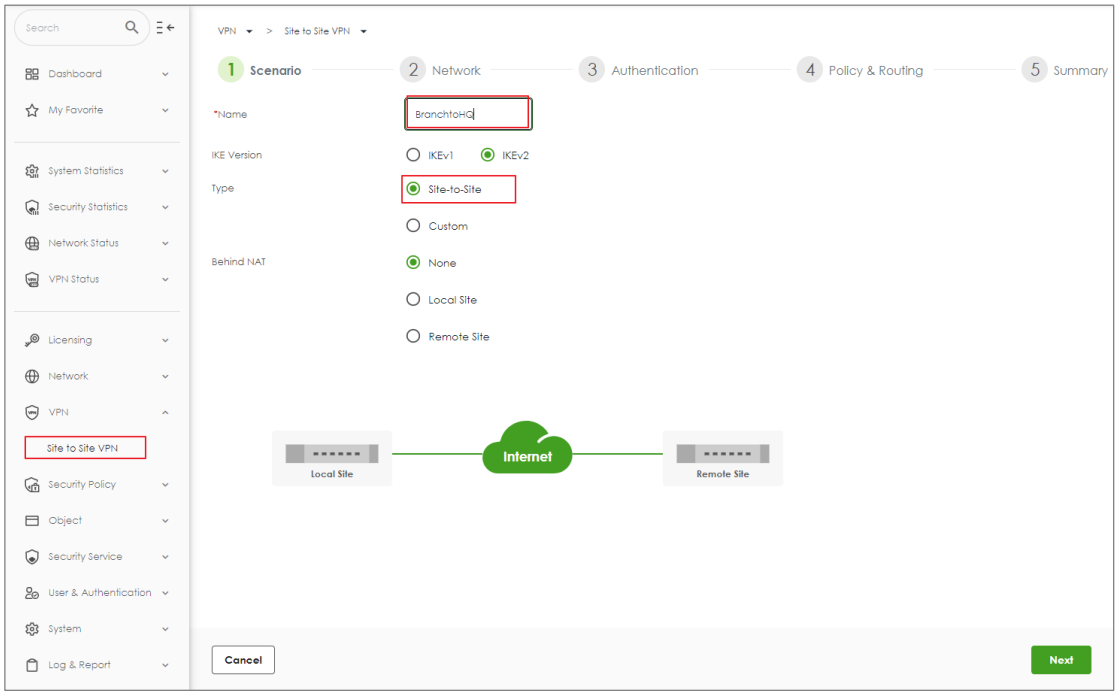
Phase 2 Settings - AES-GCM handles both encryption and authentication internally, so there is no additional integrity algorithm.



Set up IPSec VPN Tunnel for Branch

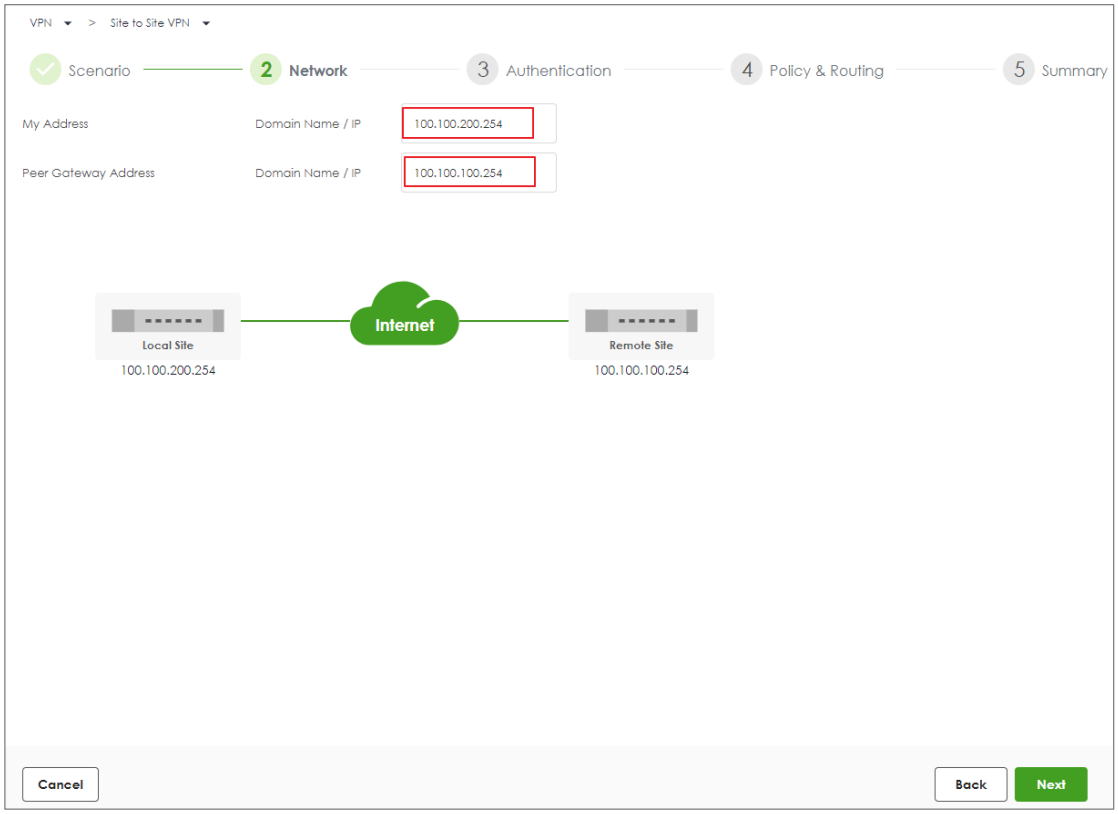
VPN > Site to Site VPN > Scenario

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



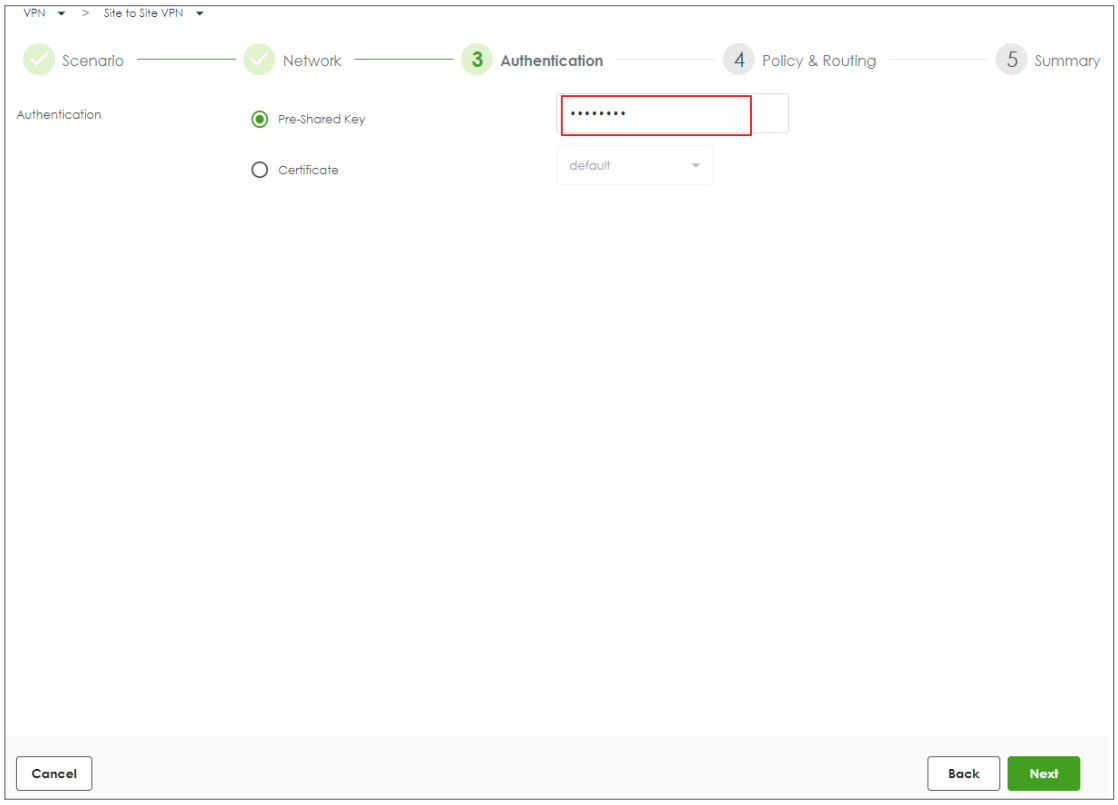
VPN > Site to Site VPN > Scenario > Network

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



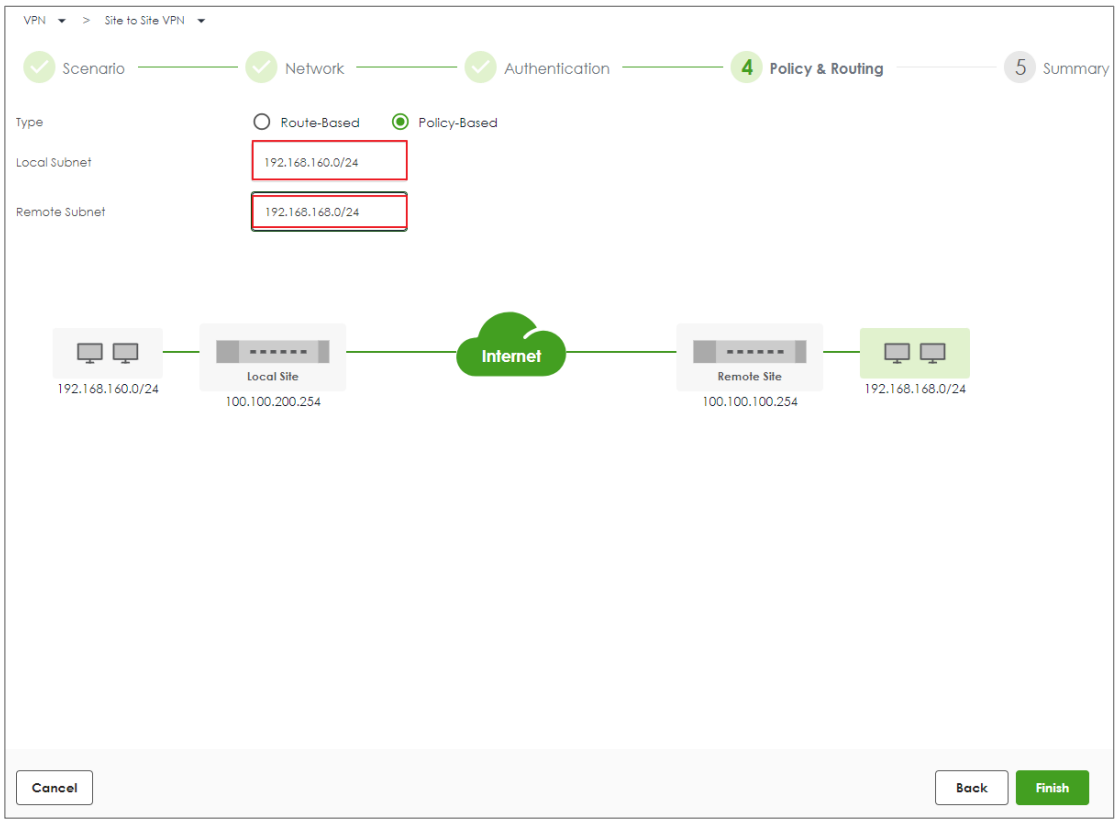
VPN > Site to Site VPN > Scenario > Network > Authentication

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



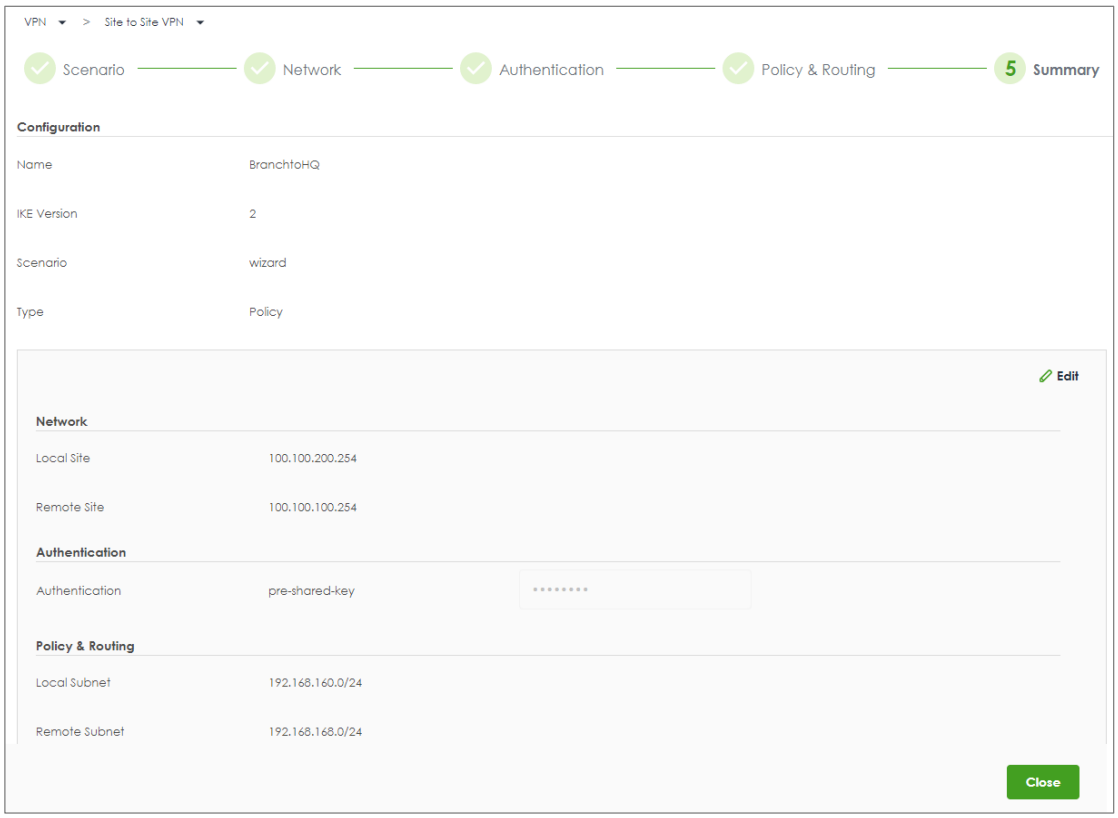
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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 > Policy & Routing > Summary

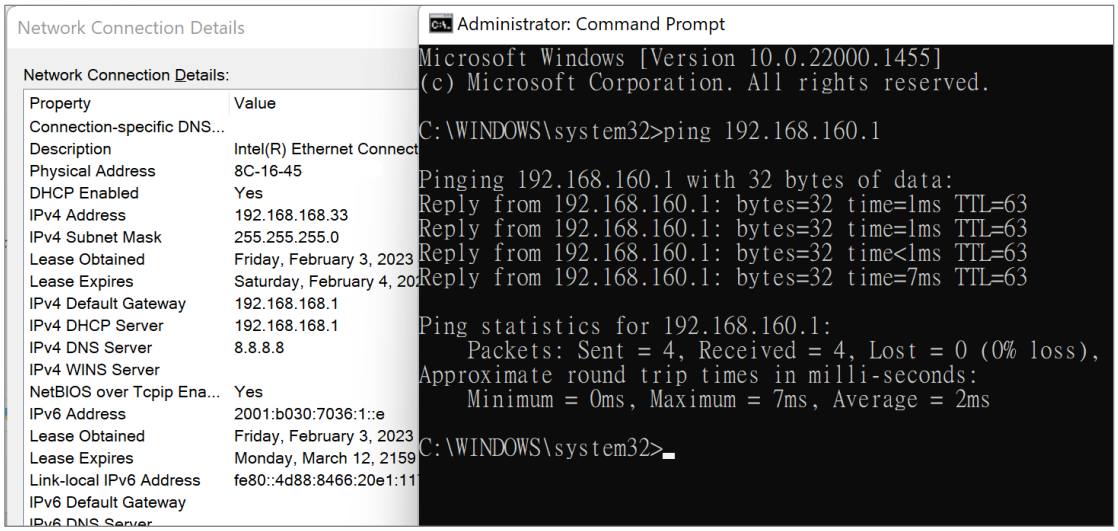
The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Test IPSec VPN Tunnel

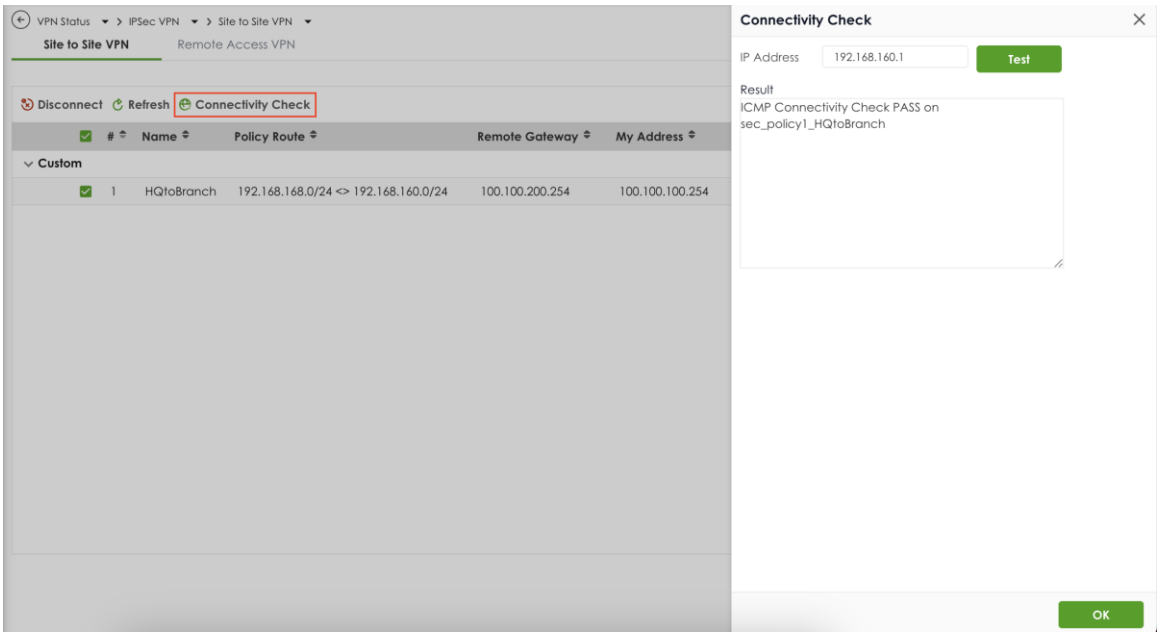
Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



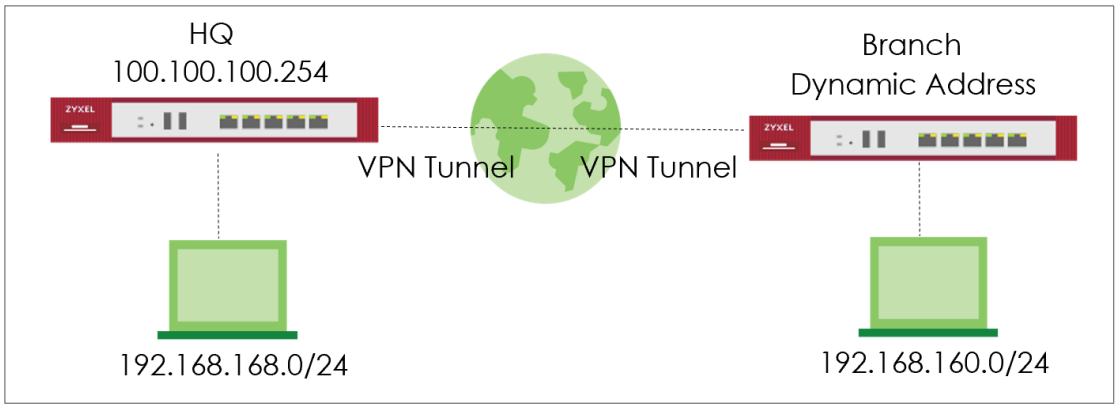
VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check



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

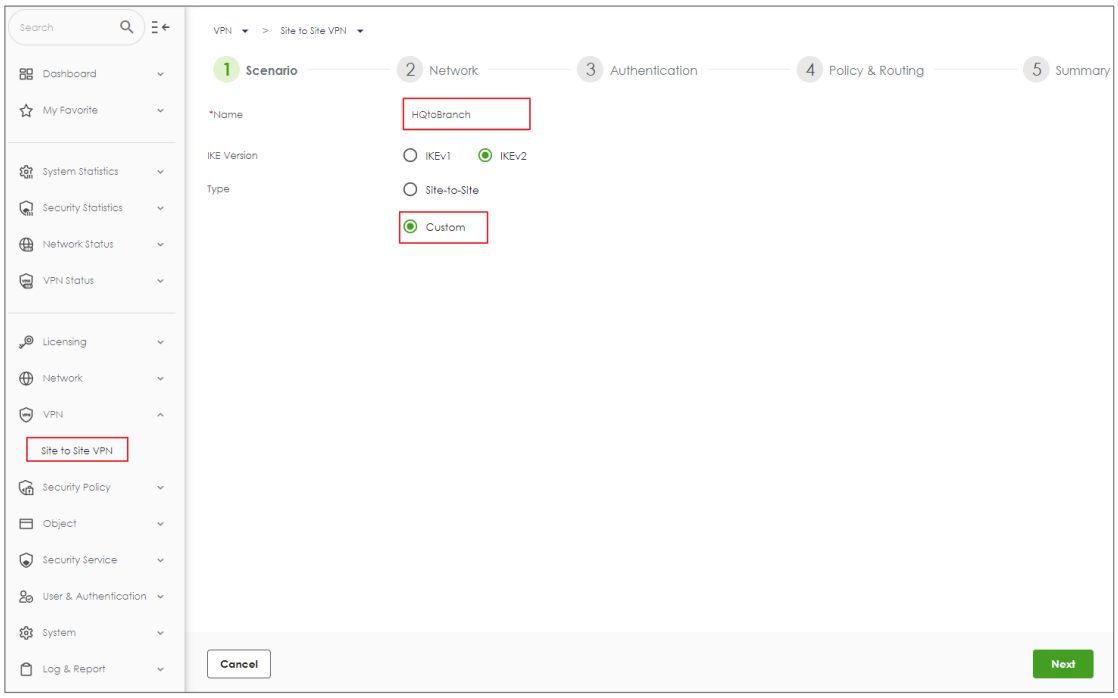
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

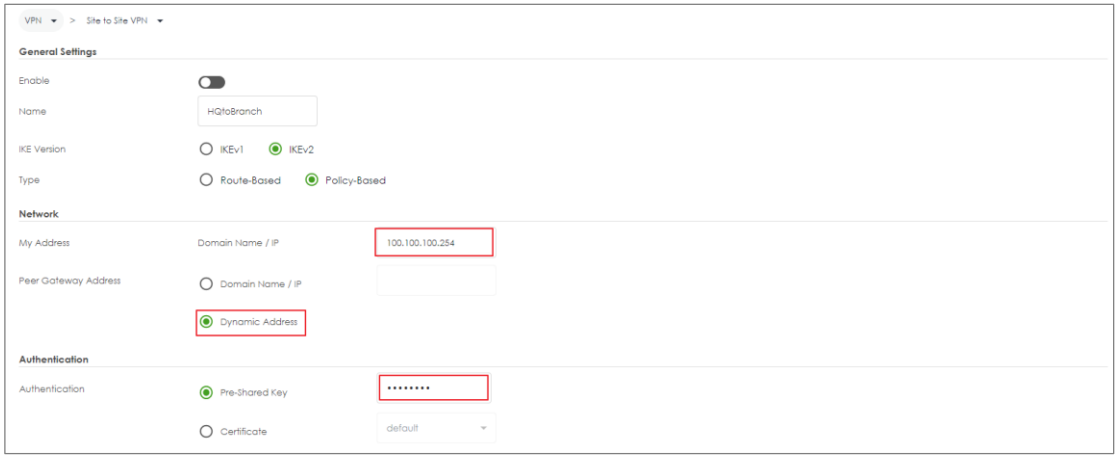
VPN > Site to Site VPN > Scenario

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

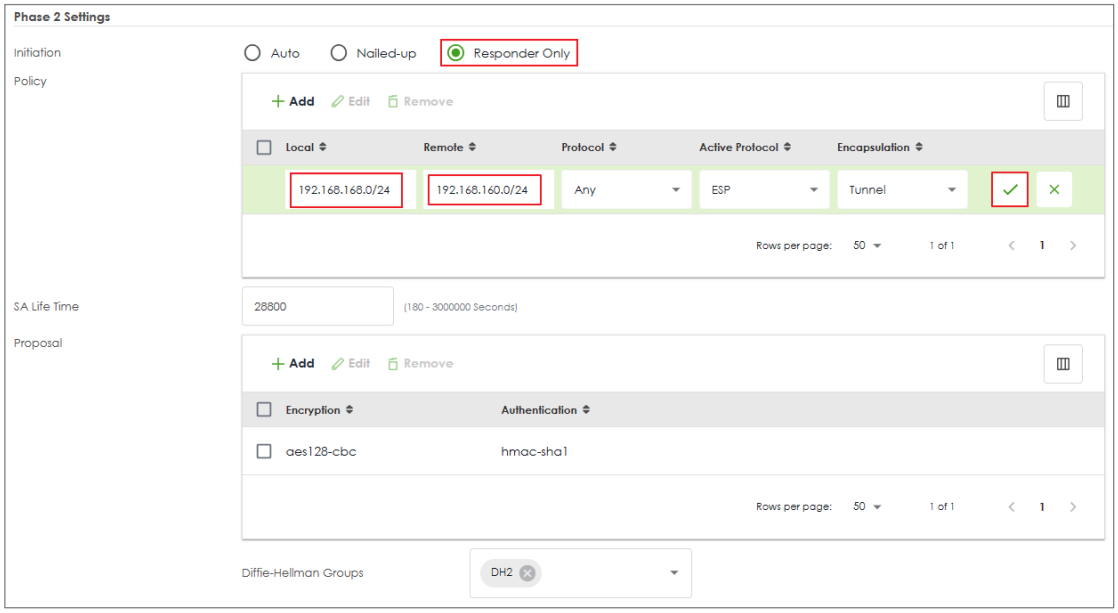


VPN > Site to Site VPN

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



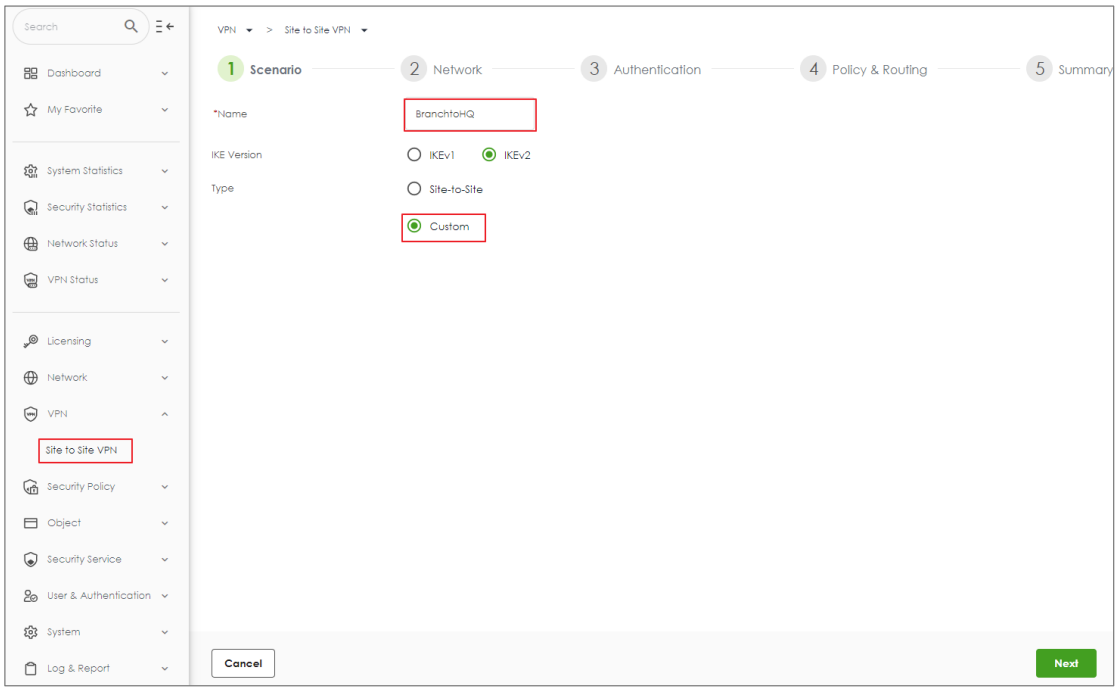
Scroll down to find the Phase2 setting. Type Local and Remote Subnet and select Responder Only. Then click save change.



Set up IPSec VPN Tunnel for Branch

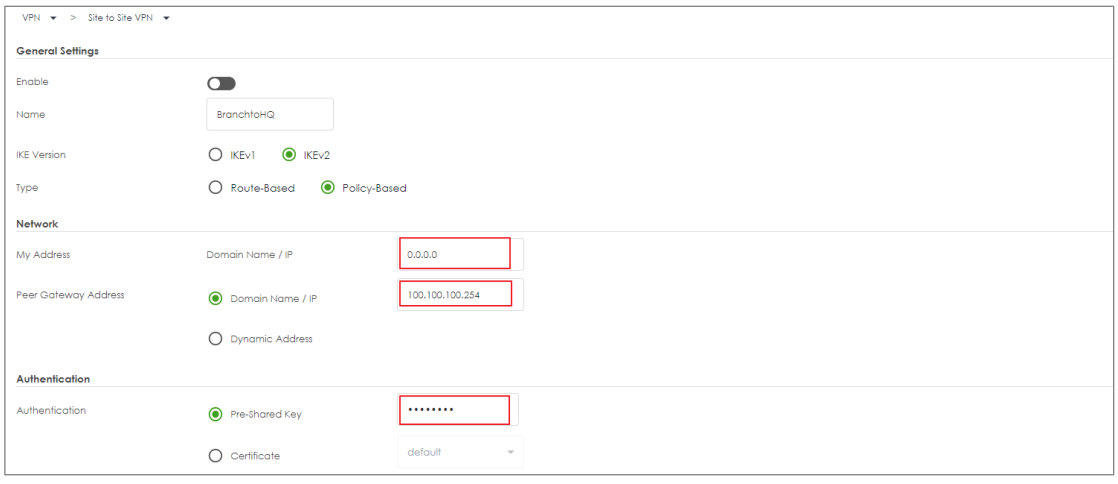
VPN > Site to Site VPN > Scenario

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

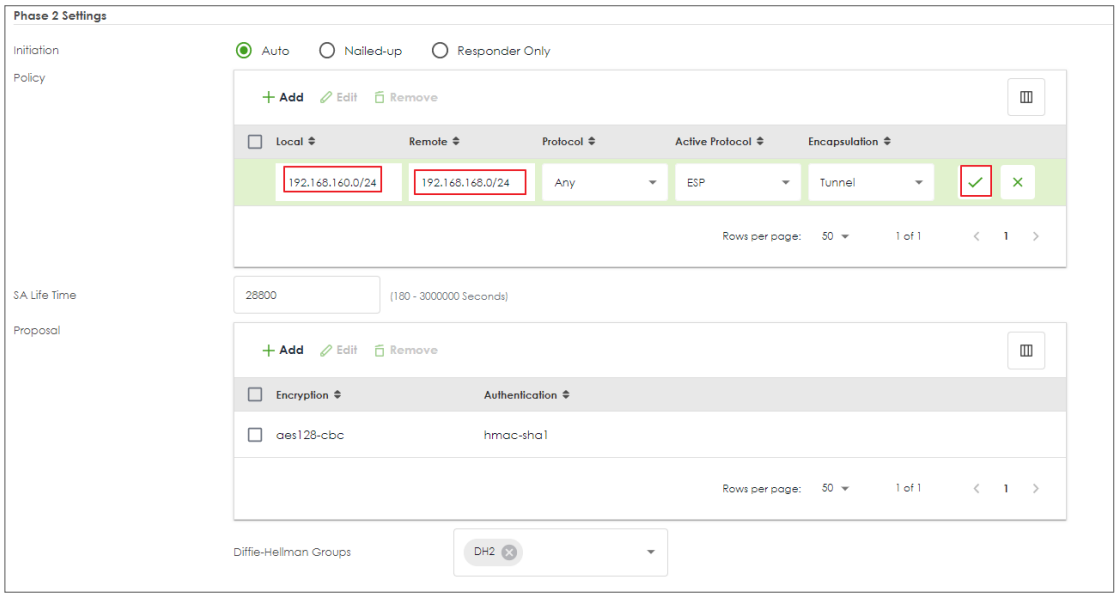


VPN > Site to Site VPN

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



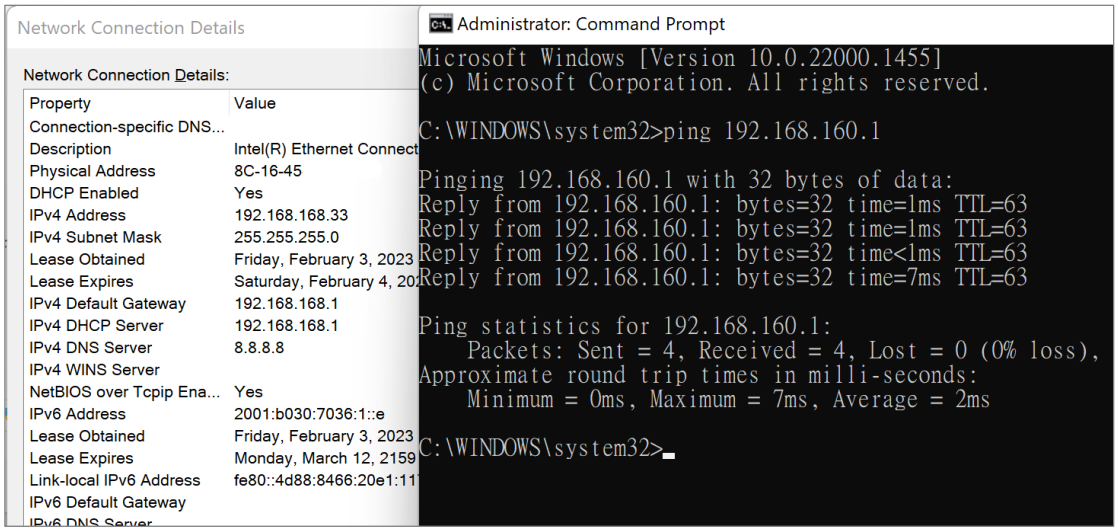
Scroll down to find the Phase2 setting, type Local and Remote Subnet. Then click save change.



Test IPSec VPN Tunnel

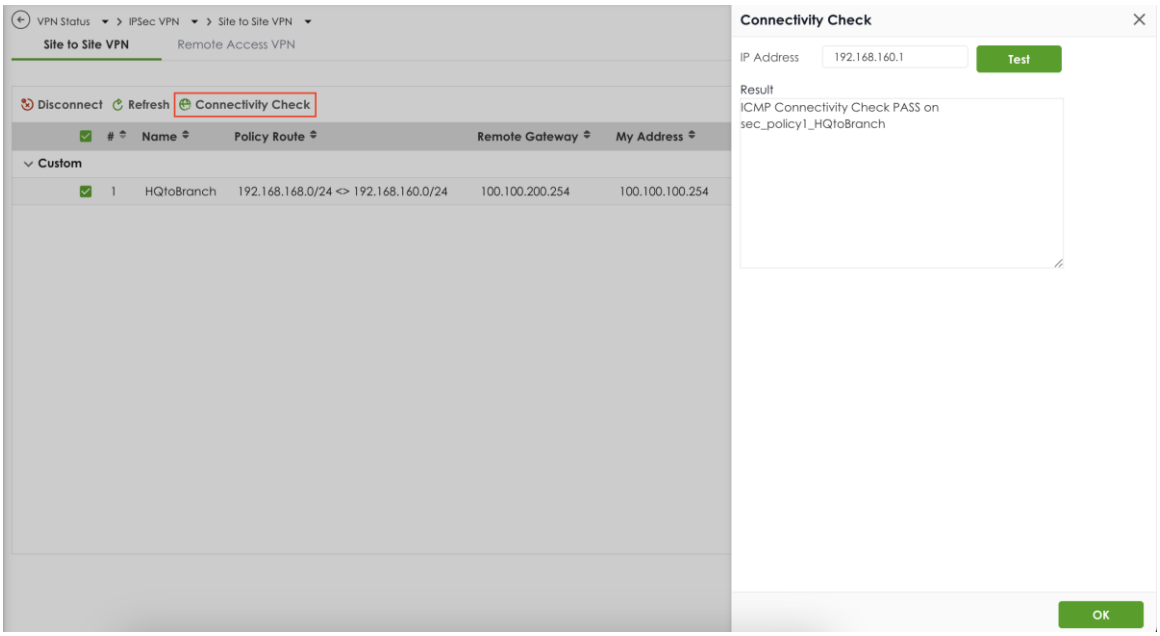
Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



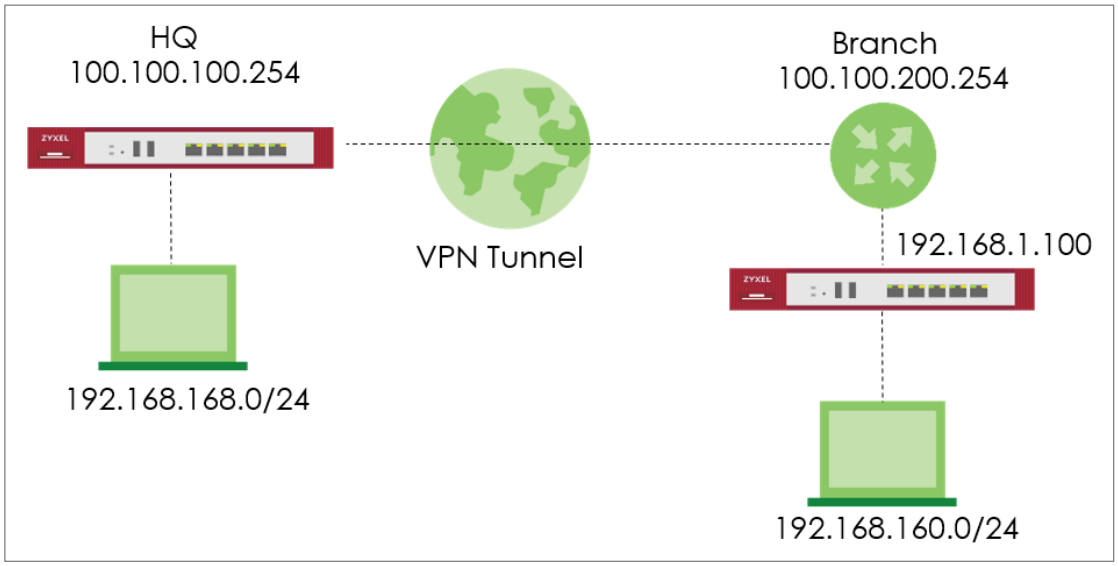
VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check



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.

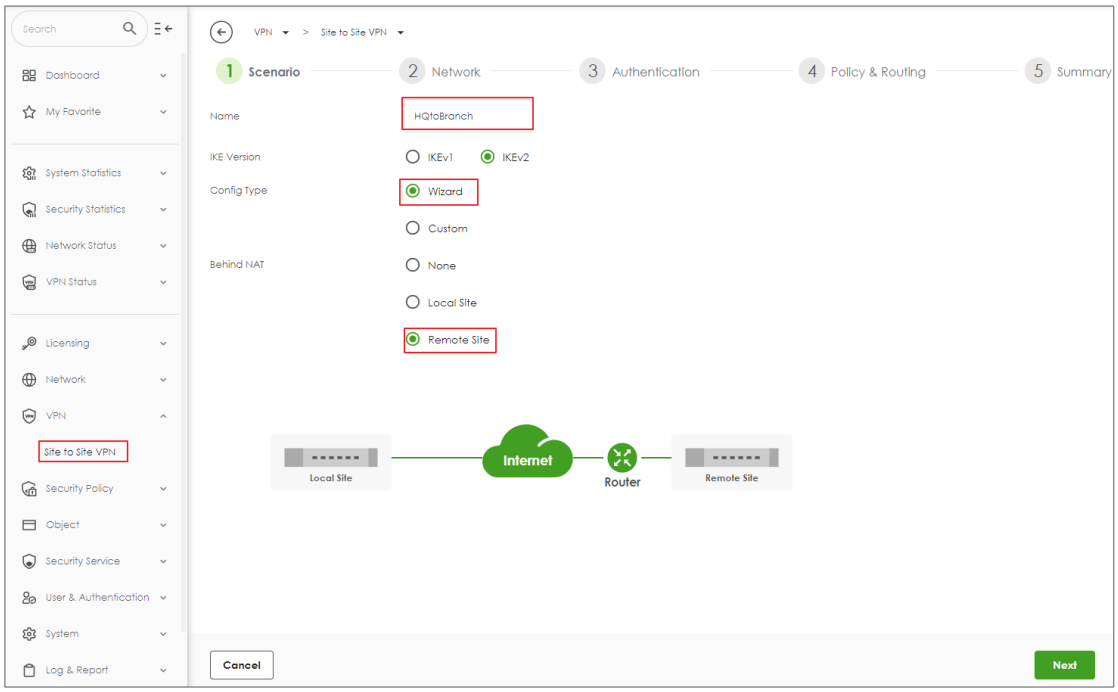


Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.

Set up IPSec VPN Tunnel for HQ

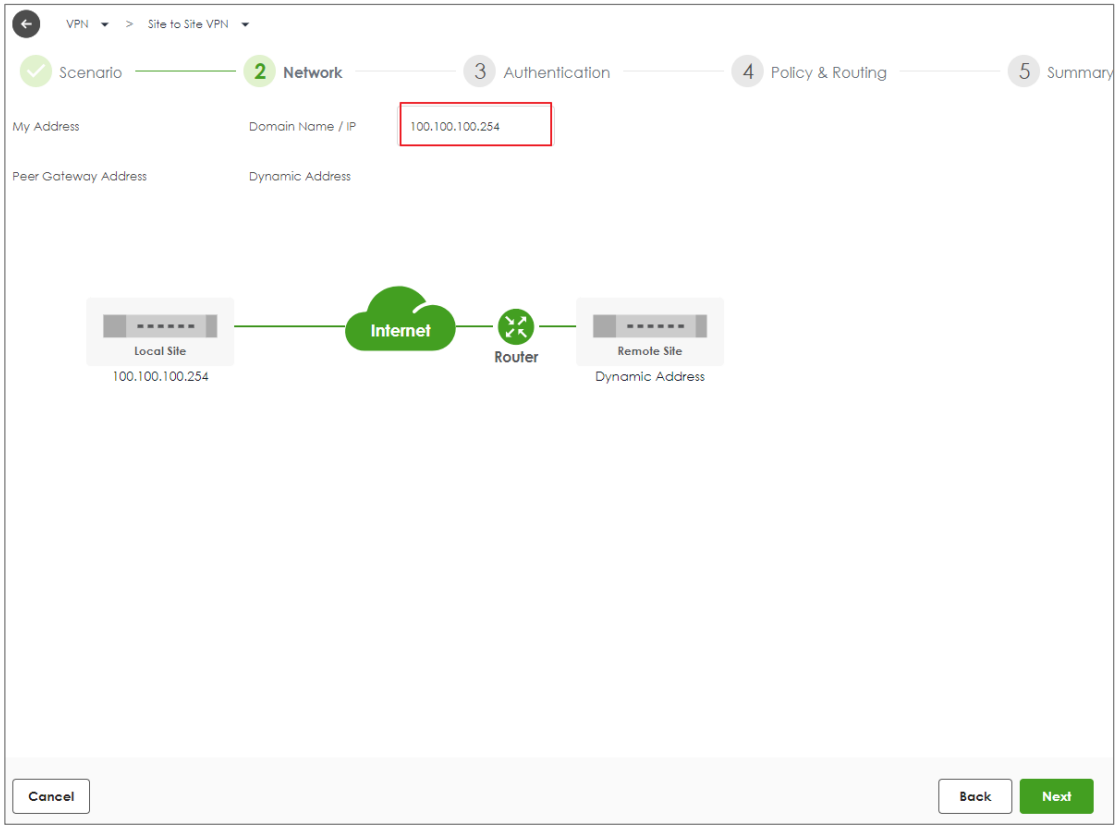
VPN > Site to Site VPN > Scenario

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



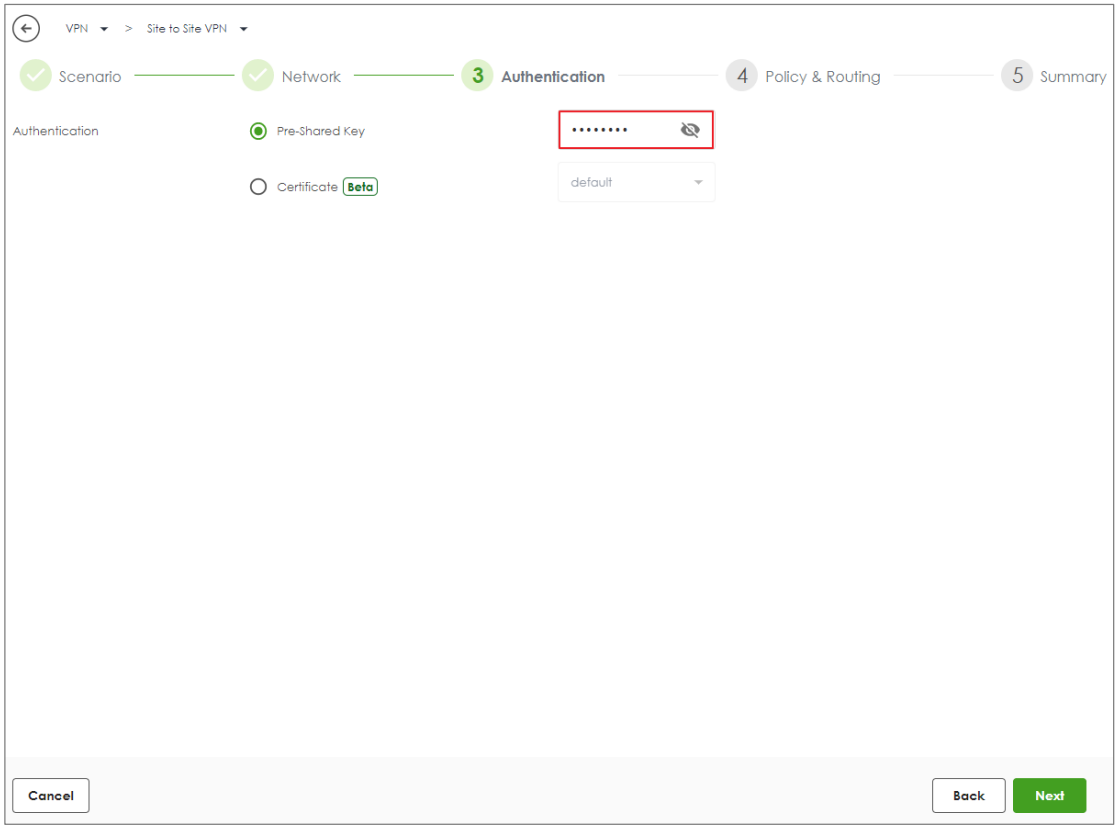
VPN > Site to Site VPN > Scenario > Network

Configure My Address. Click **Next.**



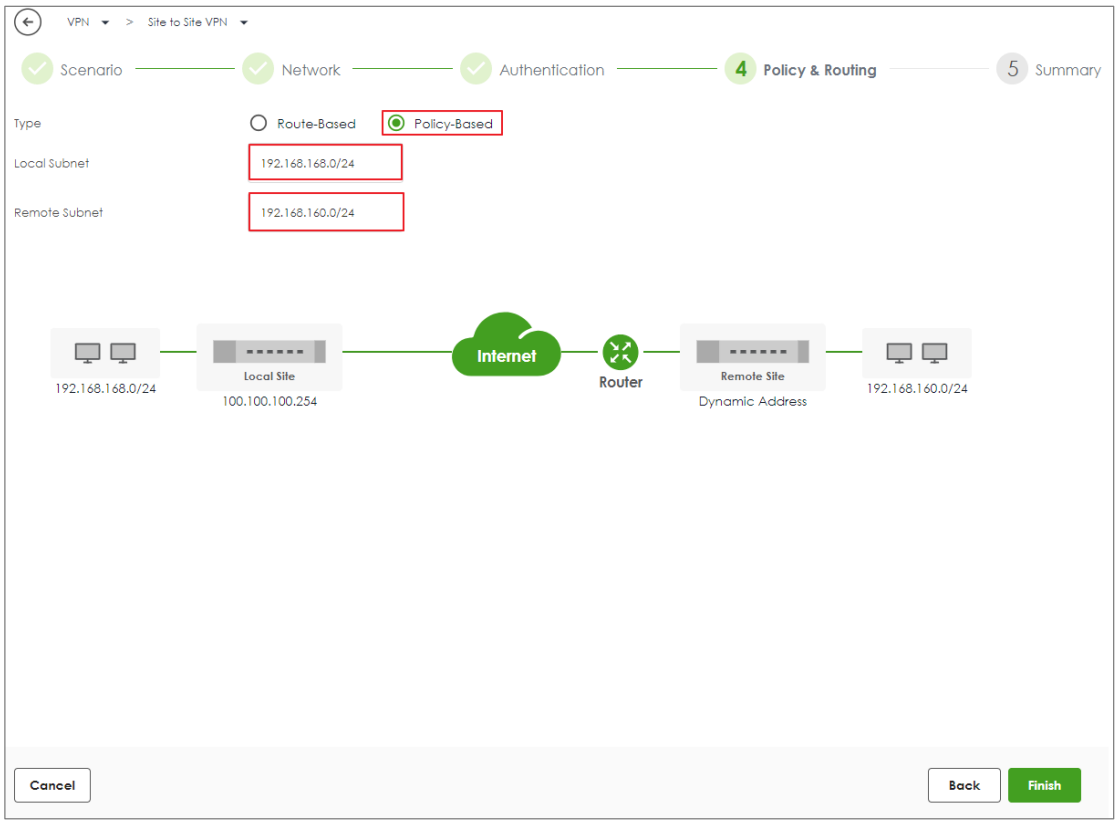
VPN > Site to Site VPN > Scenario > Network > Authentication

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



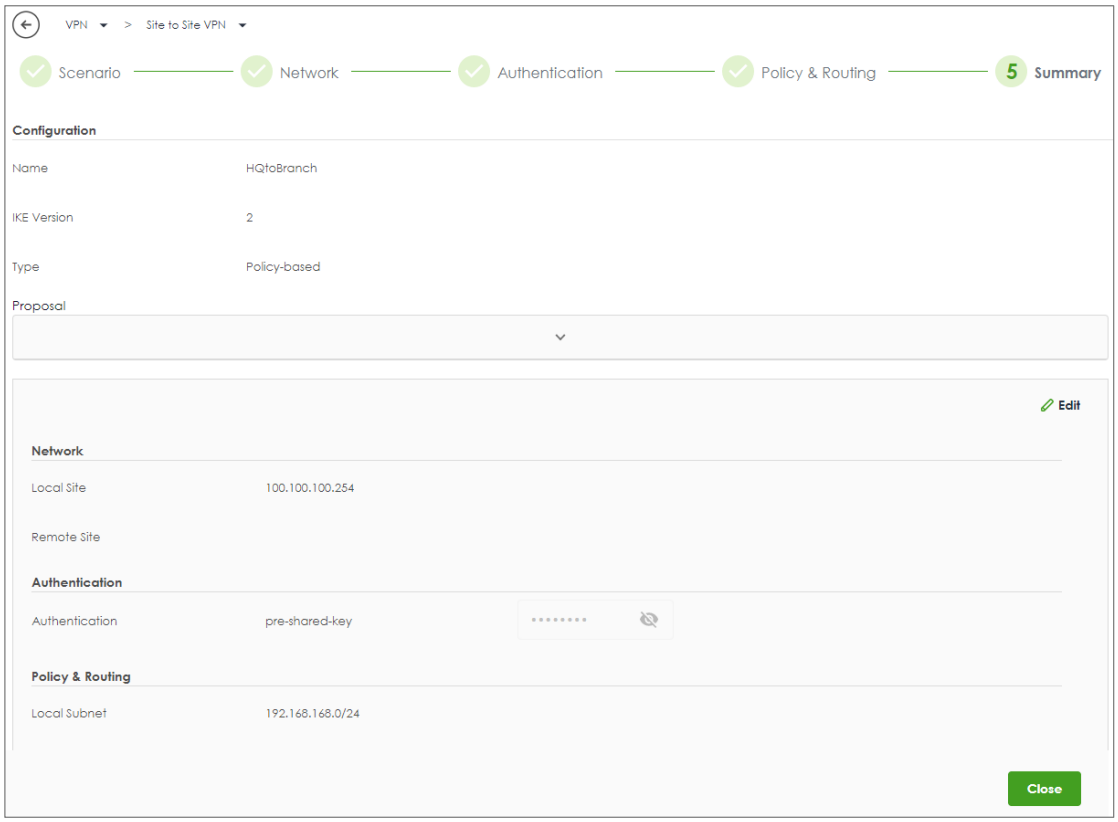
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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 > Policy & Routing > Summary

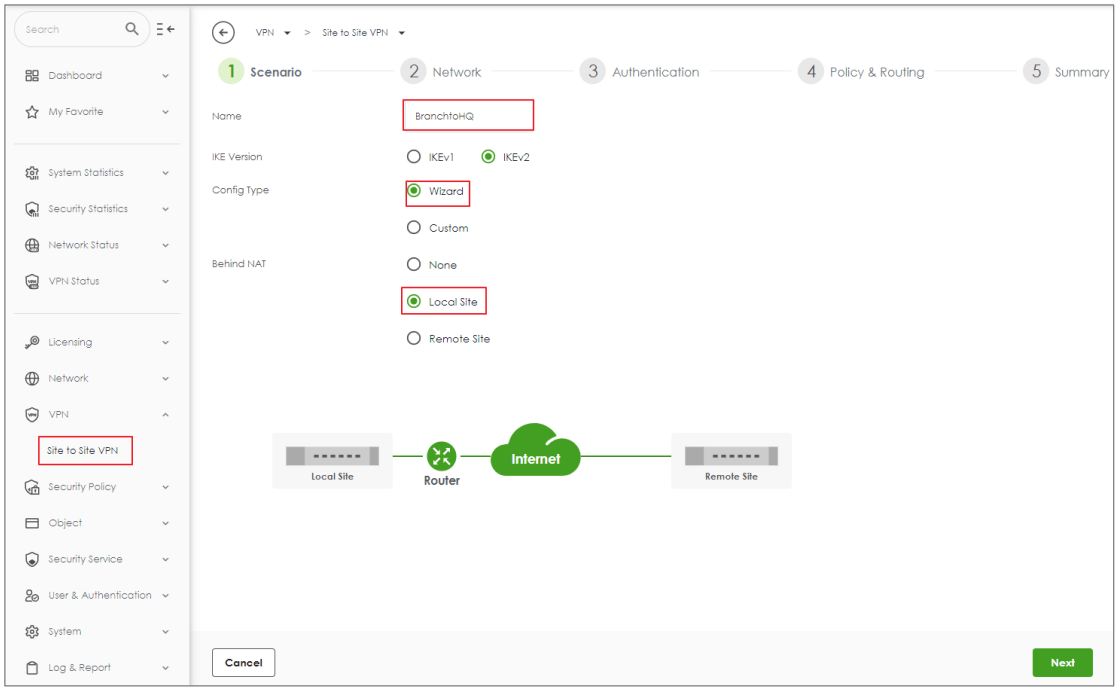
The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Set up IPSec VPN Tunnel for Branch

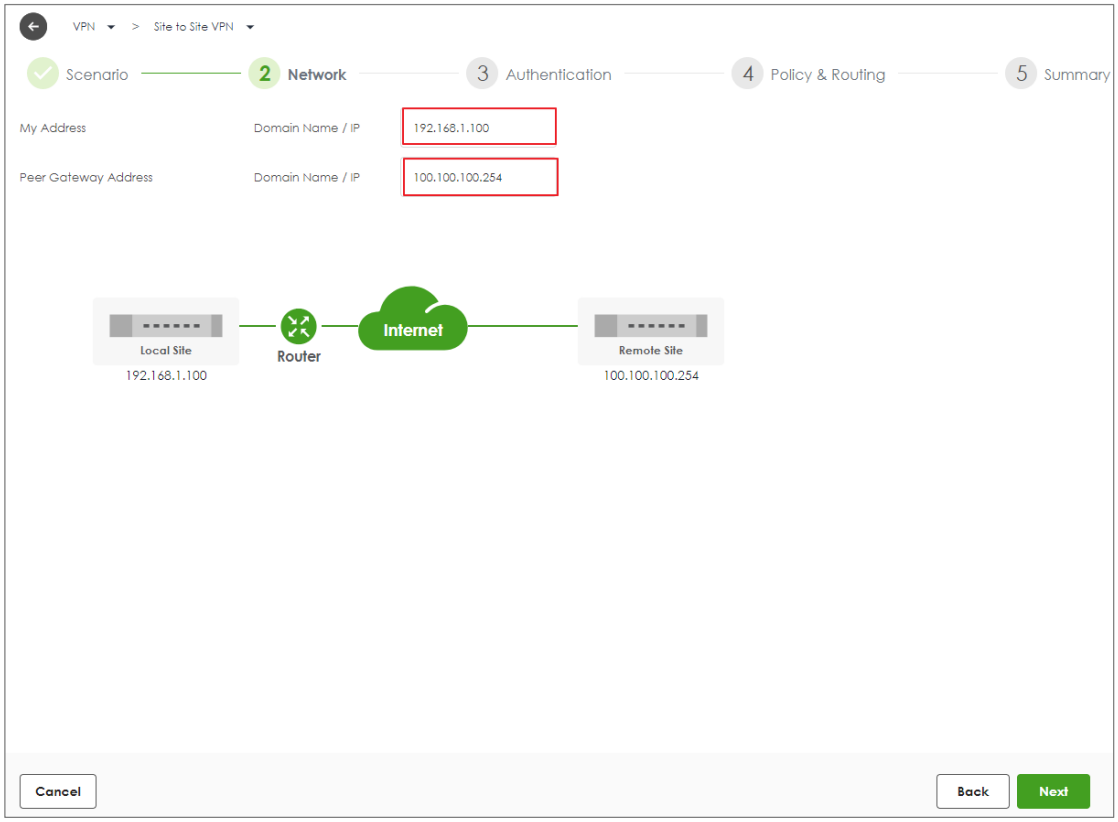
VPN > Site to Site VPN > Scenario

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



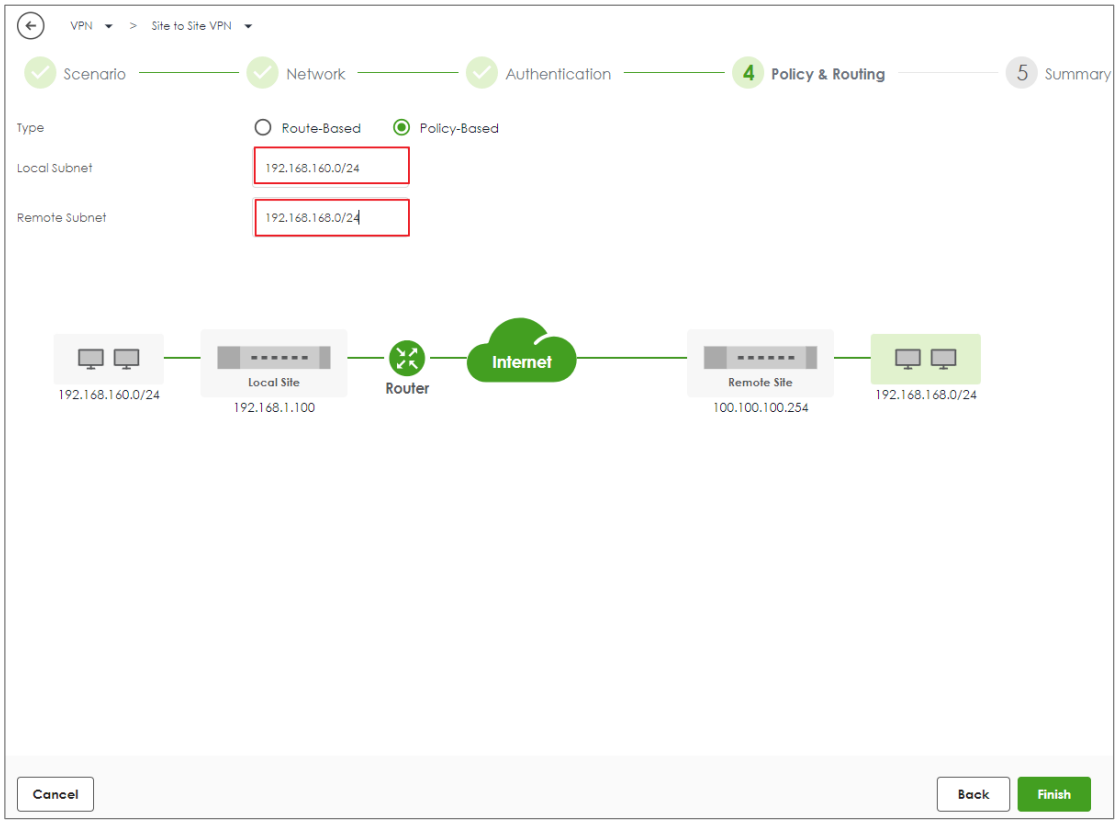
VPN > Site to Site VPN > Scenario > Network

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



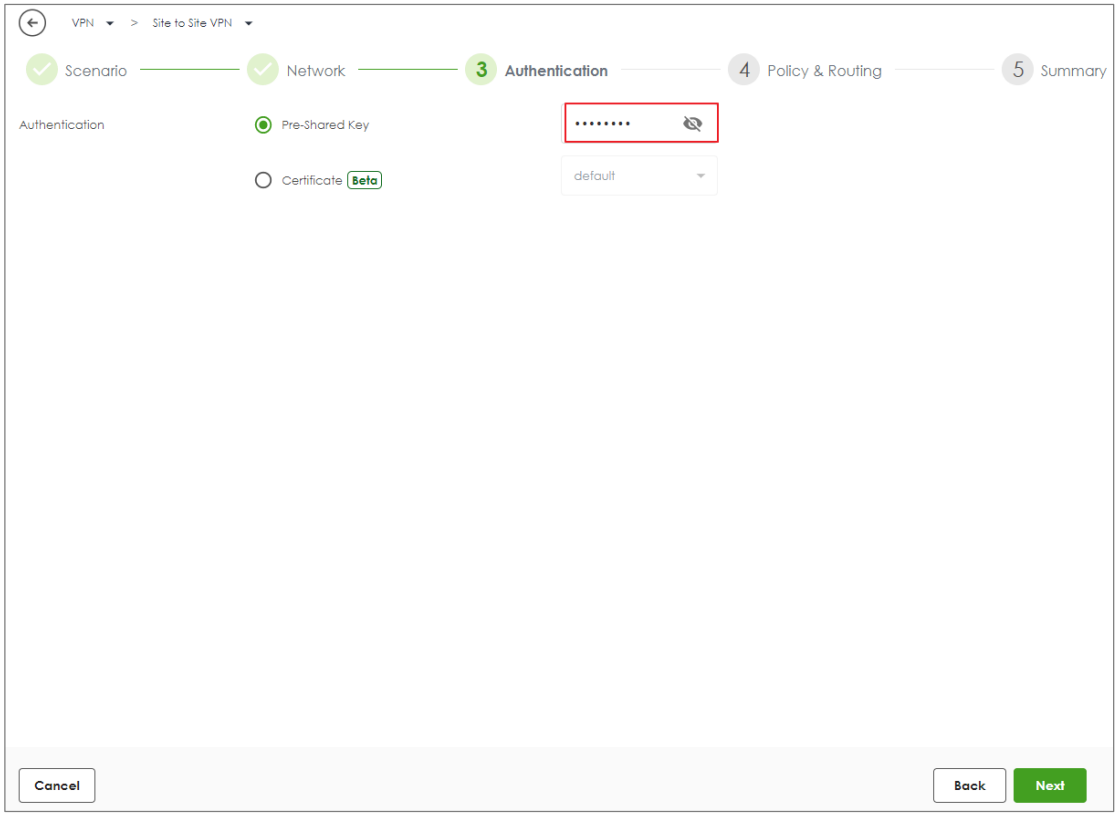
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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.



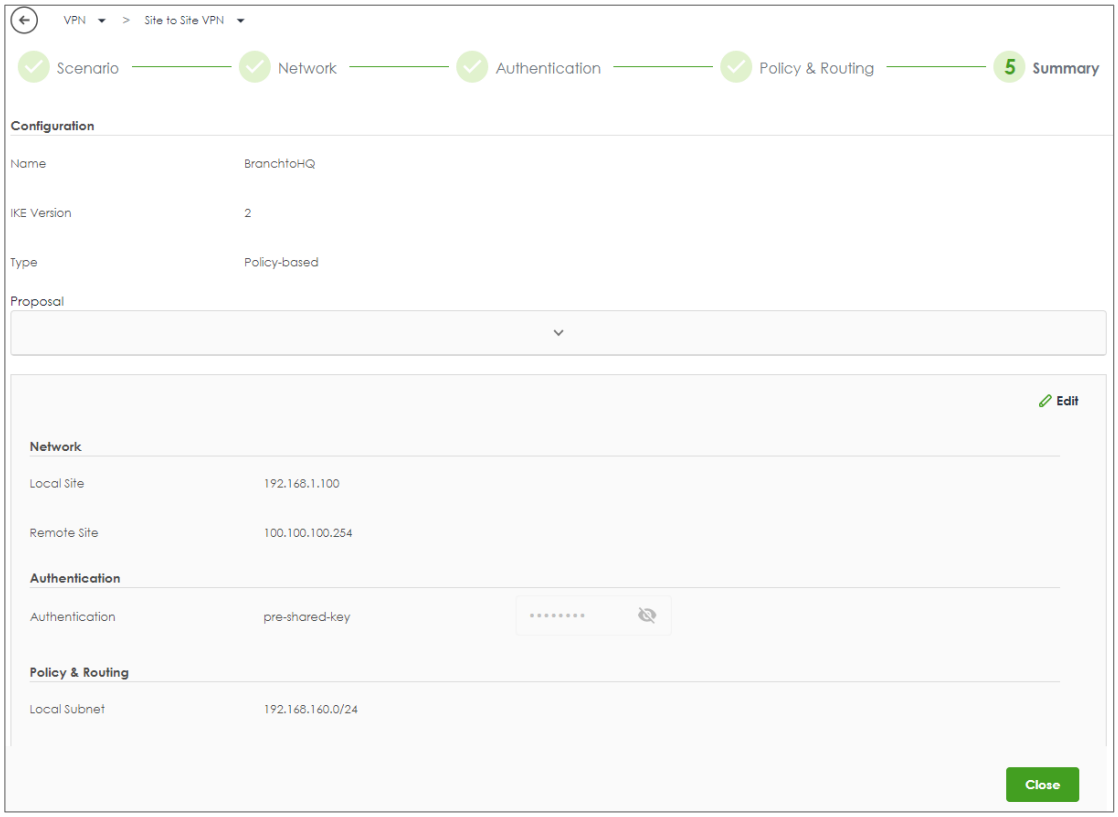
VPN > Site to Site VPN > Scenario > Network > Authentication

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



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

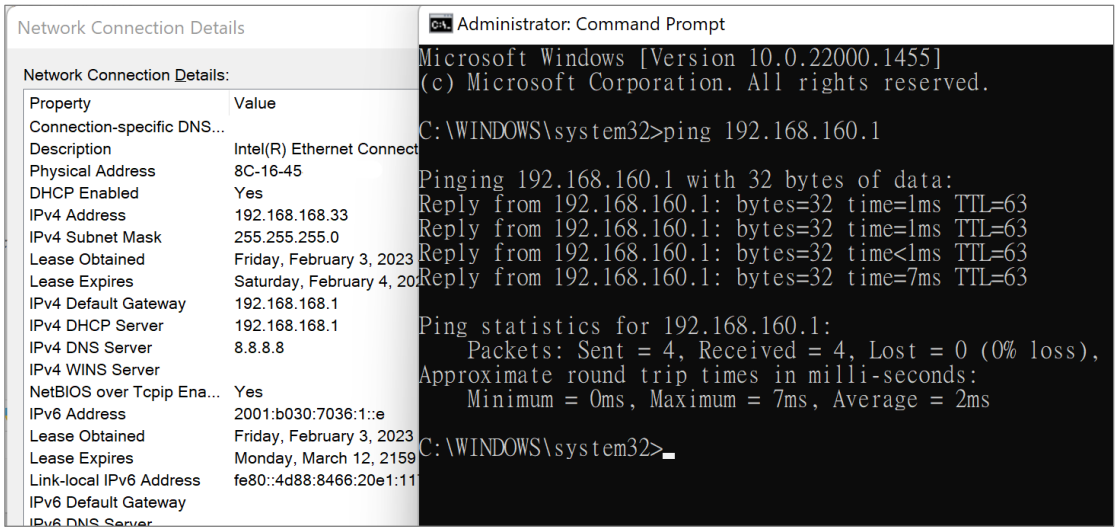
The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Test IPSec VPN Tunnel

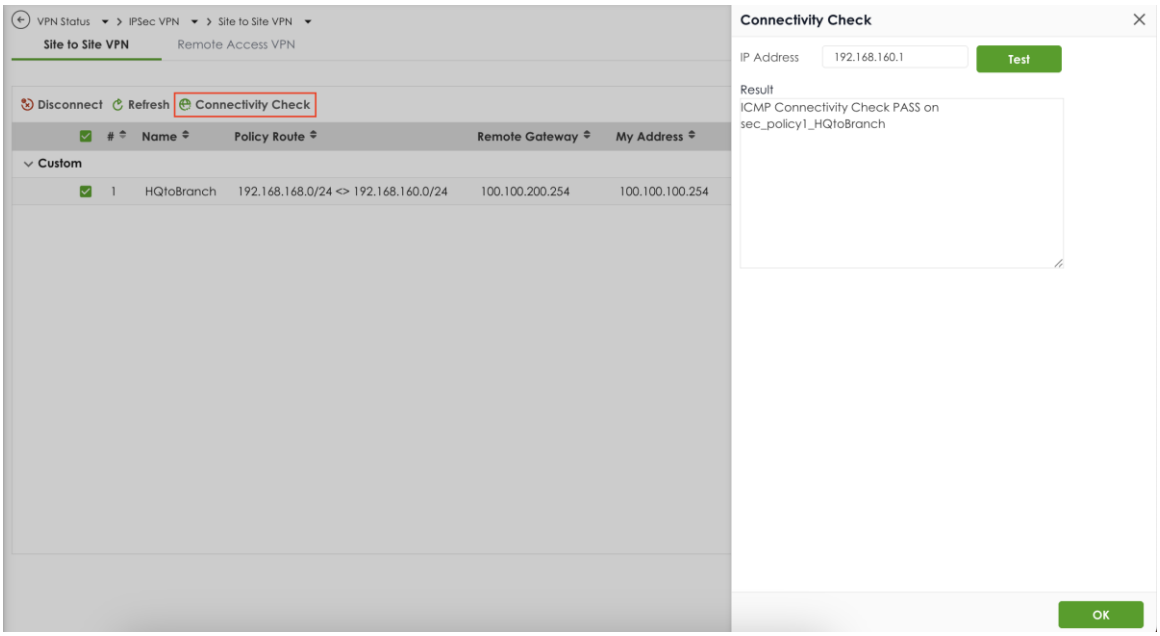
Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



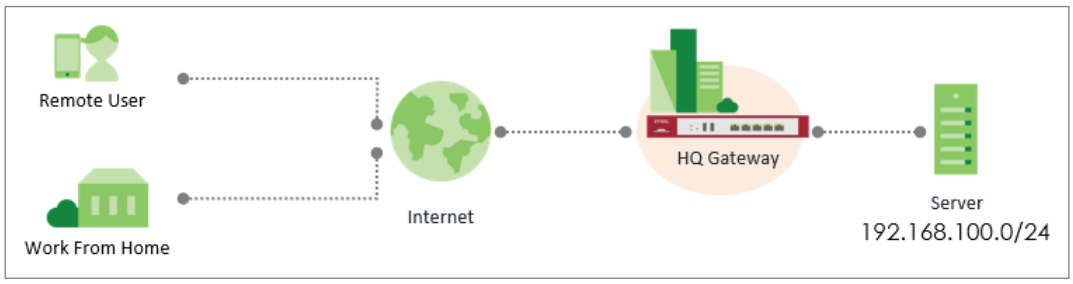
VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check



How to Configure Remote Access VPN with Zyxel VPN Client

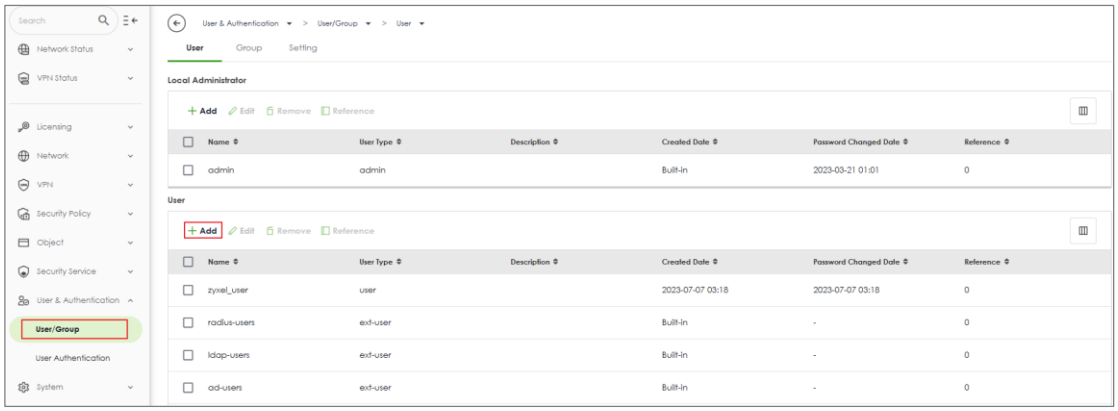
This example shows how to setup Remote Access VPN on USG FLEX H and Zyxel VPN Client. The example instructs how to implement Remote Access VPN by SSL VPN and IPSec VPN.

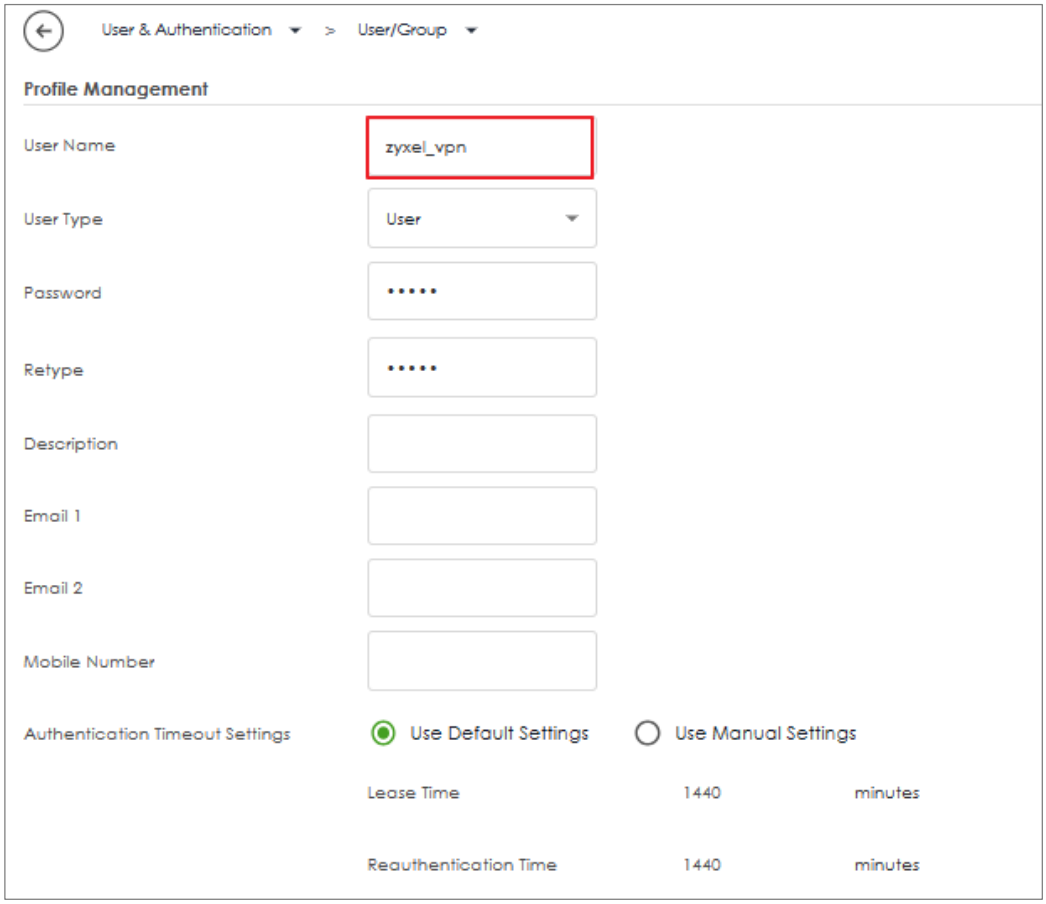


Before Begin

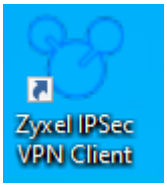
User & Authentication > User/Group > User

Create local user for remote access authentication.





Download and install the new TGB Client

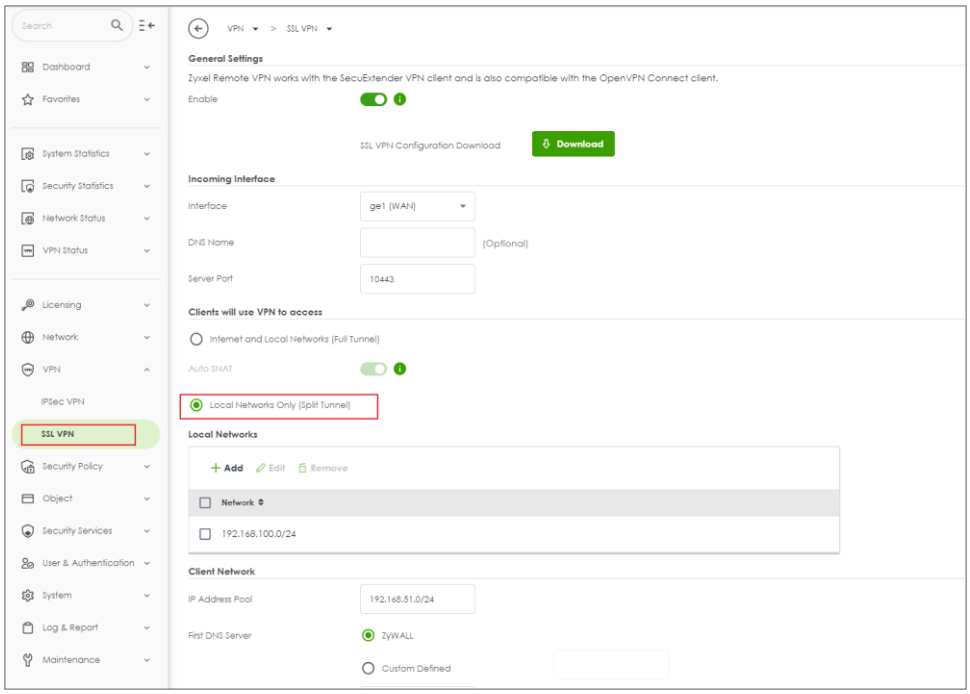


Set up SSL VPN

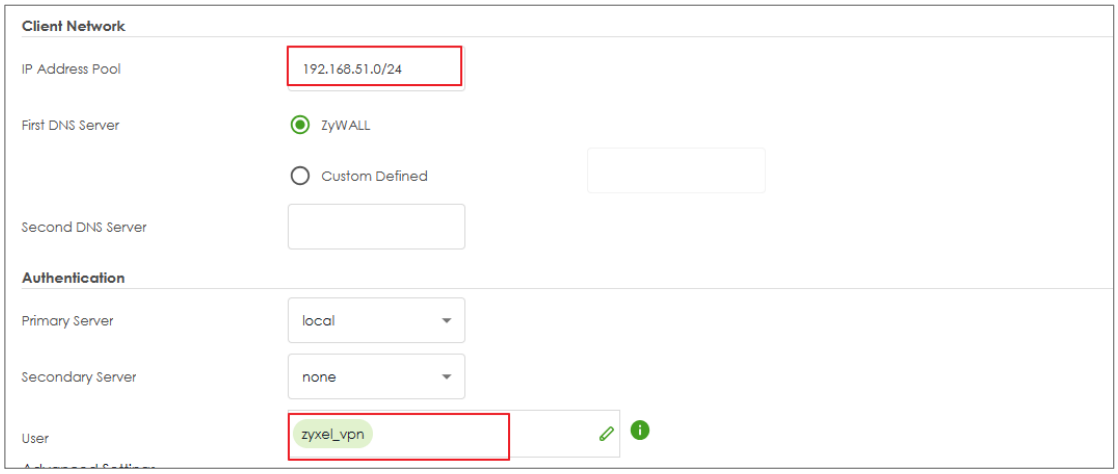
VPN > SSL VPN

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

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



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

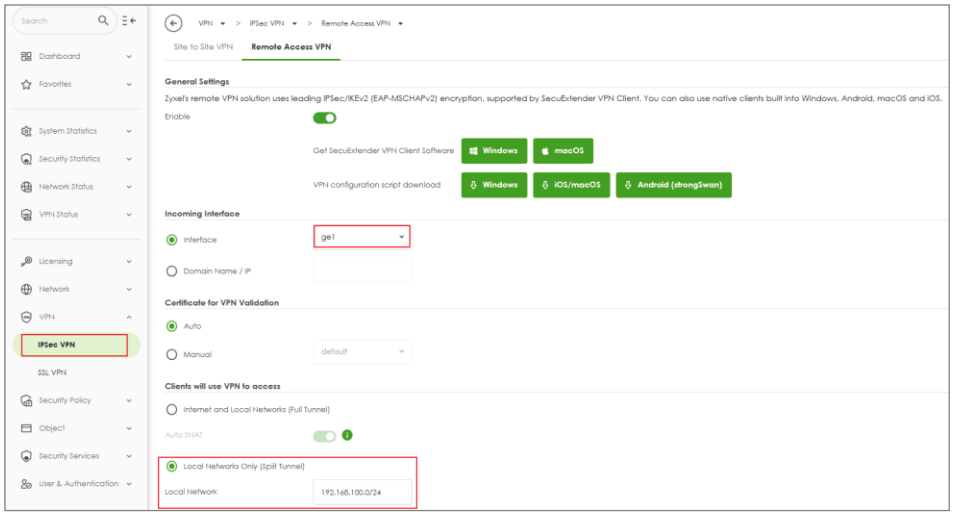


Set up IKEv2 VPN

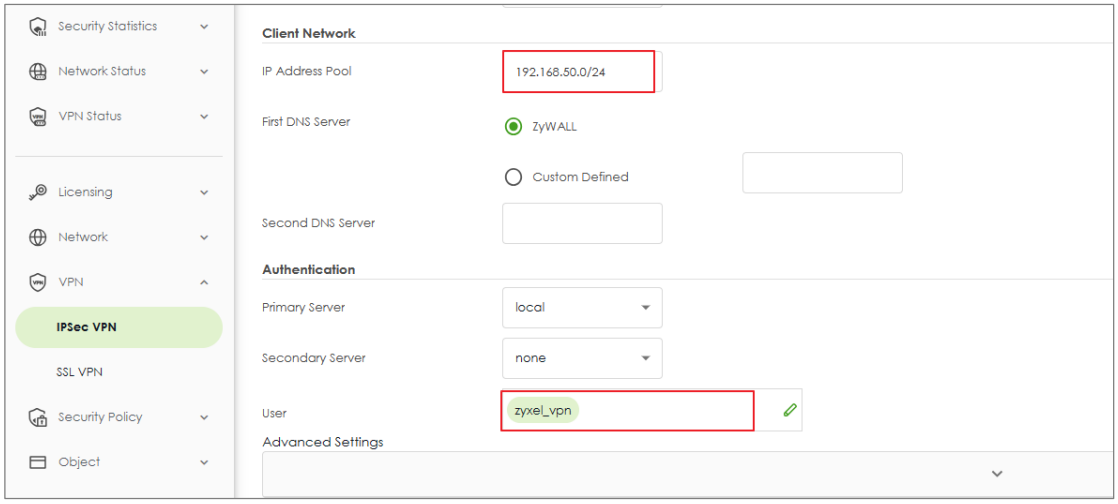
VPN > IPSec VPN > Remote Access VPN

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

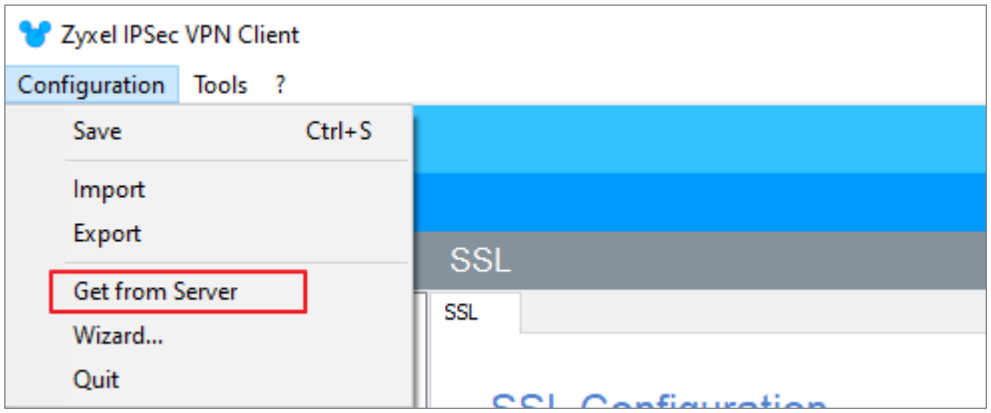


The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.

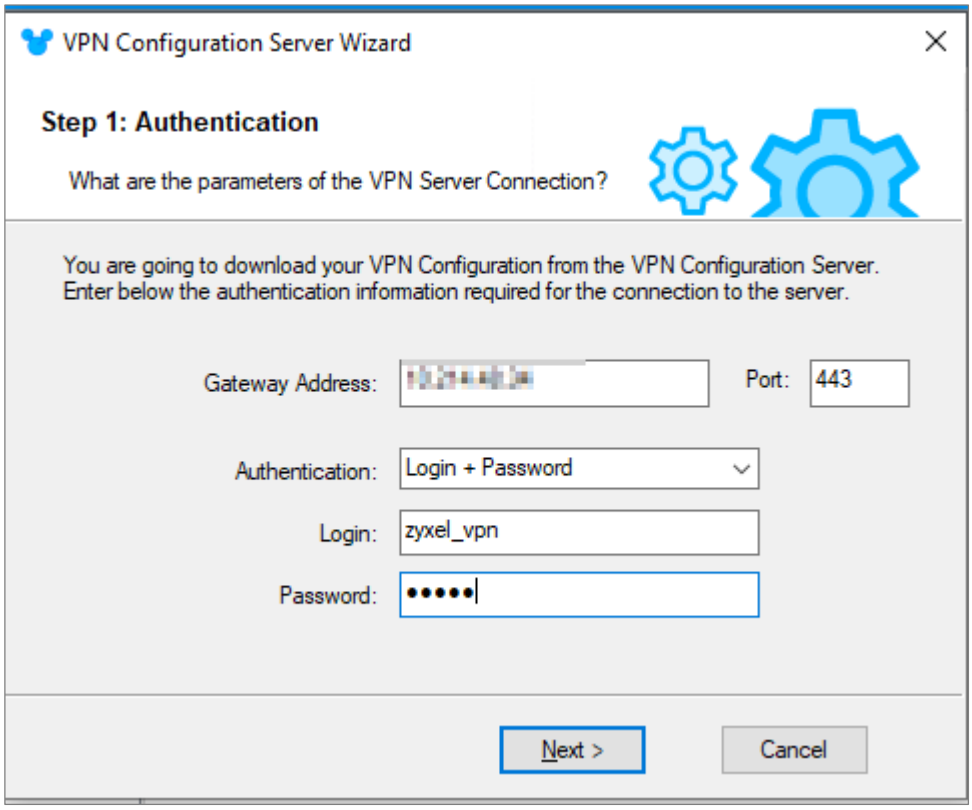


Set up Remote Access on TGB Client

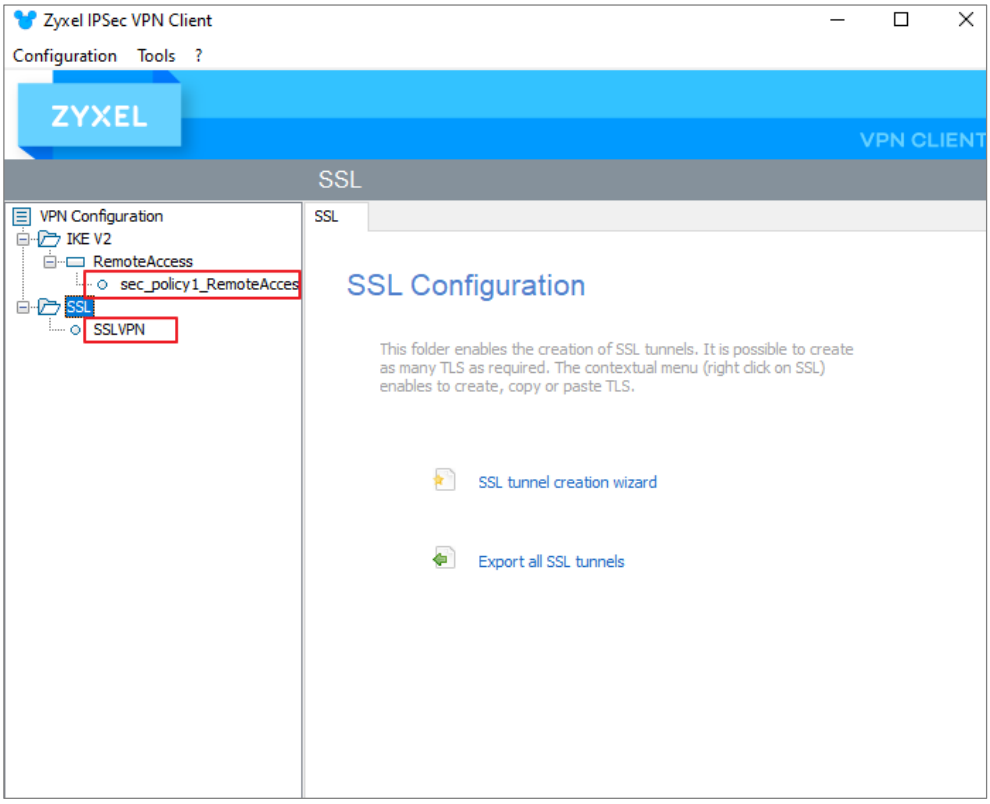
The new TGB Client merge SSL VPN and IKEv2 VPN. You don't need additional software for each other.



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



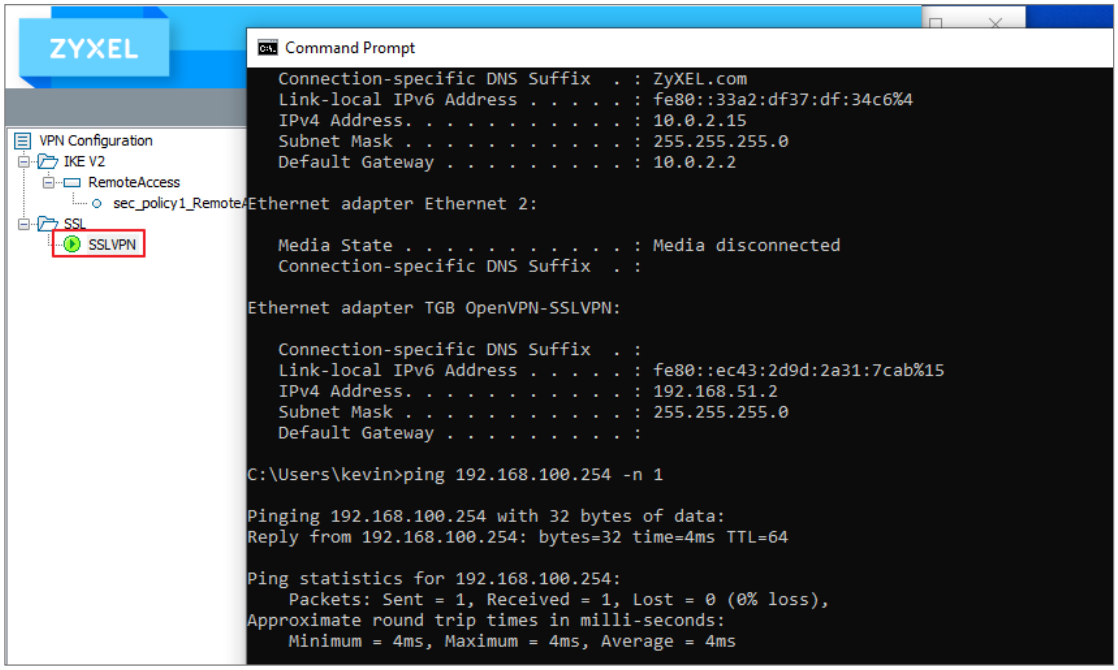
You will obtain IKEv2 as well as SSLVPN settings.



Test SSLVPN Tunnel on TGB Client

Right click the profile and “Open Tunnel” and log in.

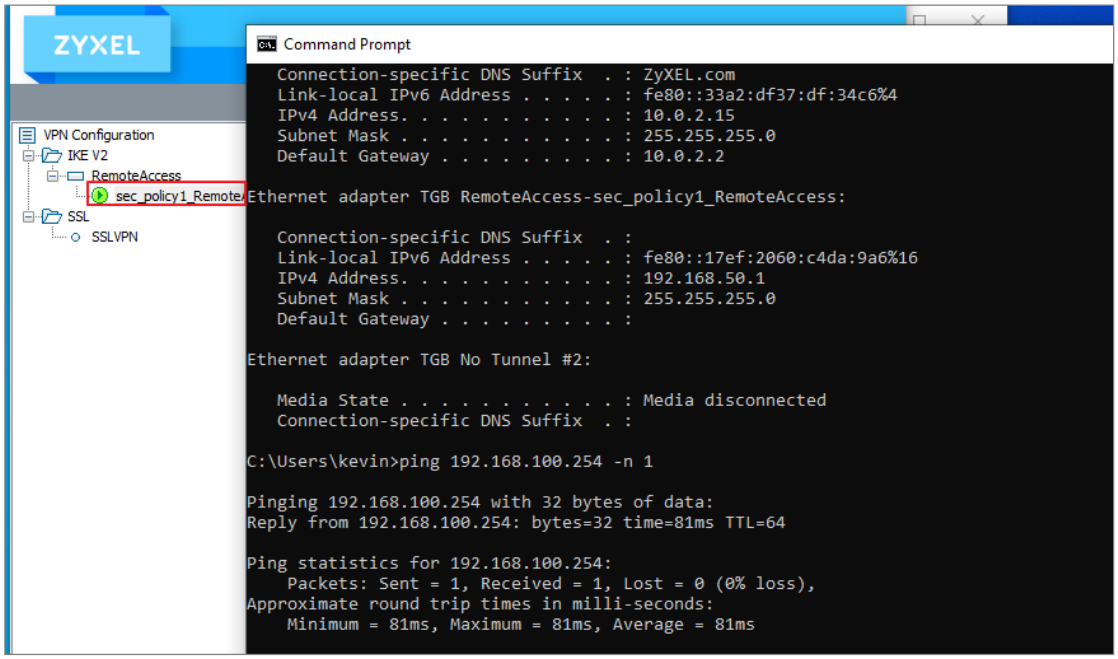
You will see the profile being green and can access internal resource now.



Test IKEv2 Tunnel on TGB Client

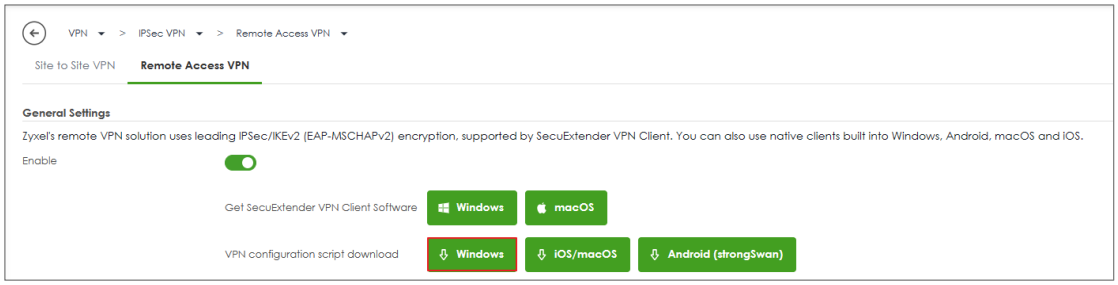
Right click the profile and “Open Tunnel” and log in.

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

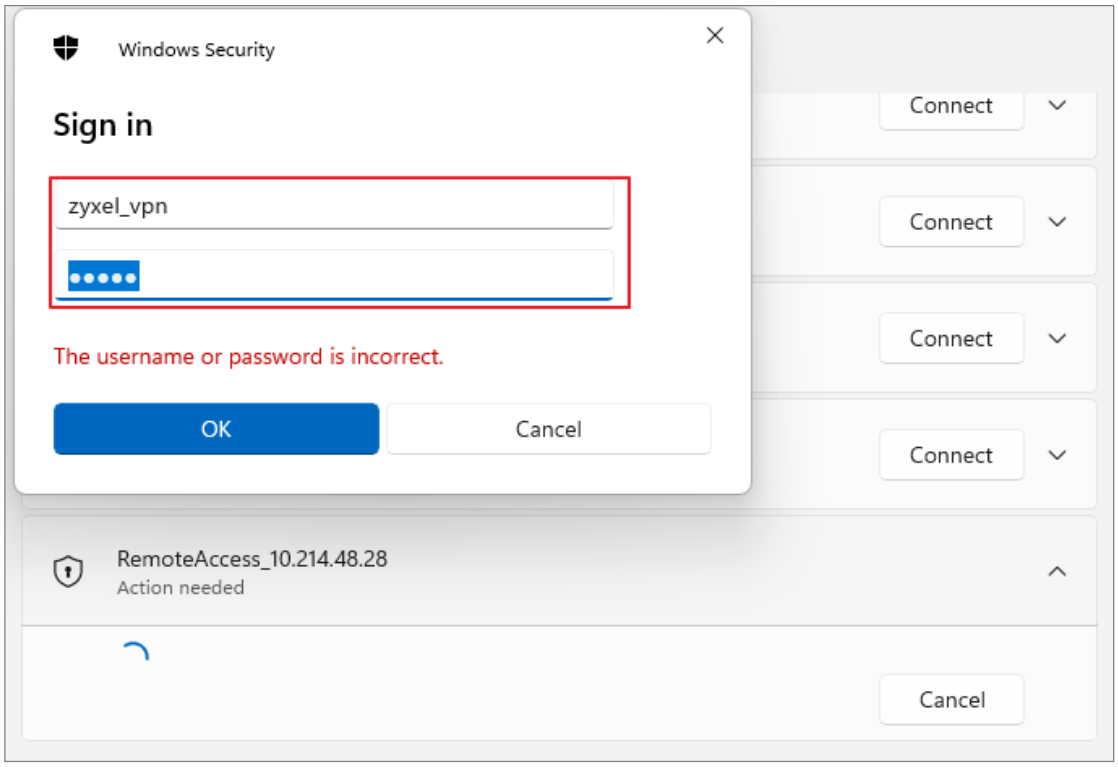


Test IKEv2 Tunnel on Windows Client

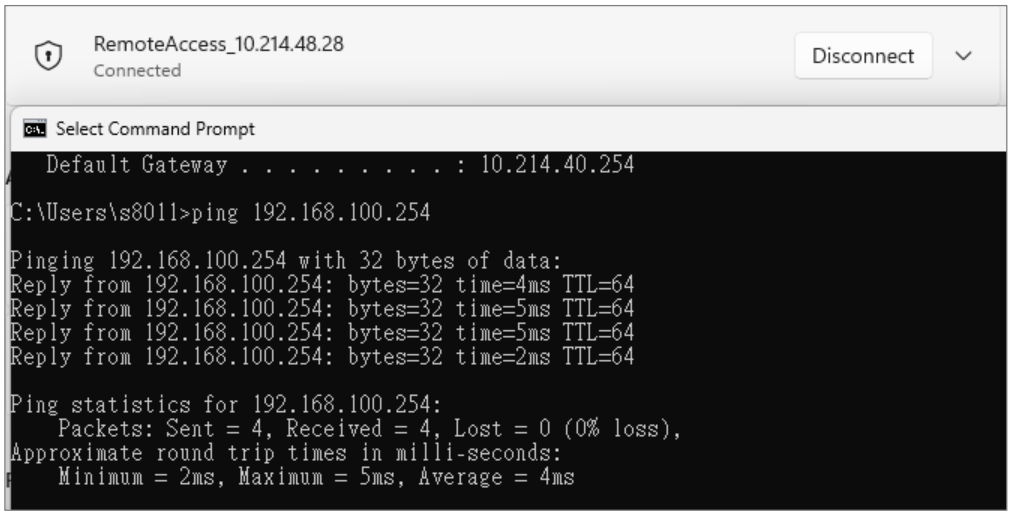
Download Windows VPN configuration script



Perform the windows bat file and input credentials.

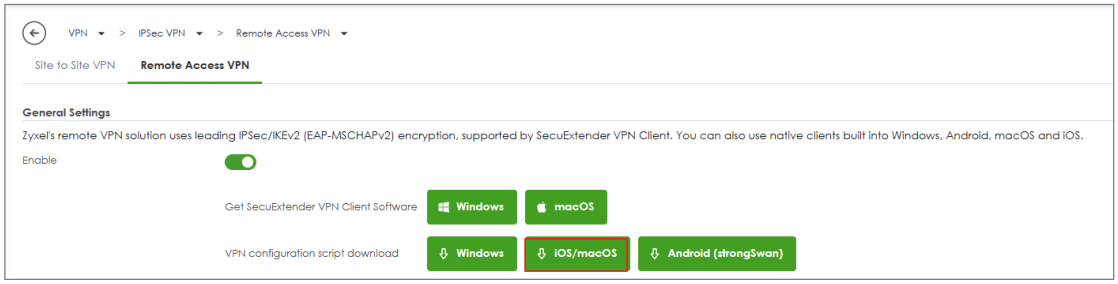


VPN is connected and can access internal resource.

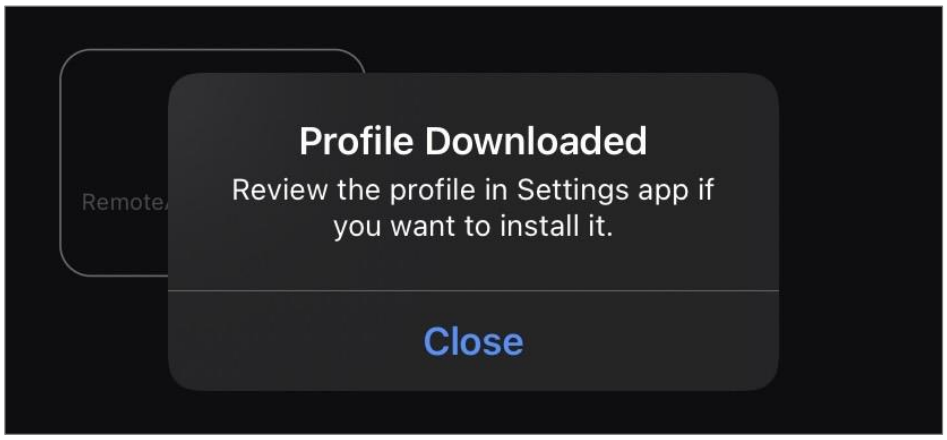


Test IKEv2 Tunnel on iOS Client

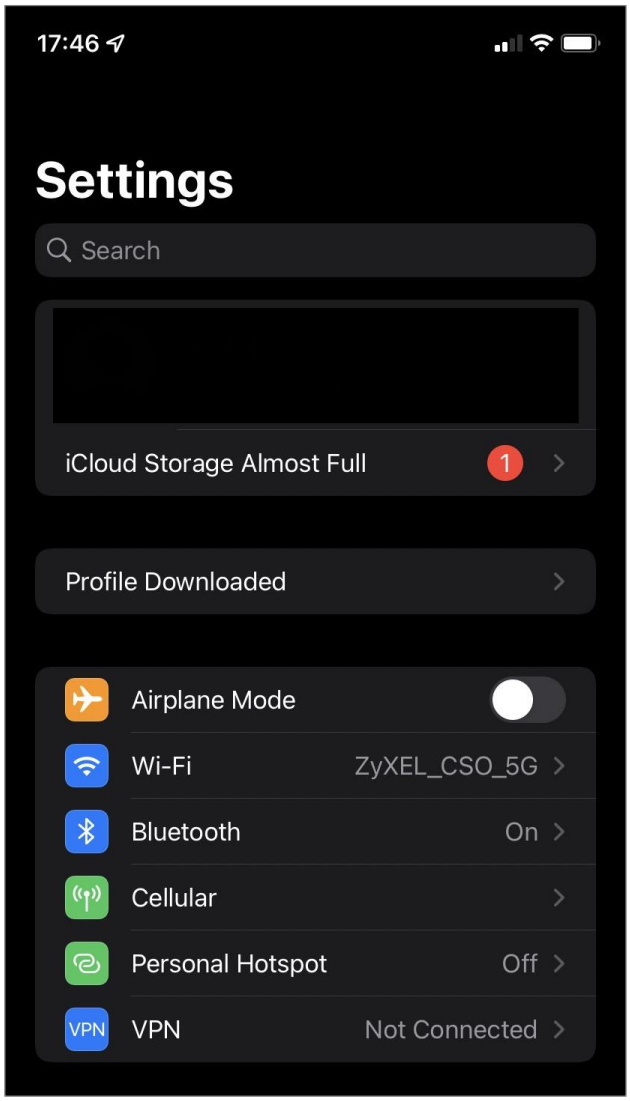
Download iOS/macOS VPN configuration script.



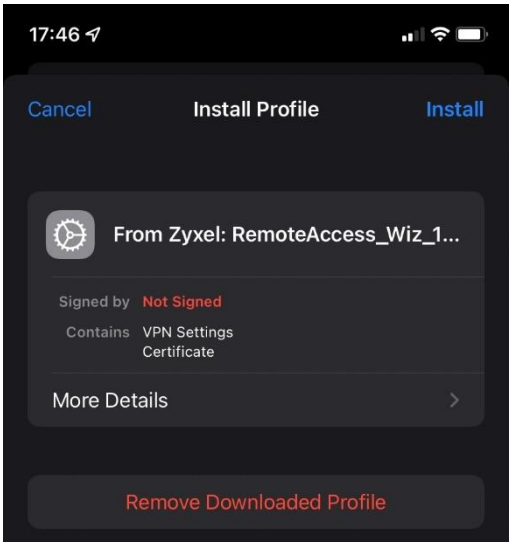
Send the script to Device.



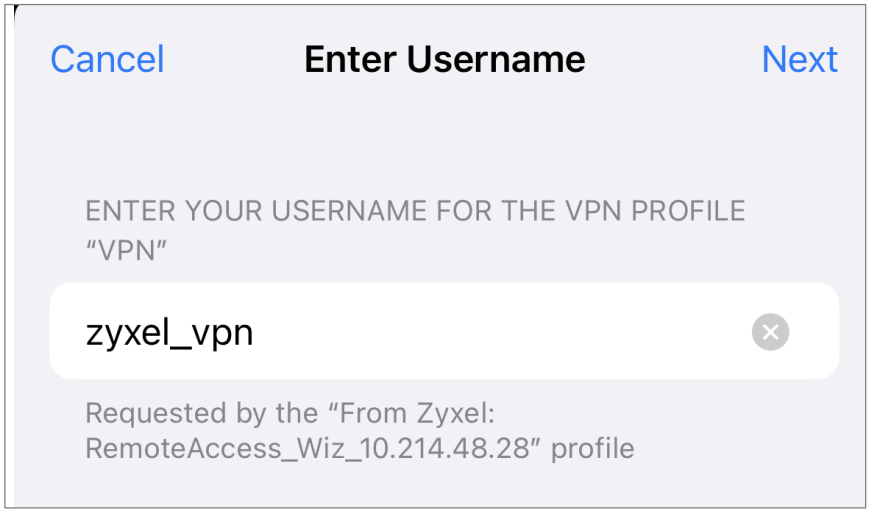
Settings > Profile Downloaded

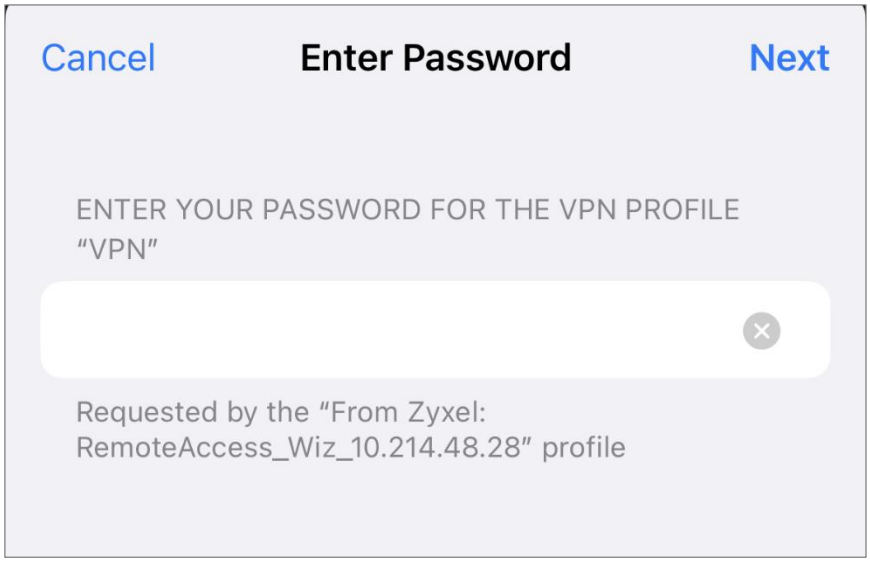


Press Install.

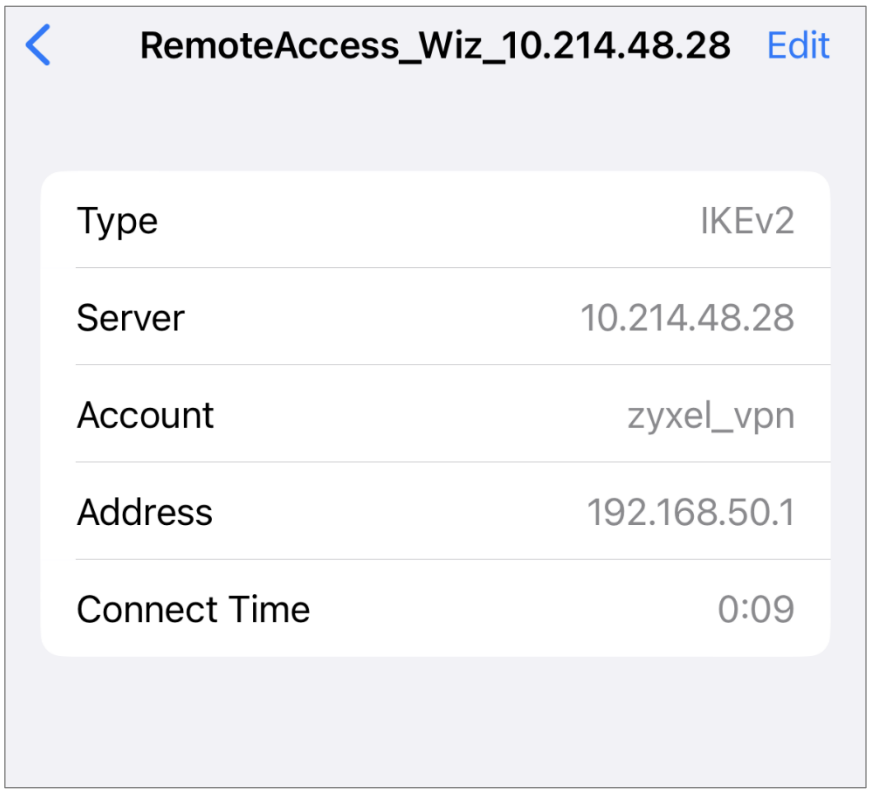


Enter Username and Password.



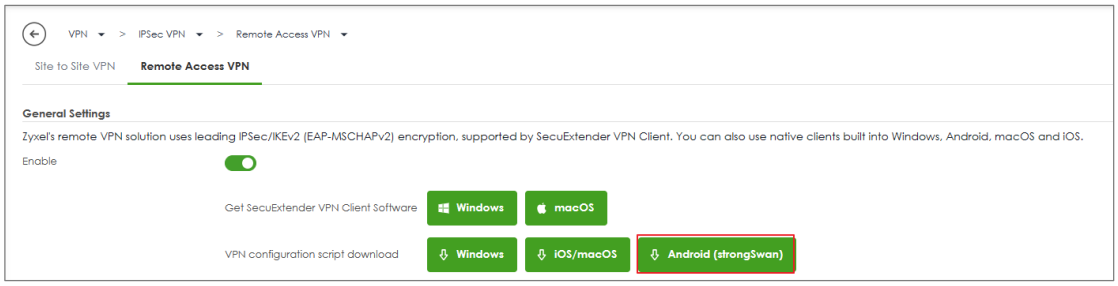


Now, it can connect.

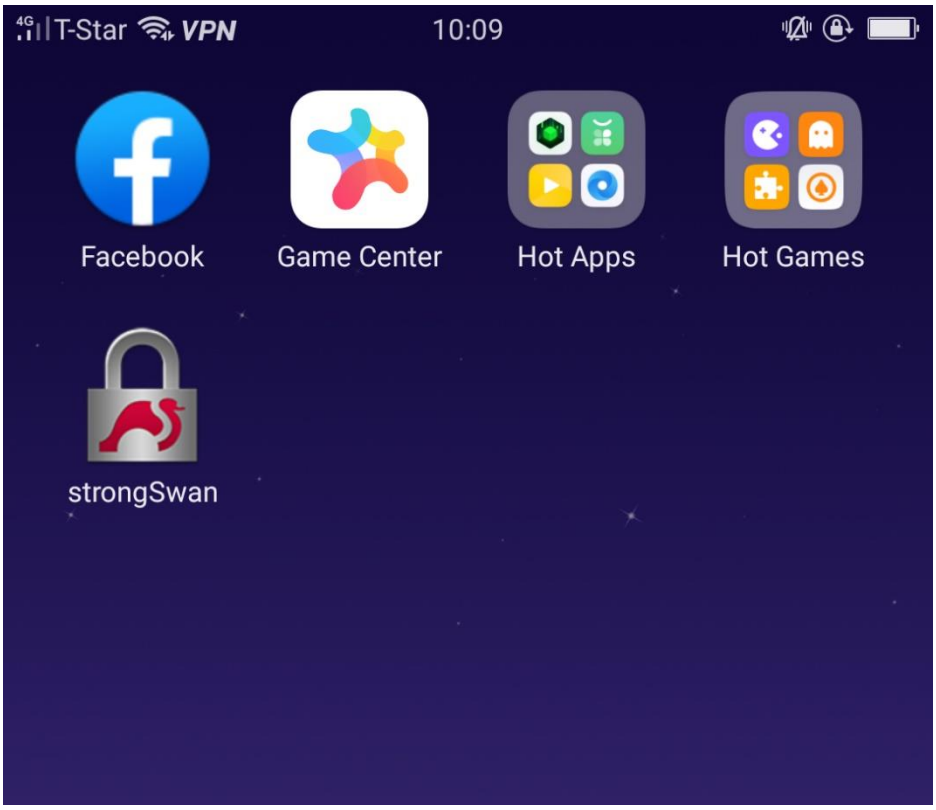


Test IKEv2 Tunnel on Android Client

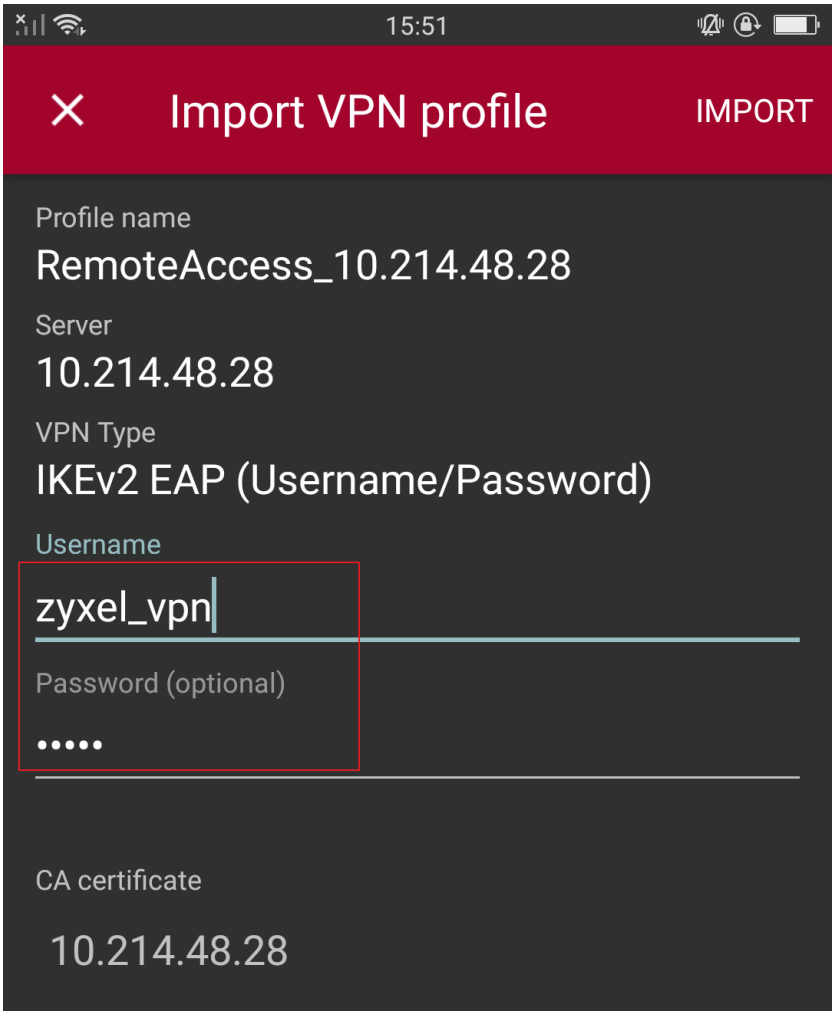
Download Android(strongSwan) VPN configuration script.



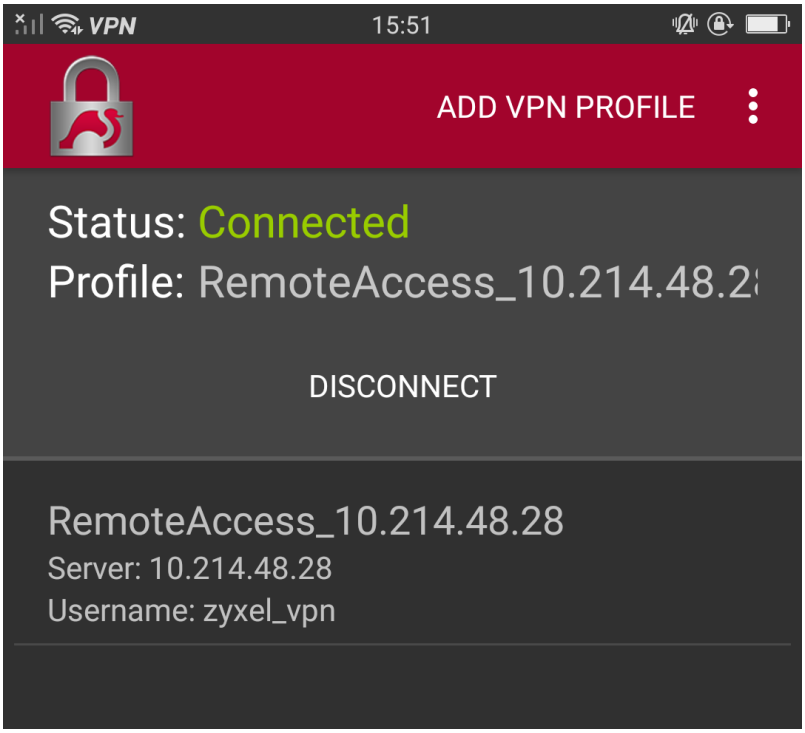
Download strongSwan from Google Play Store.



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



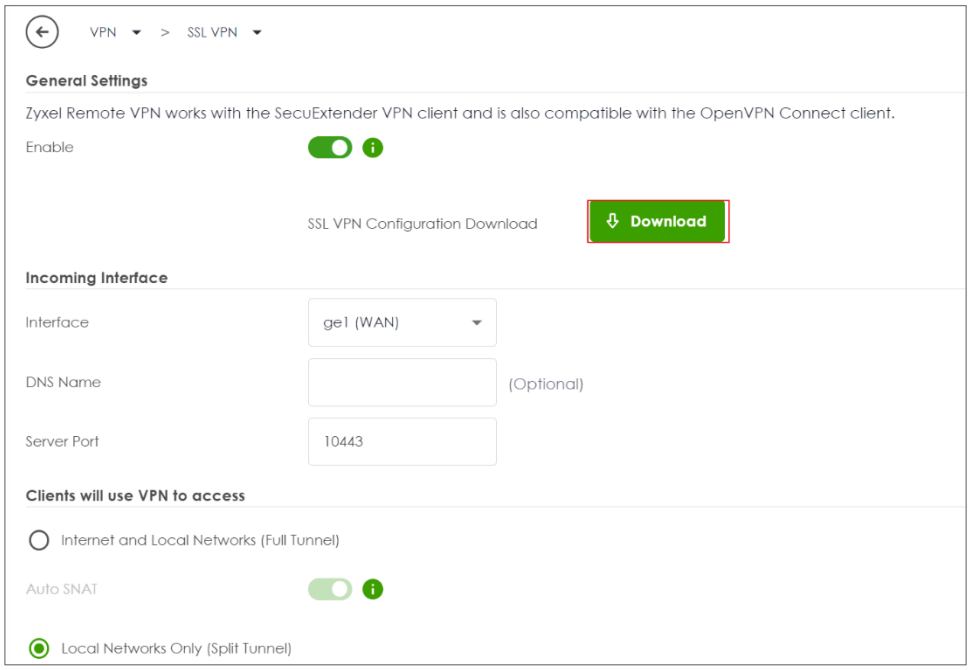
VPN is connected.



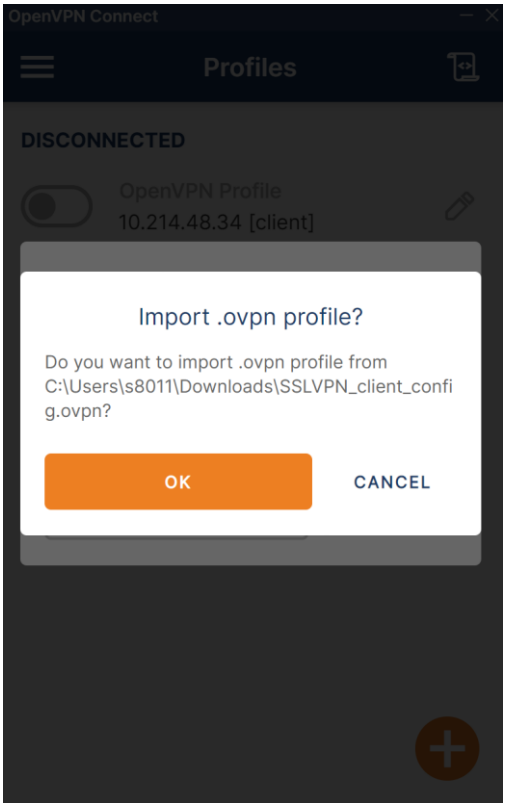
Test OpenVPN

VPN > SSL VPN

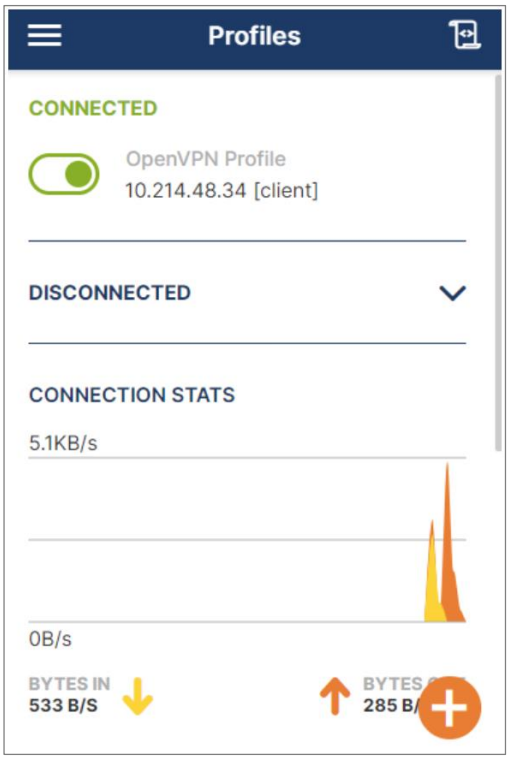
We now support OpenVPN config file, Click Download to obtain the ovpn file.



Import the config file.

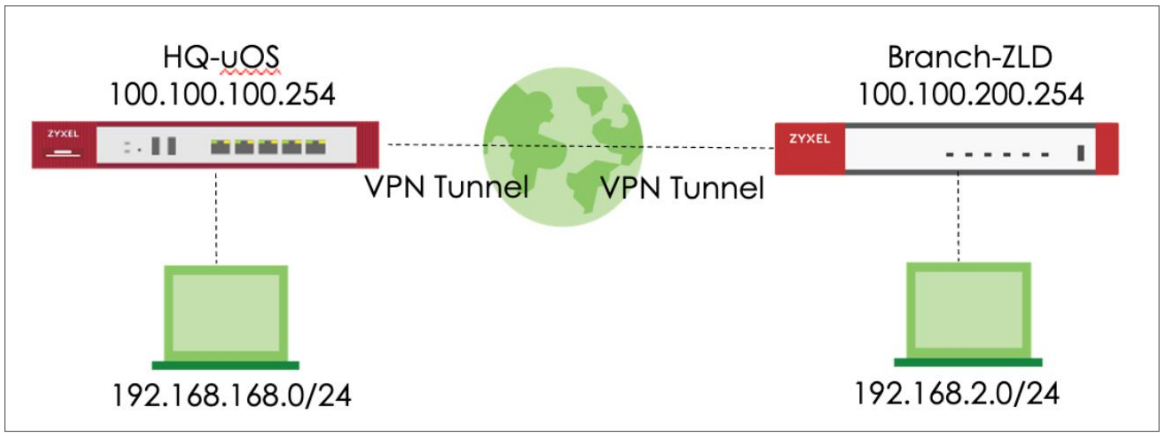


VPN is connected.



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

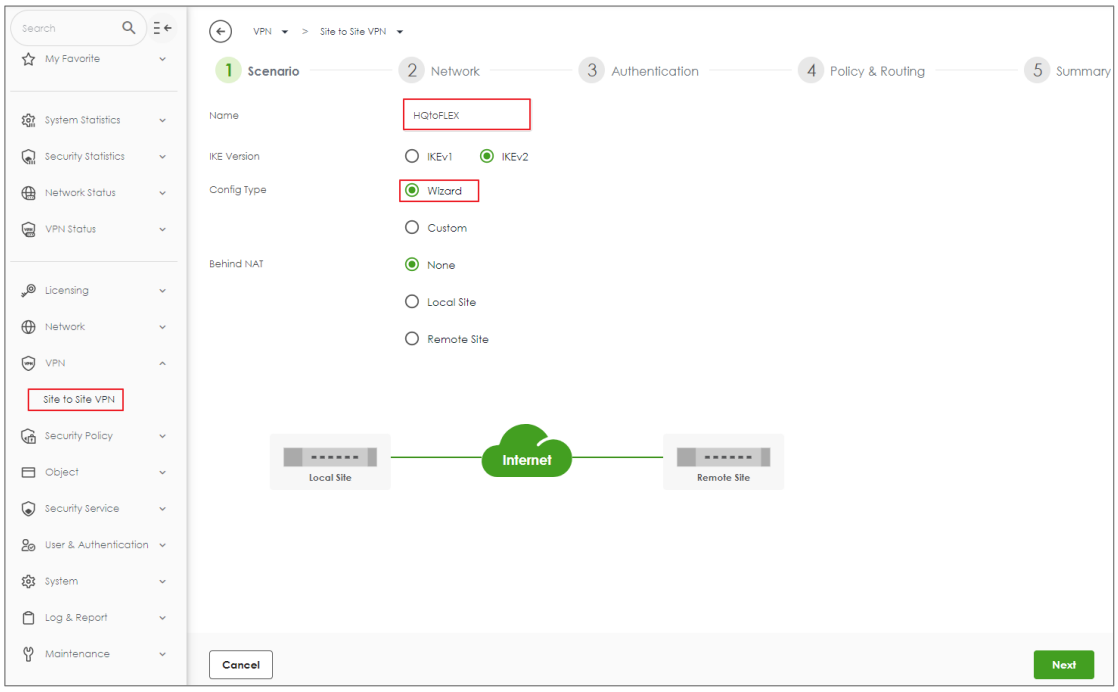
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer gateway is ZLD device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for uOS

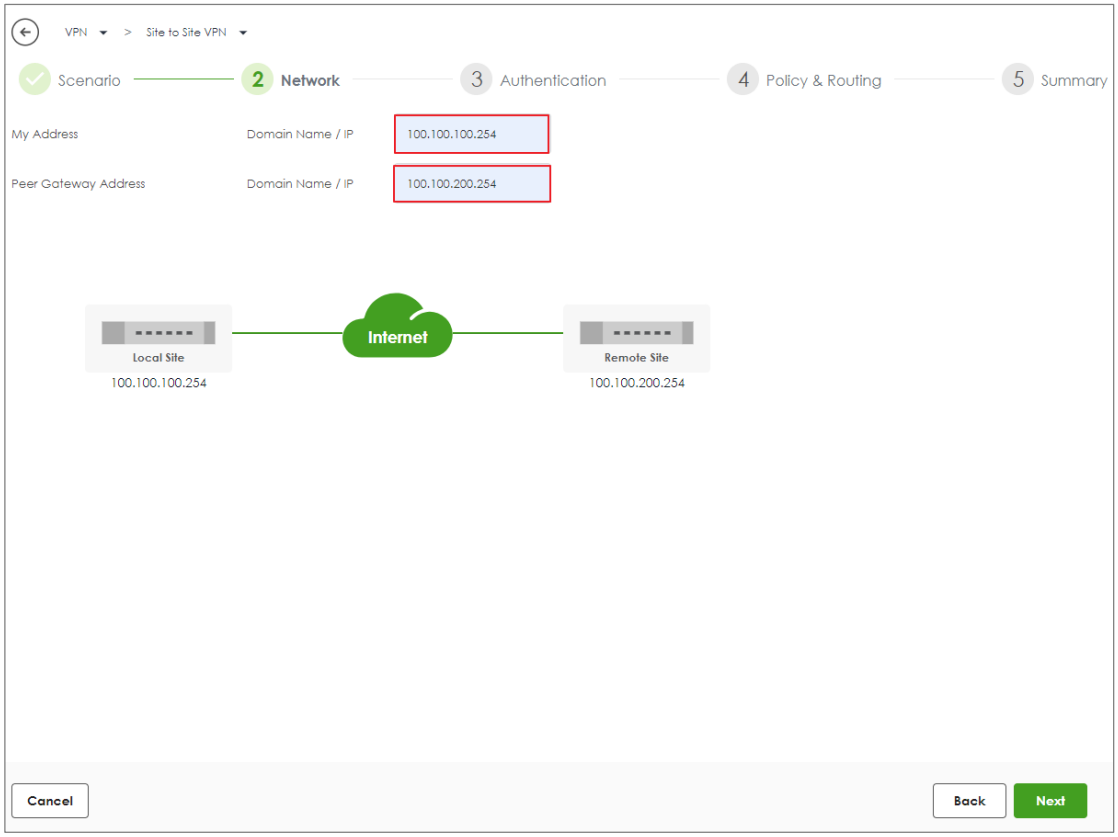
VPN > Site to Site VPN > Scenario

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



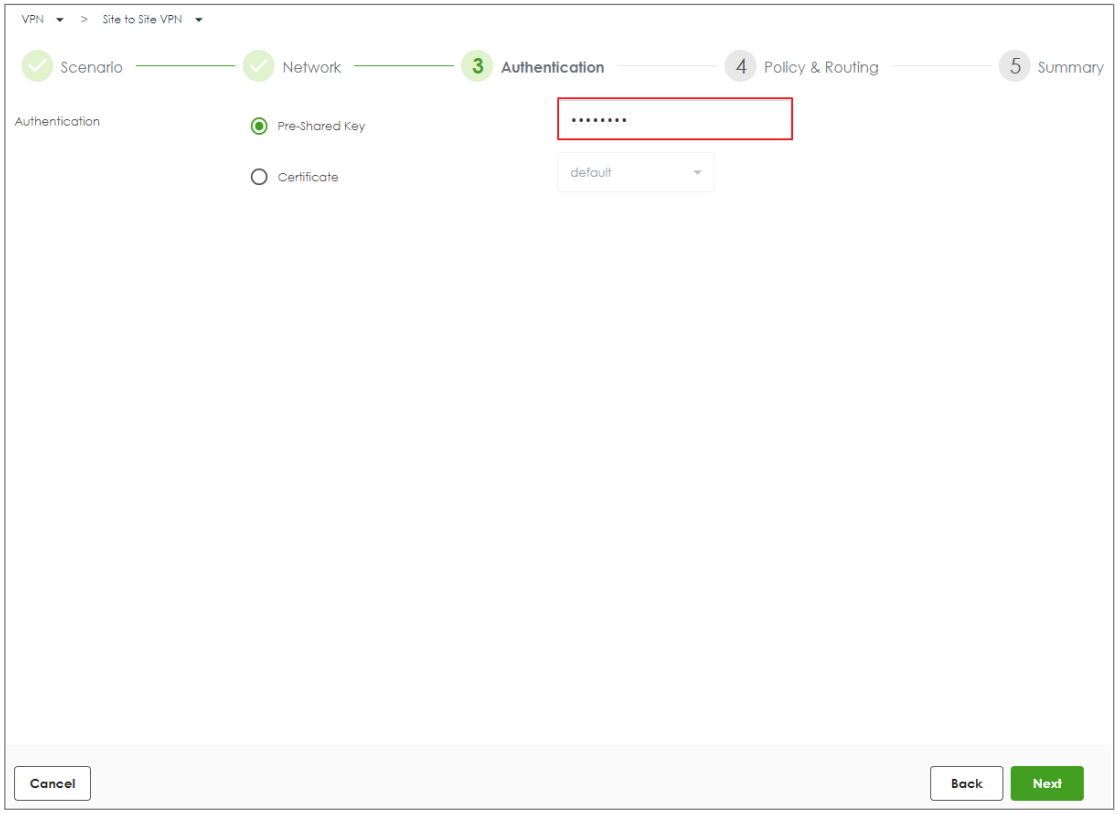
VPN > Site to Site VPN > Scenario > Network

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



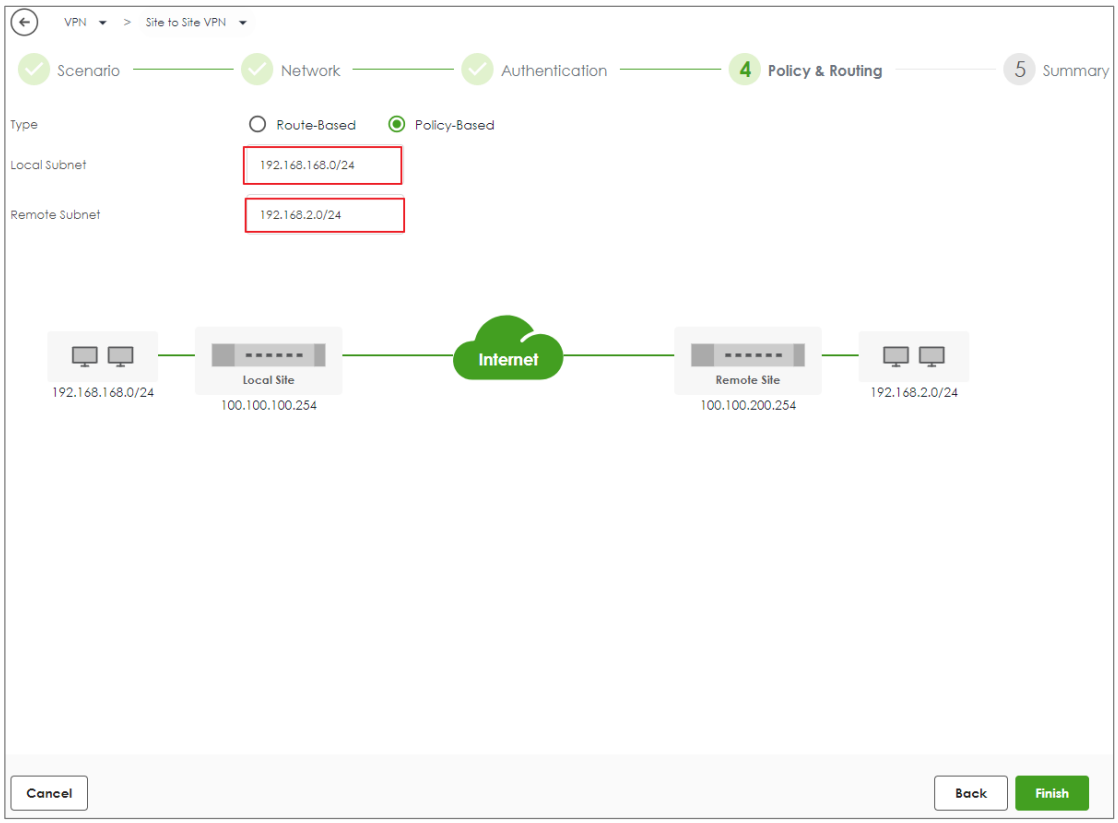
VPN > Site to Site VPN > Scenario > Network > Authentication

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



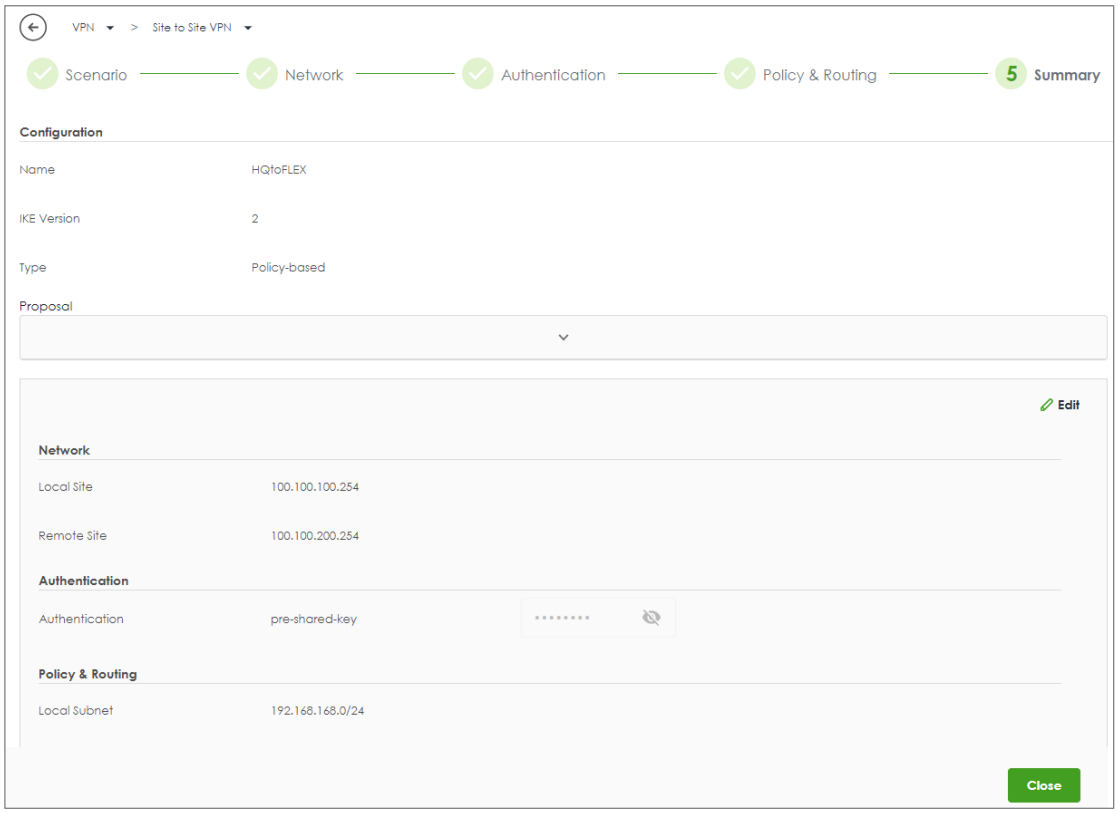
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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



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

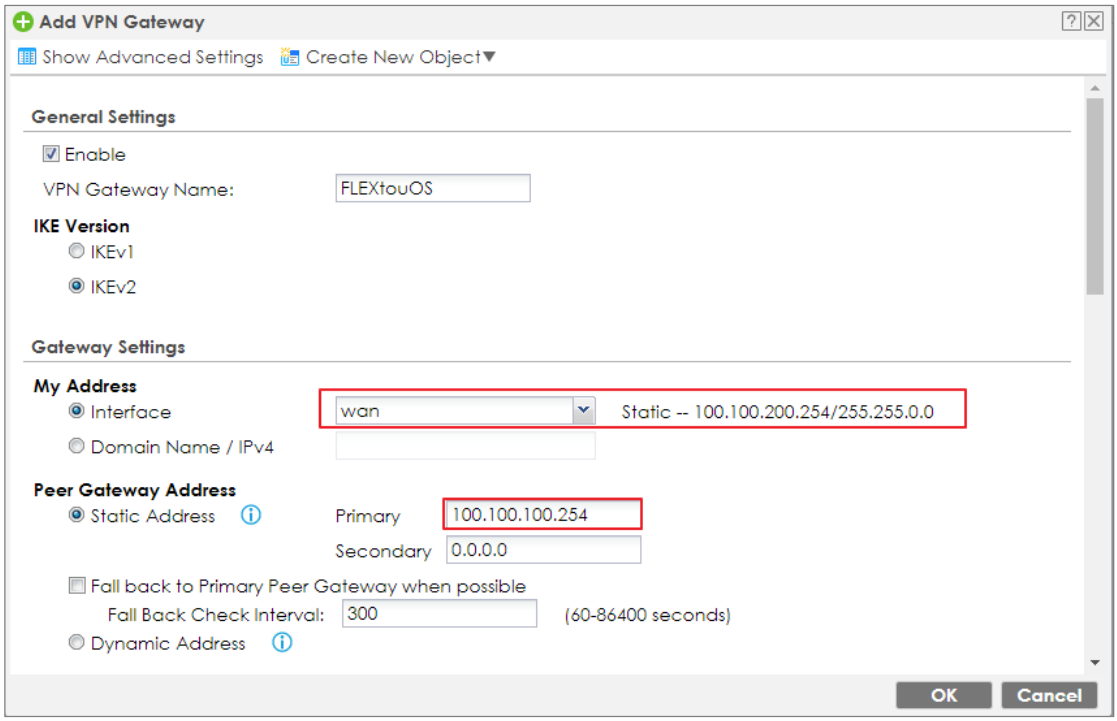
The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



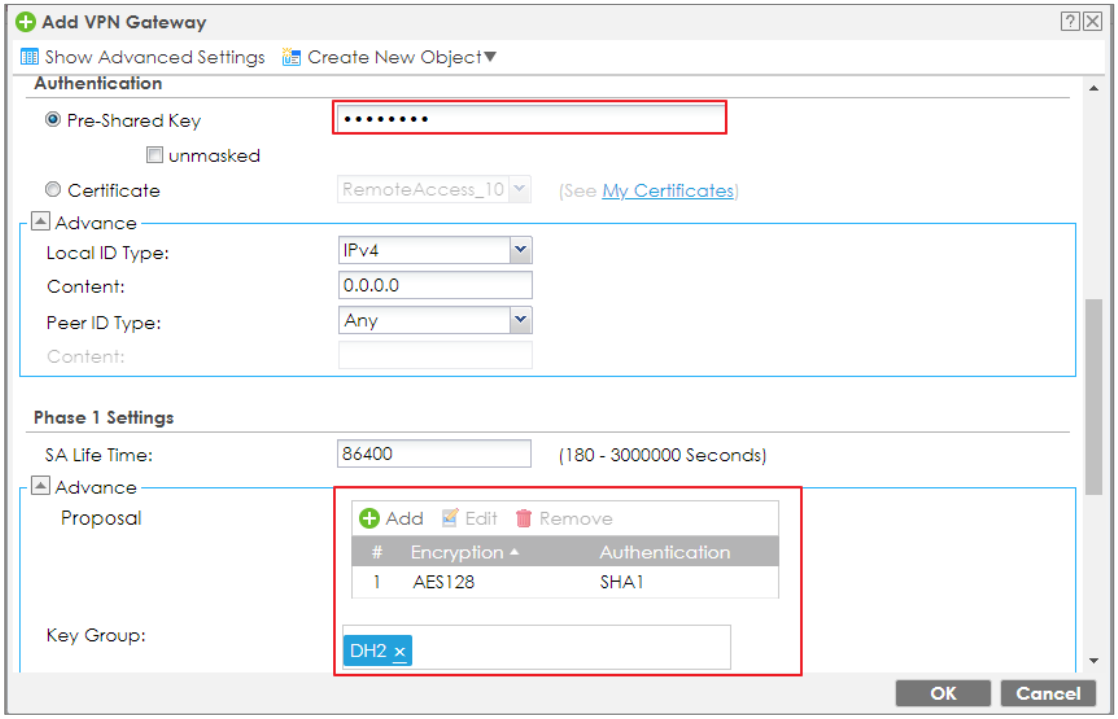
Set up IPSec VPN Tunnel for ZLD

VPN > IPSec VPN > VPN Gateway

Select the WAN interface and type the Peer Gateway Address.

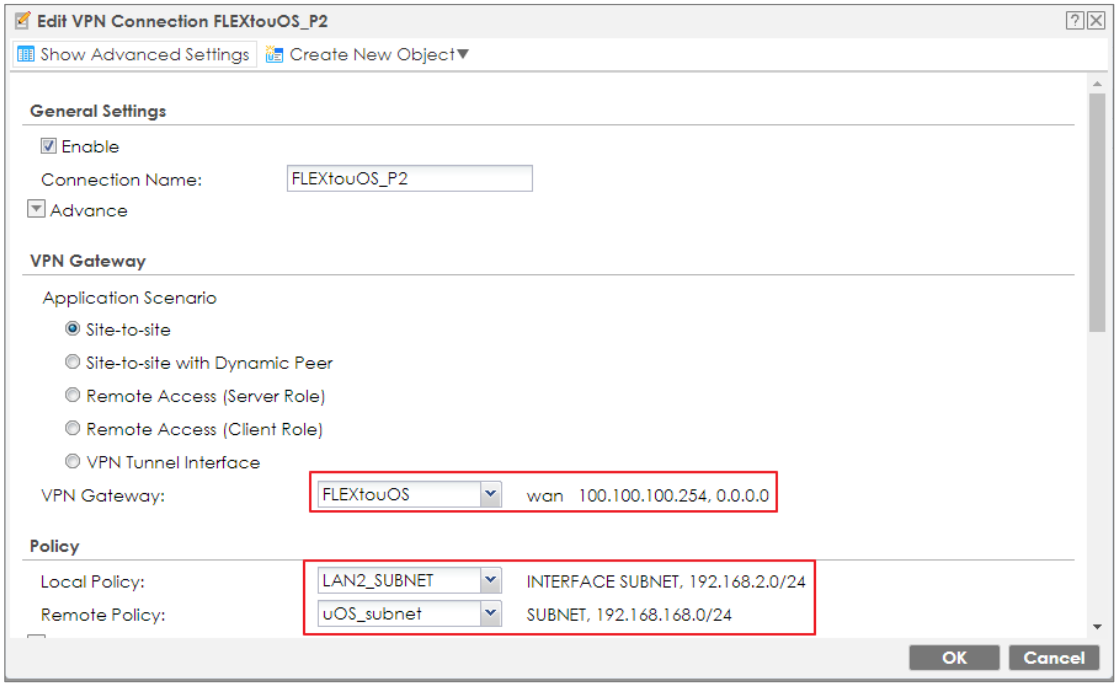


Type Pre-shared Key. The default proposal which created by wizard is “Encryption:AES128, Authentication:SHA1, Key Group:DH2”. Those are the same as uOS.

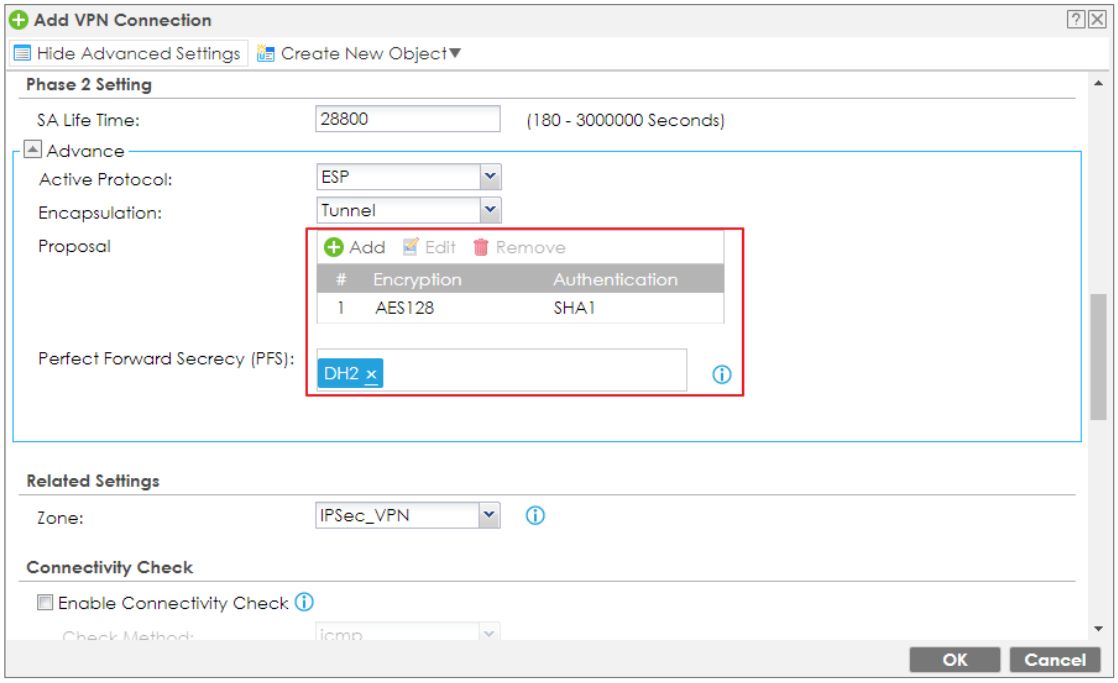


VPN > IPSec VPN > VPN Connection

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.



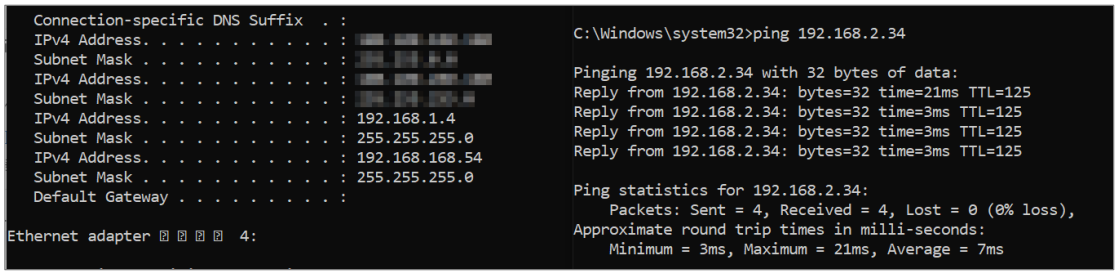
The default proposal which created by wizard is “Encryption: AES128, Authentication: SHA1, Key Group: DH2”. Those are the same as uOS.



Test IPSec VPN Tunnel

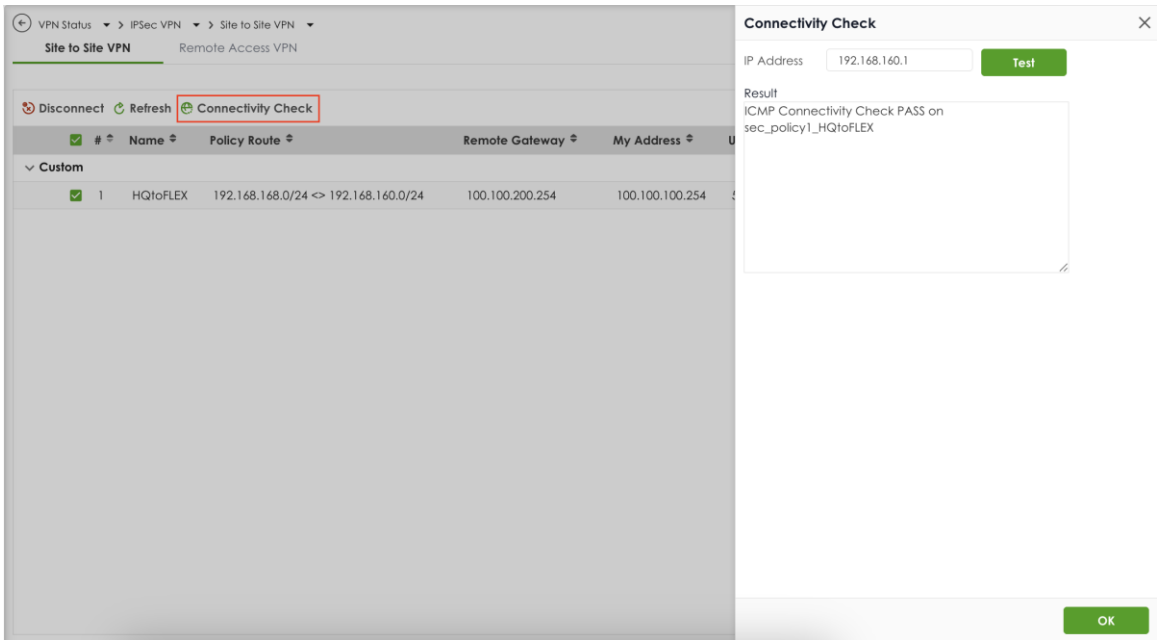
Ping the PC that is connected to ZLD device

Win 11 > cmd > ping 192.168.2.34



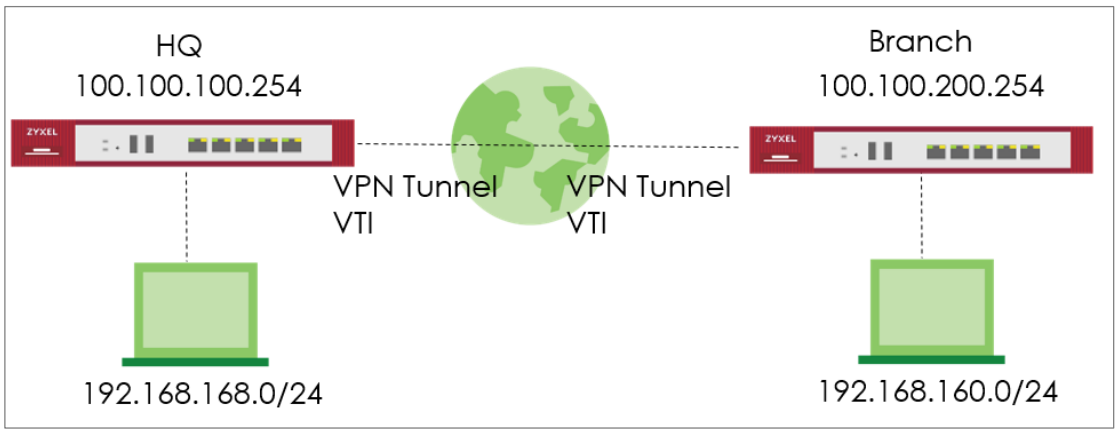
VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check



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.

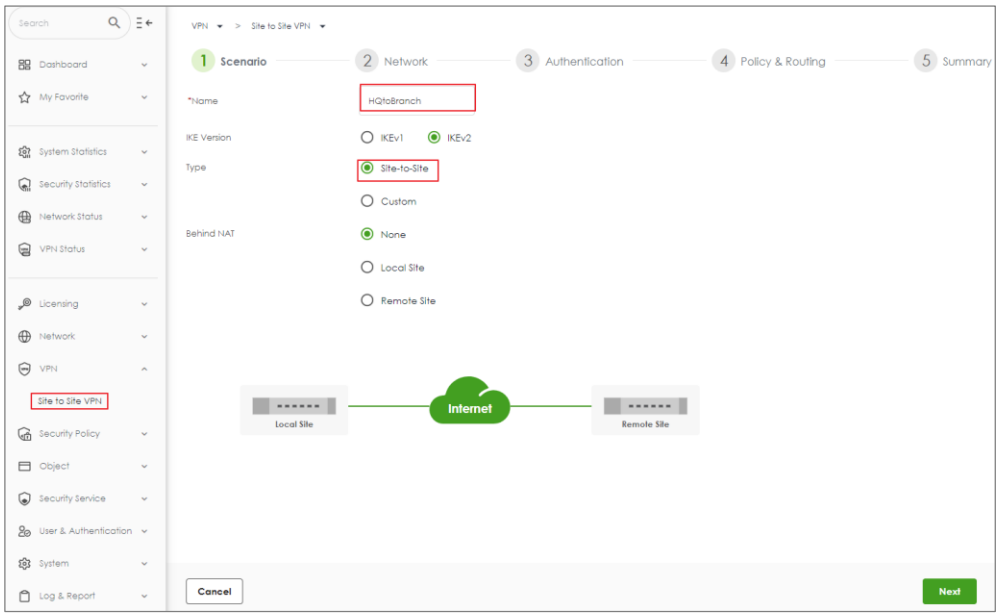


Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

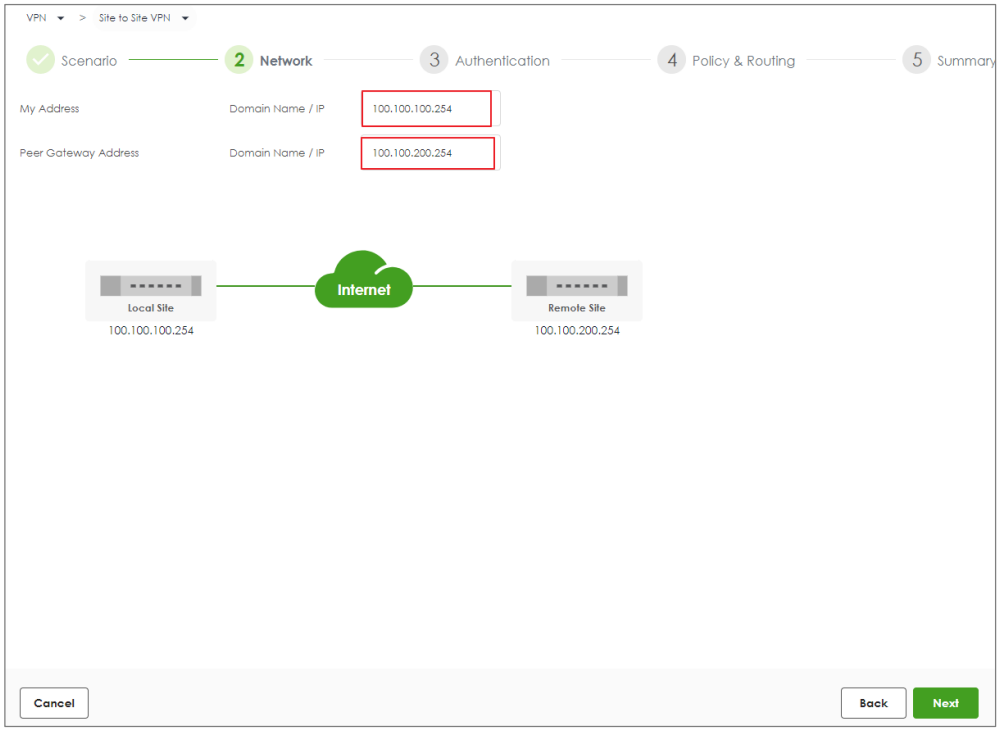
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site.

Click **Next**.



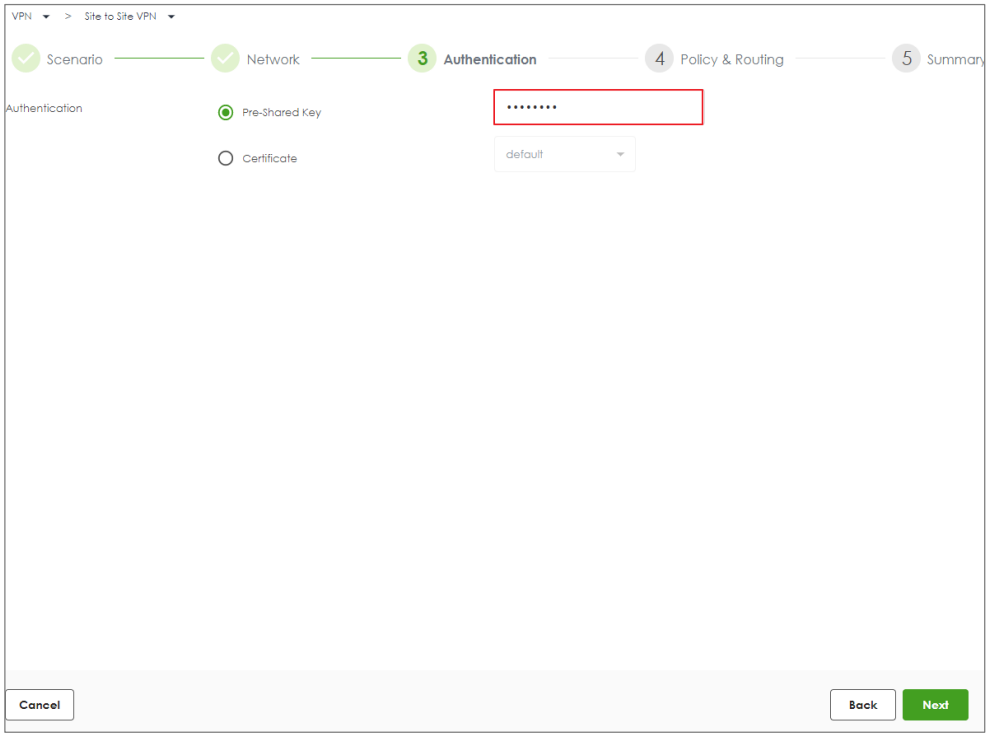
VPN > Site to Site VPN > Scenario > Network

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



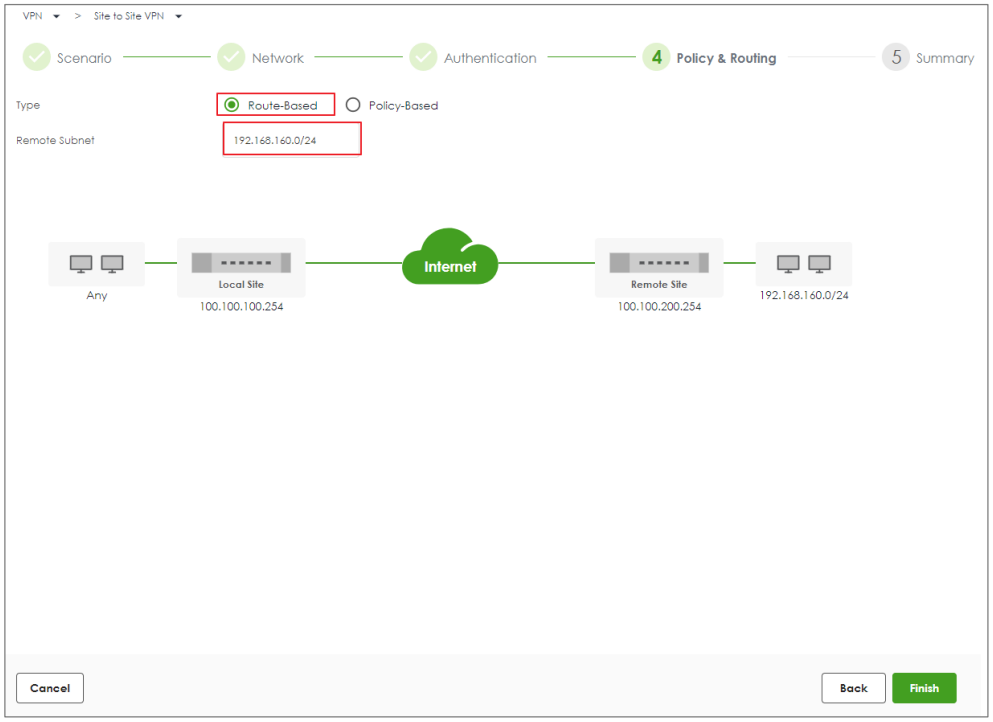
VPN > Site to Site VPN > Scenario > Network > Authentication

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



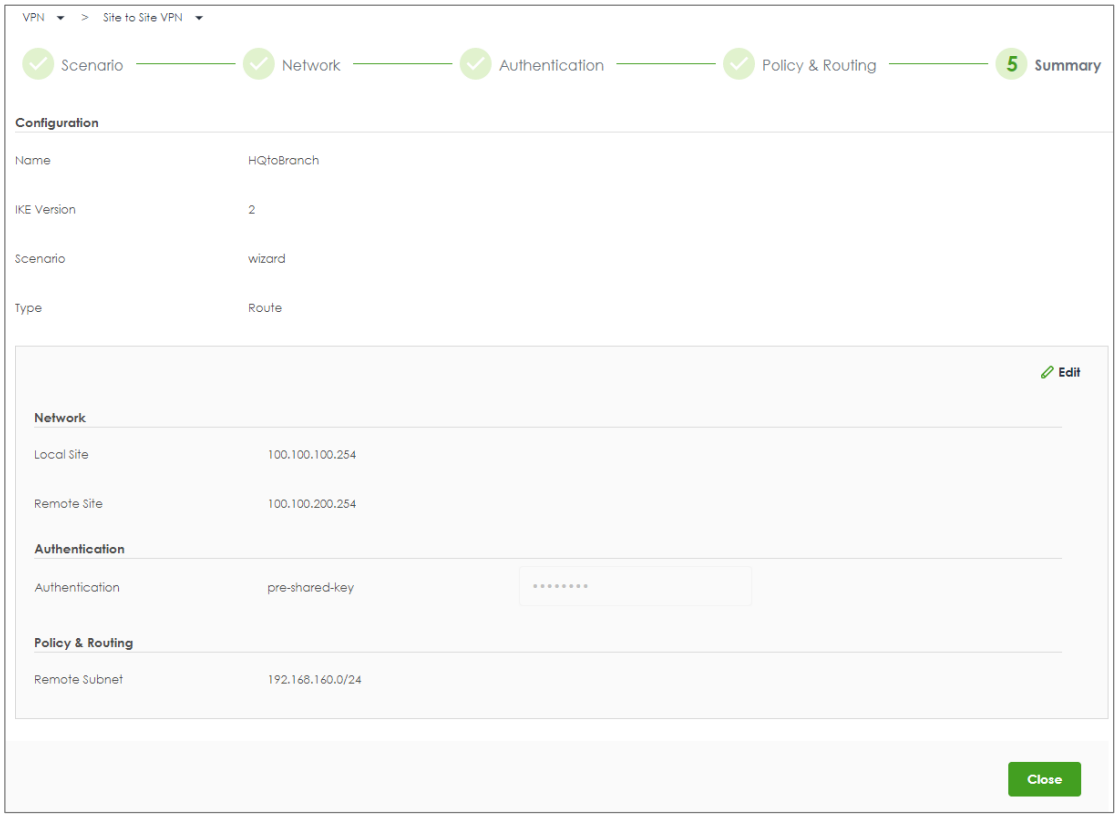
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

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



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

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

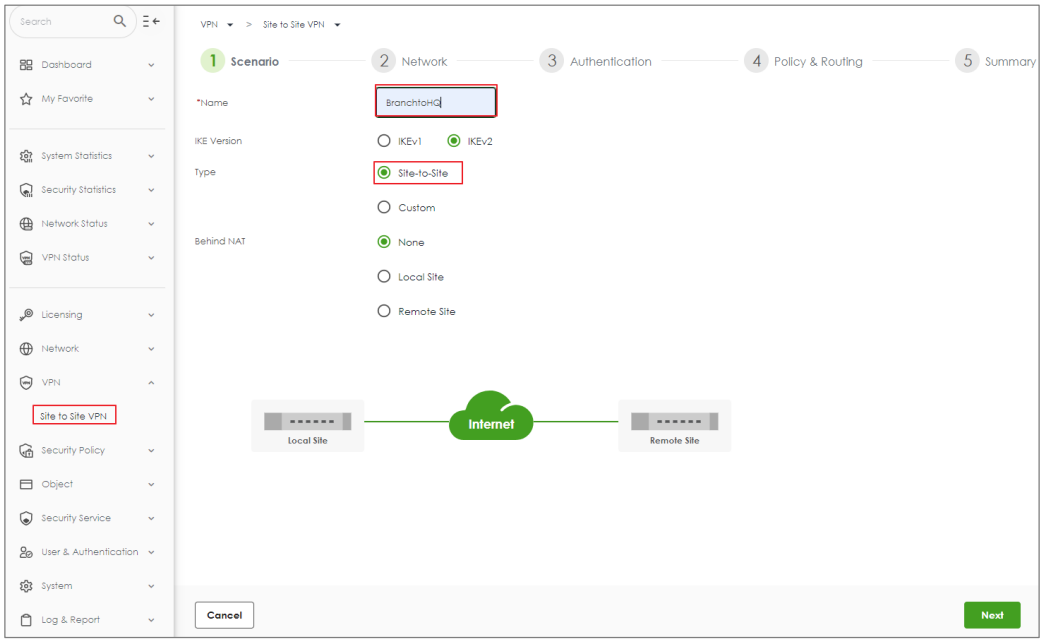


Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

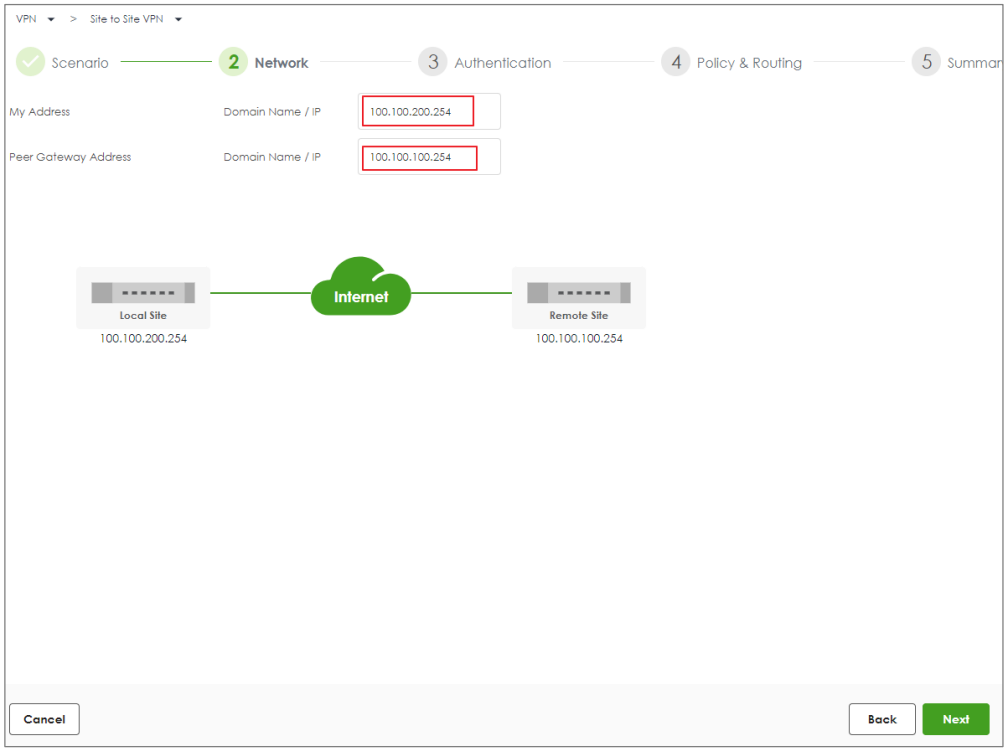
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site.

Click **Next**.



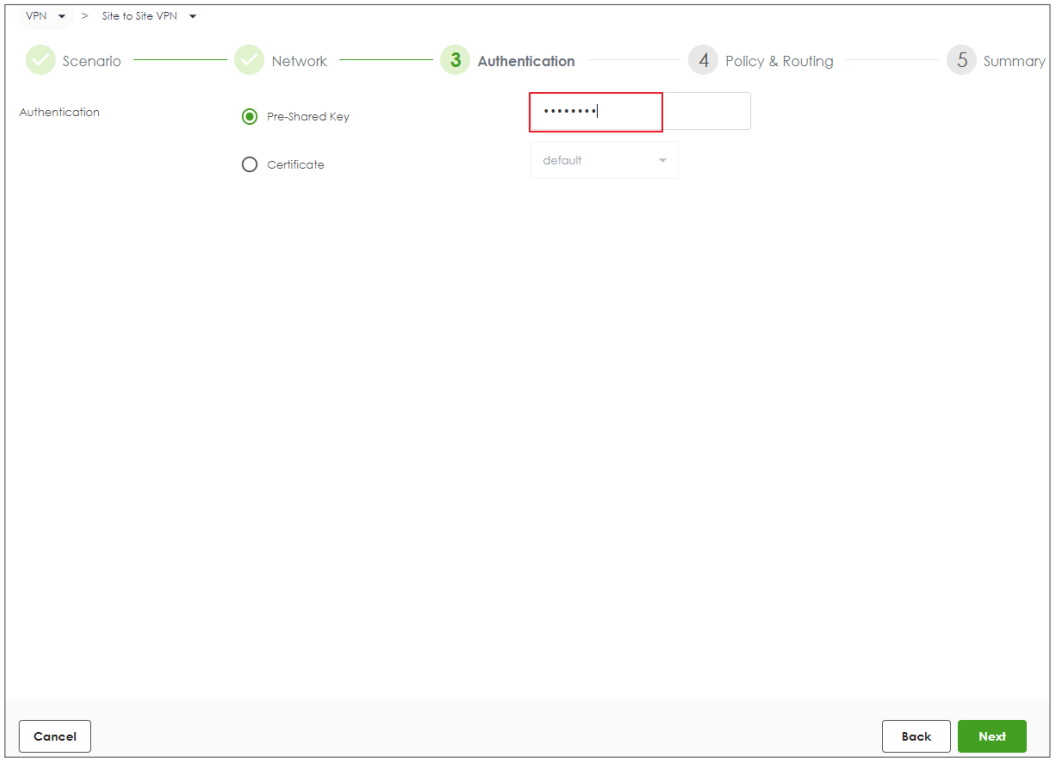
VPN > Site to Site VPN > Scenario > Network

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



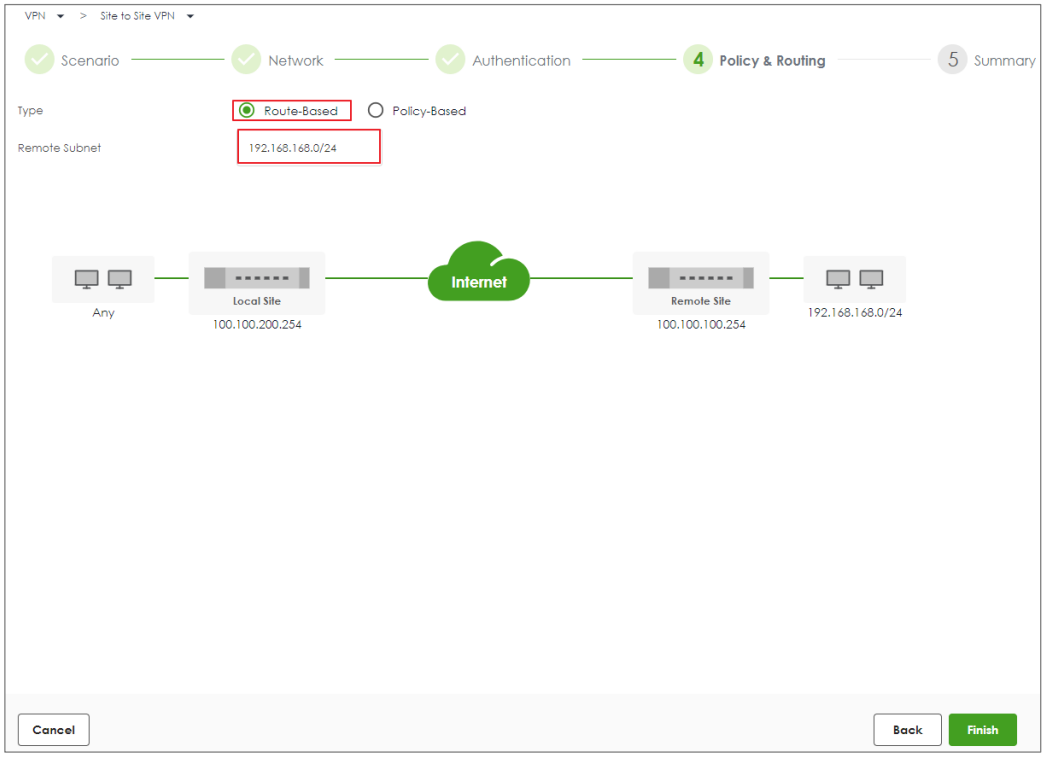
VPN > Site to Site VPN > Scenario > Network > Authentication

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



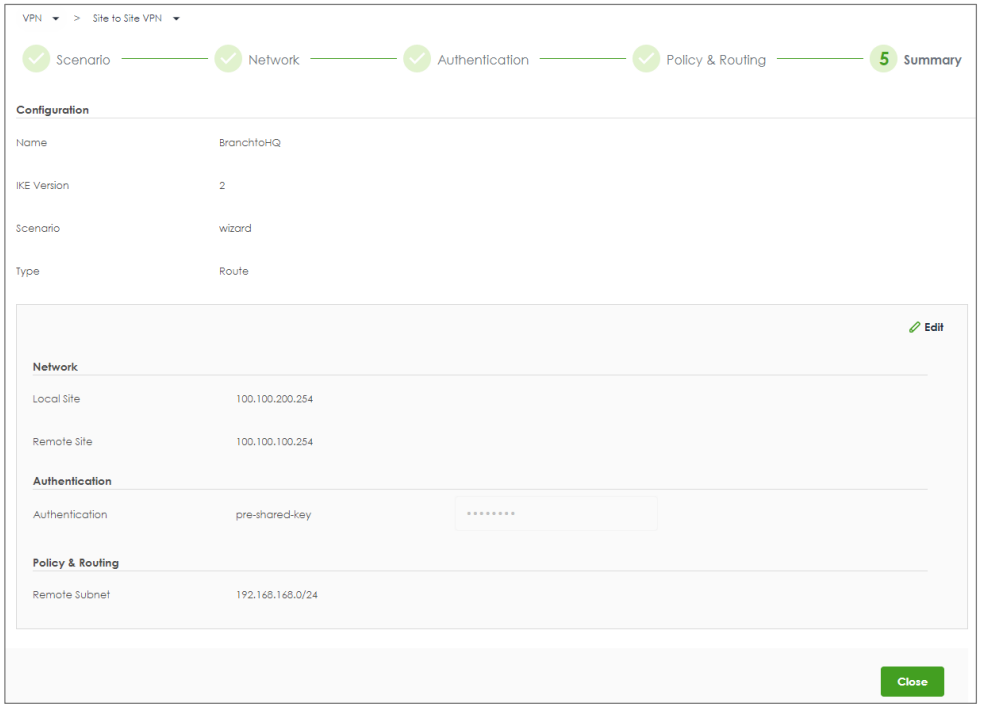
VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Type to Route-Based and Remote Subnet.



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

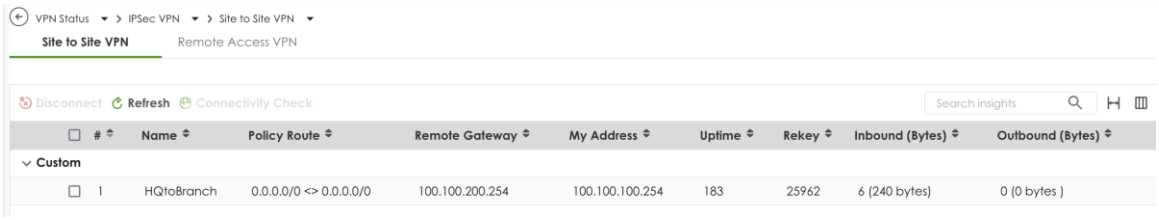
The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Test IPSec VPN Tunnel

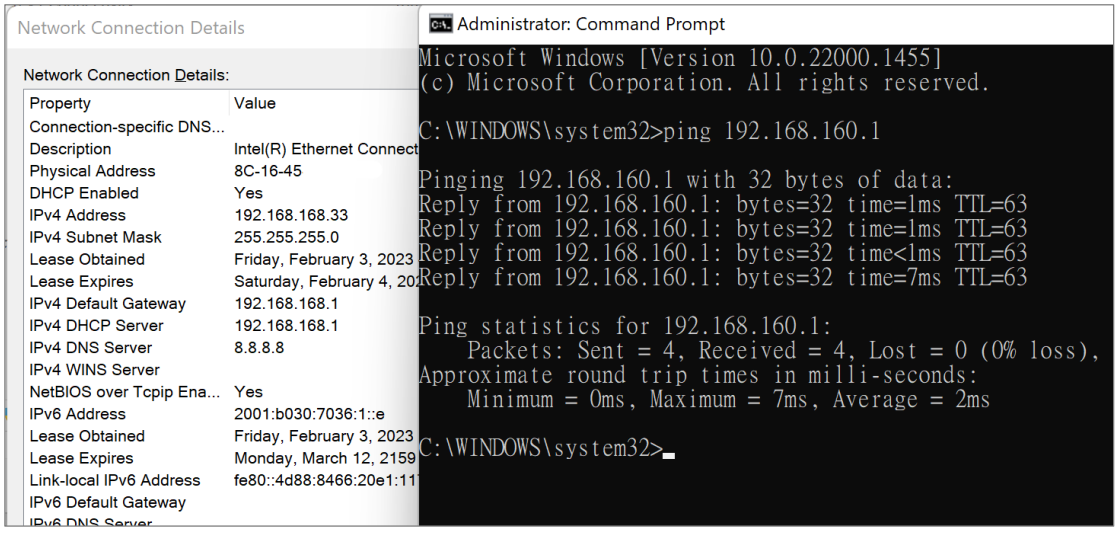
VPN Status > IPSec VPN

Verify the IPSec VPN status.



Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



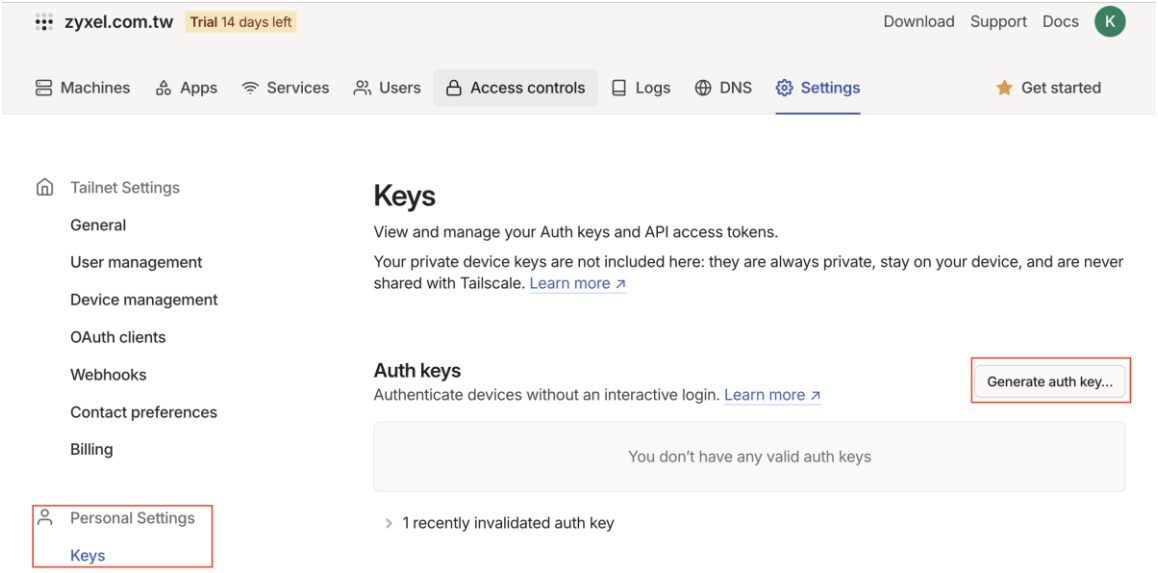
How to Use Tailscale

What's Tailscale?

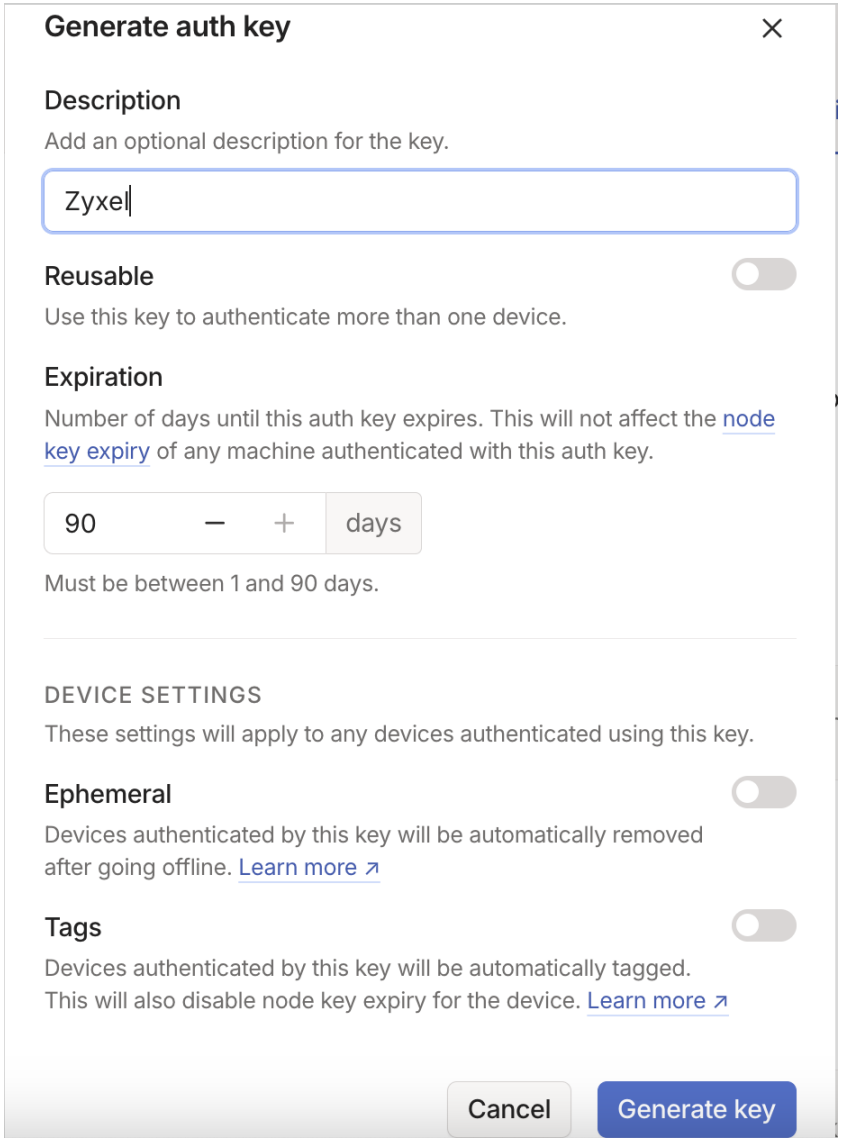
Tailscale is a secure, peer-to-peer VPN solution that simplifies connecting devices over the internet. Unlike traditional VPNs, Tailscale establishes direct connections between devices without requiring complex firewall configurations or static IP addresses. It uses a mesh network topology, allowing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

Start to Tailscale and implement on Firewall

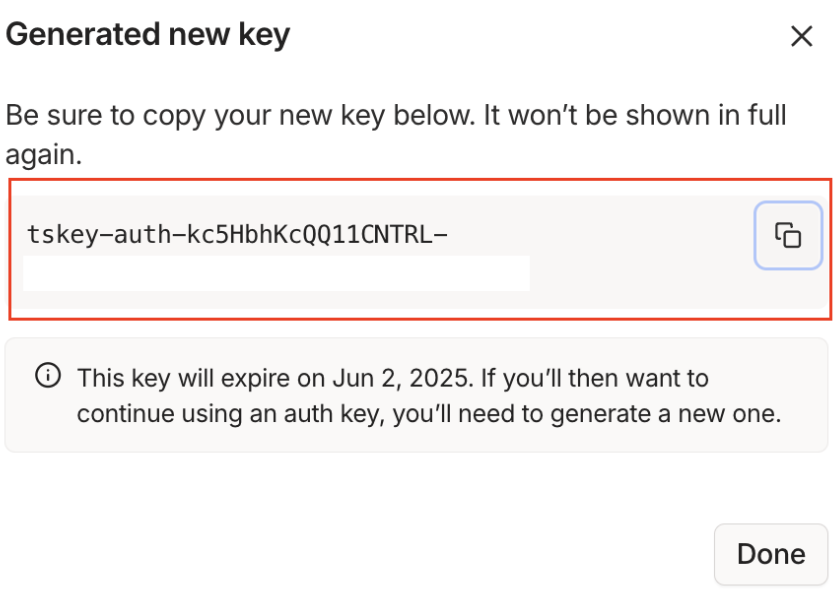
1. Please refer TailScale KB to create an account and start.
2. Navigate to "Settings -> Personal Settings -> Keys" and "Generate auth key".



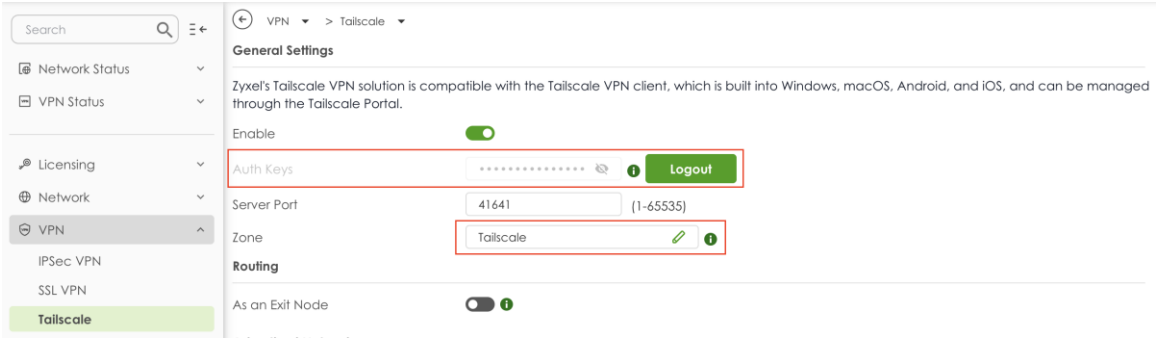
3. Give a Description Name as you want and disable “Reusable” due to security reason then click “Generate key”.



Copy the key.

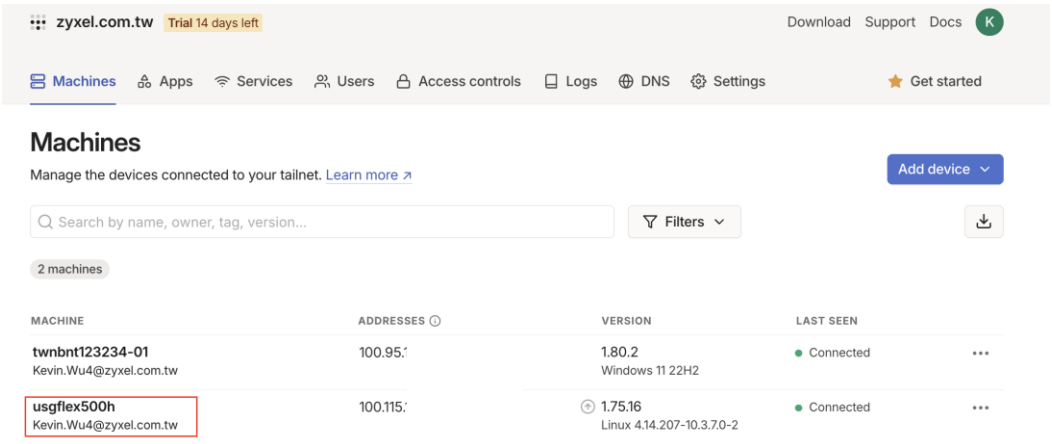


4. Login Firewall and navigate to "VPN -> Tailscale", paste to the "Auth Keys".

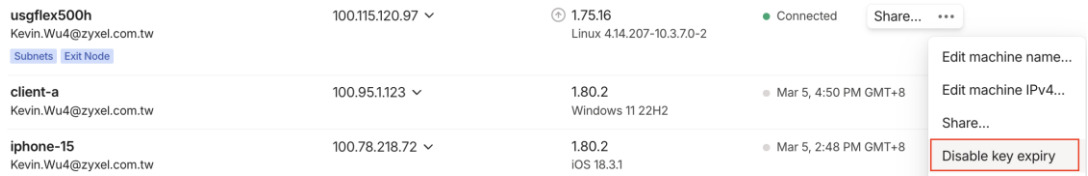


- When you want to change the key, please click Logout.
- You can choose the zone by yourself. We recommend using Tailscale zone for some predefined rules.

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

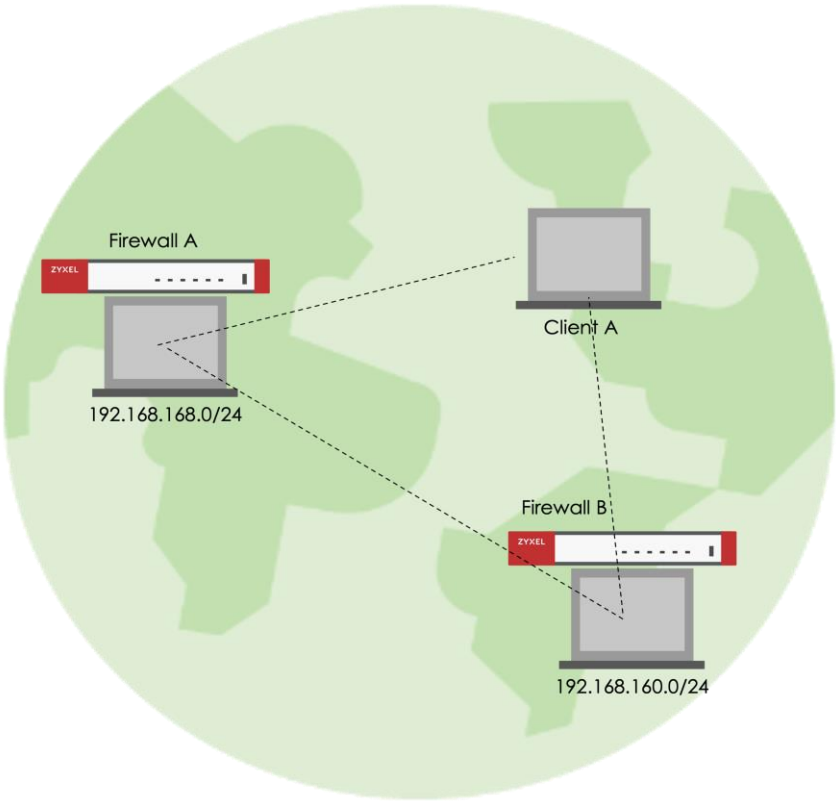


Click “Disable key expiry” for all client to prevent lost connection while expire.



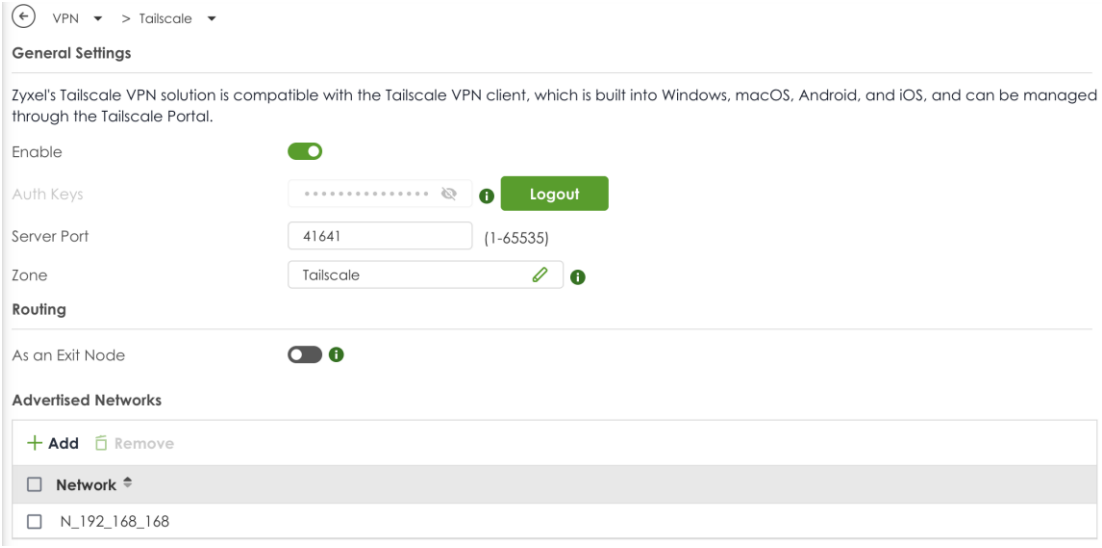
Scenario

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:

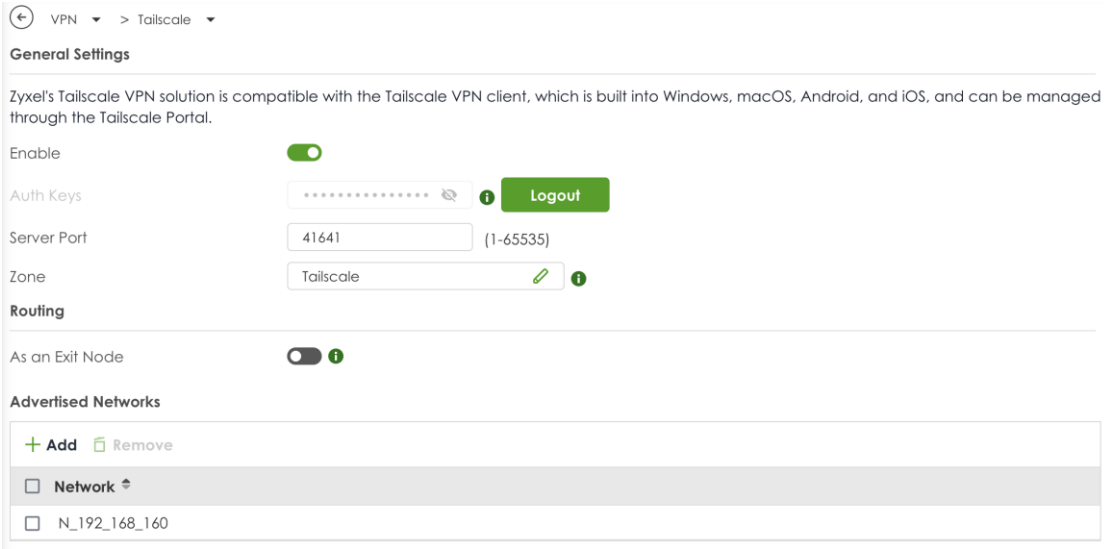


Case1: Allow Client A to access the 192.168.168.0/24 and 192.168.160.0/24 subnets

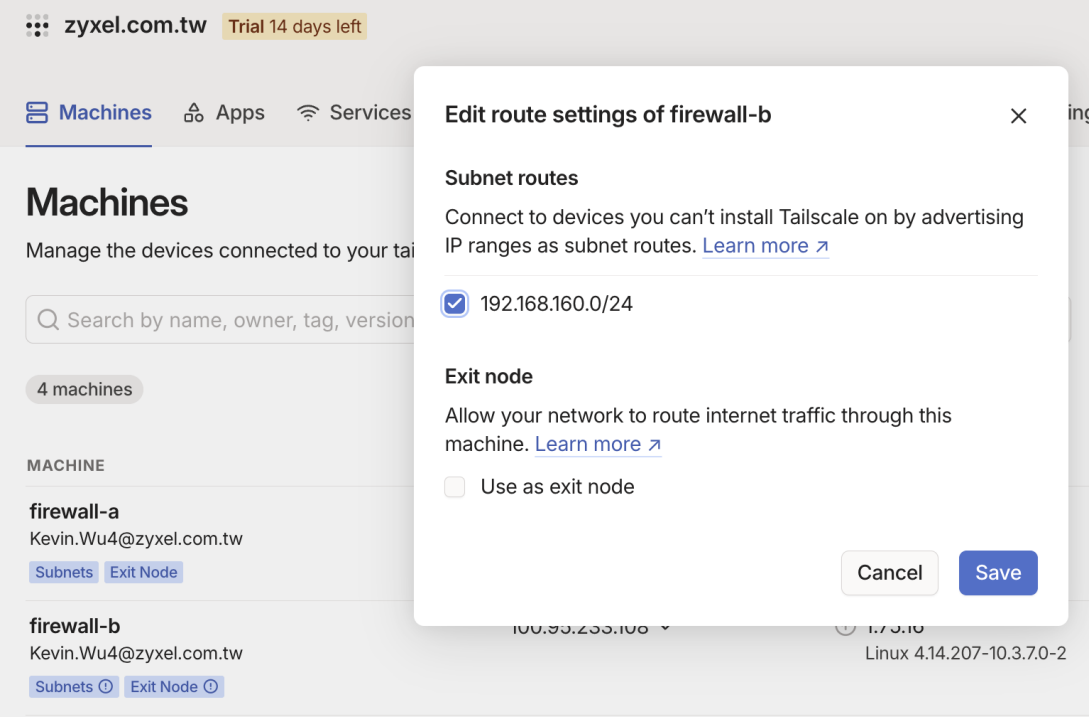
1. Advertised 192.168.168.0/24 in Firewall A.



2. Advertised 192.168.160.0/24 in Firewall B.



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



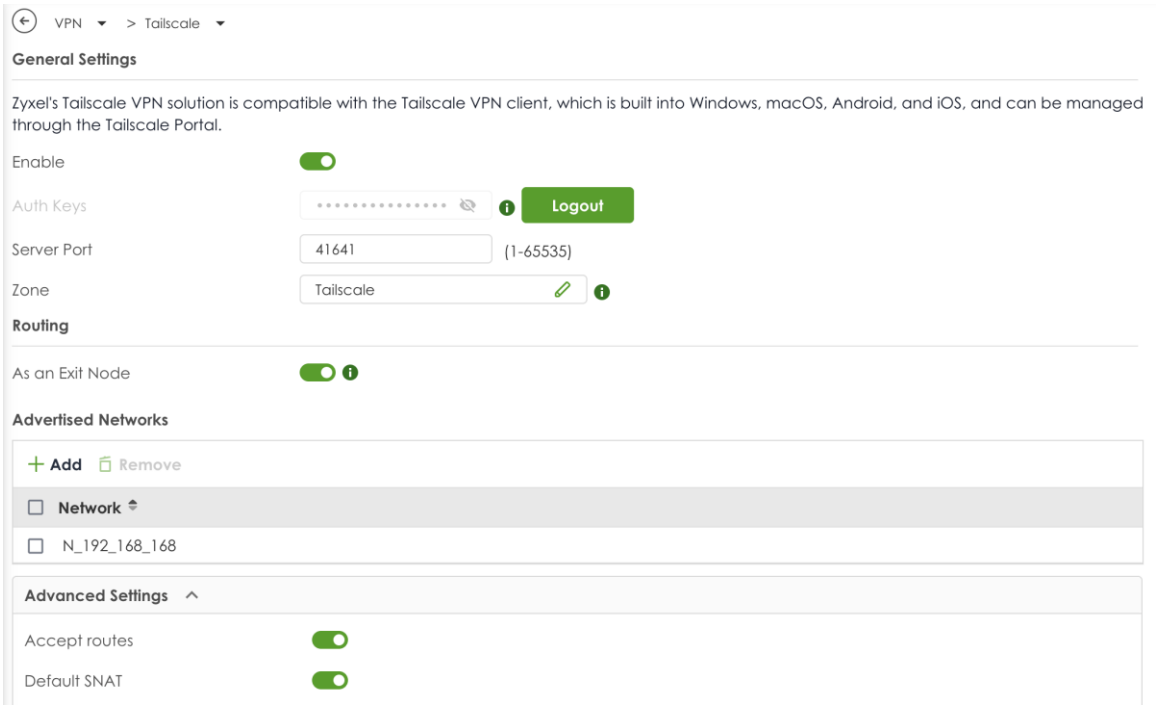
Test the Result

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

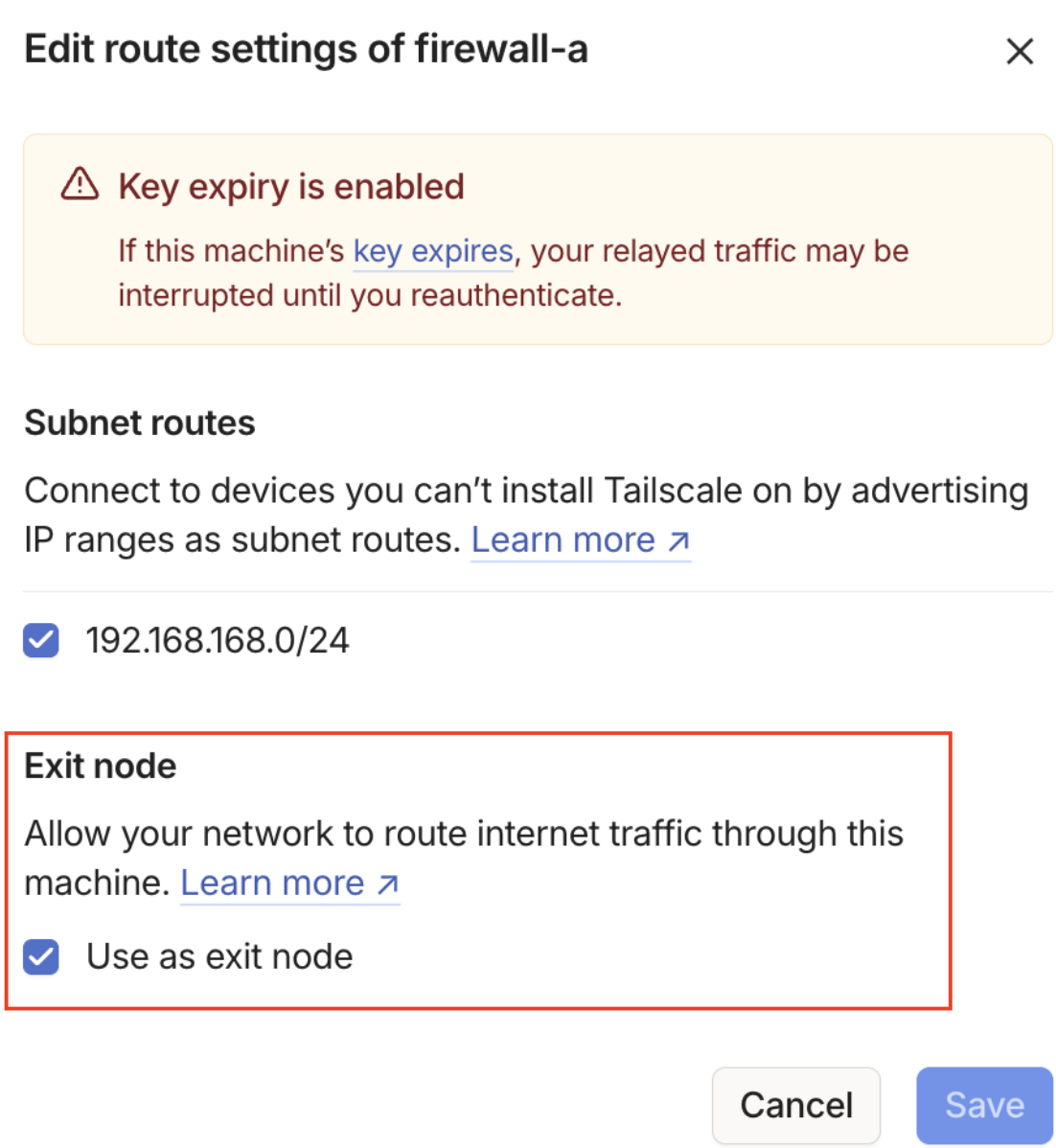
```
C:\Users\NT03234\Downloads>route print | findstr "192.168.168.0 192.168.160.0"
    192.168.160.0    255.255.255.0  100.100.100.100     100.95.1.123      0
    192.168.168.0    255.255.255.0  100.100.100.100     100.95.1.123      0

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

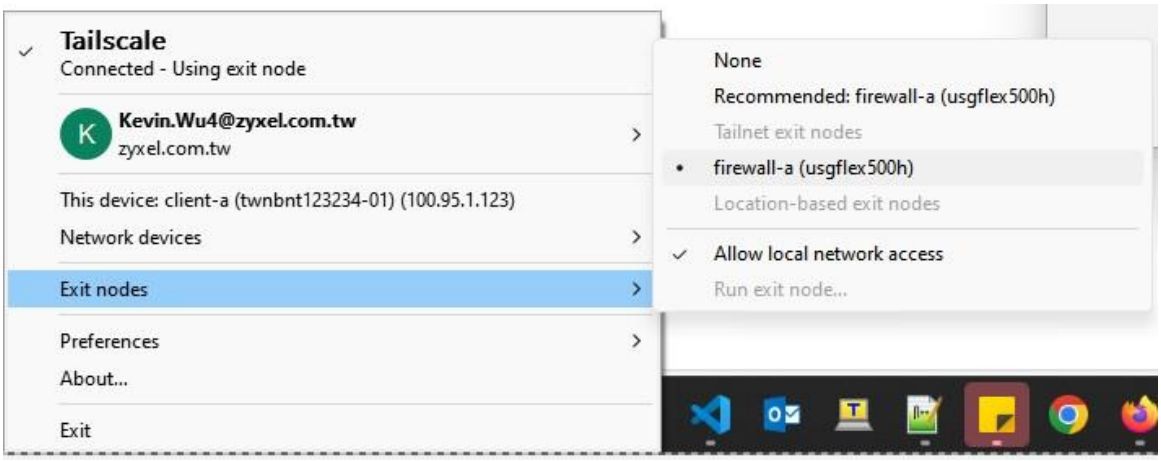
1. Take Firewall A as example. Enable “Exit Node” and “Default SNAT”.



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



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

  1     2 ms     2 ms     1 ms  100.115.120.97
  2     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@wujiaxuandeMacBook-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 0xffffff00 broadcast 192.168.168.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (1000baseT <full-duplex>)
        status: active
kevin@wujiaxuandeMacBook-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

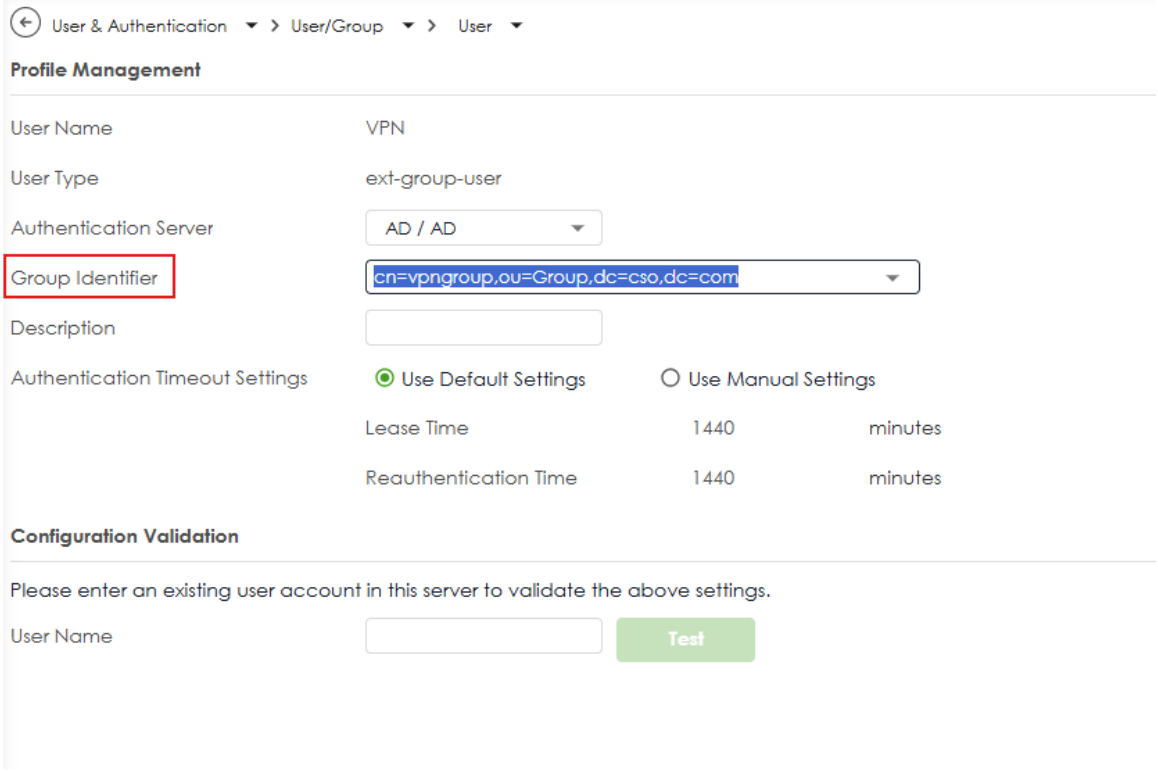
Remote Access VPN now supports using external user groups for VPN accounts. This article will guide you through the setup process

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.

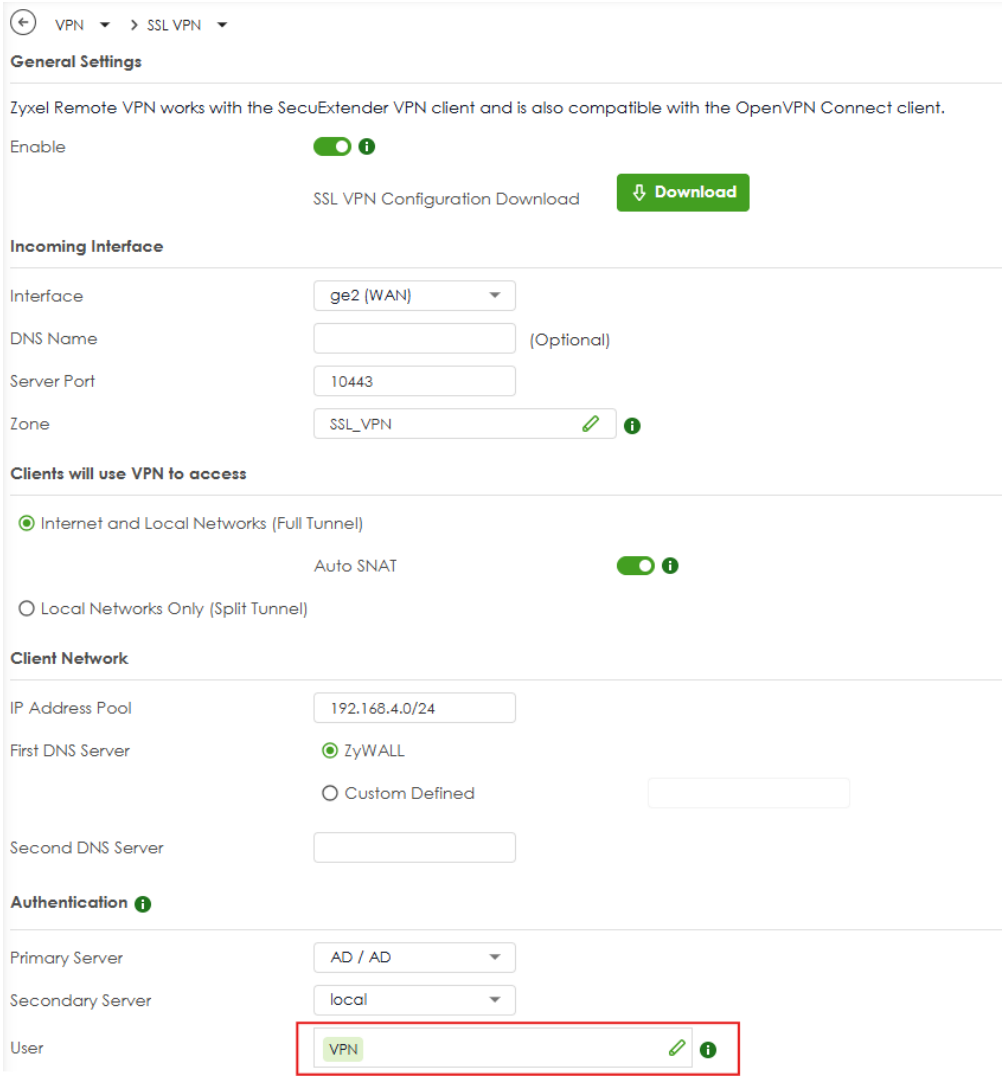
User & Authentication > User/Group > User

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.



VPN > SSL VPN

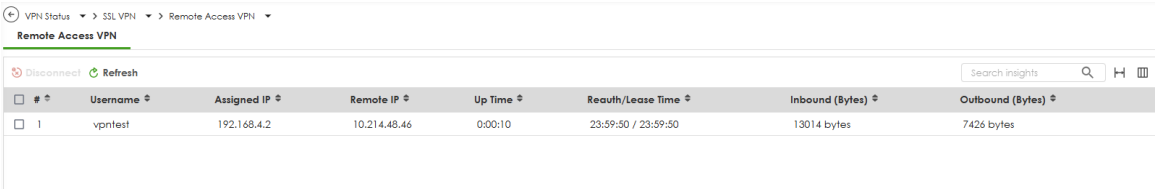
Taking SSL VPN as an example, User select the ext-group user you just created. And choosing AD authentication.



Test the Result

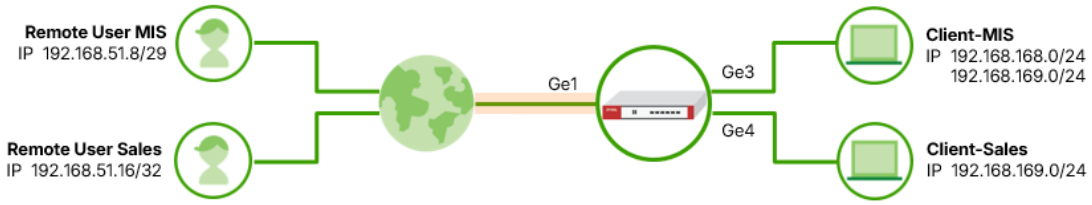
VPN Status > SSL VPN > Remote Access VPN

User within the group can successfully connect



How to Configure SSL VPN Access Profile

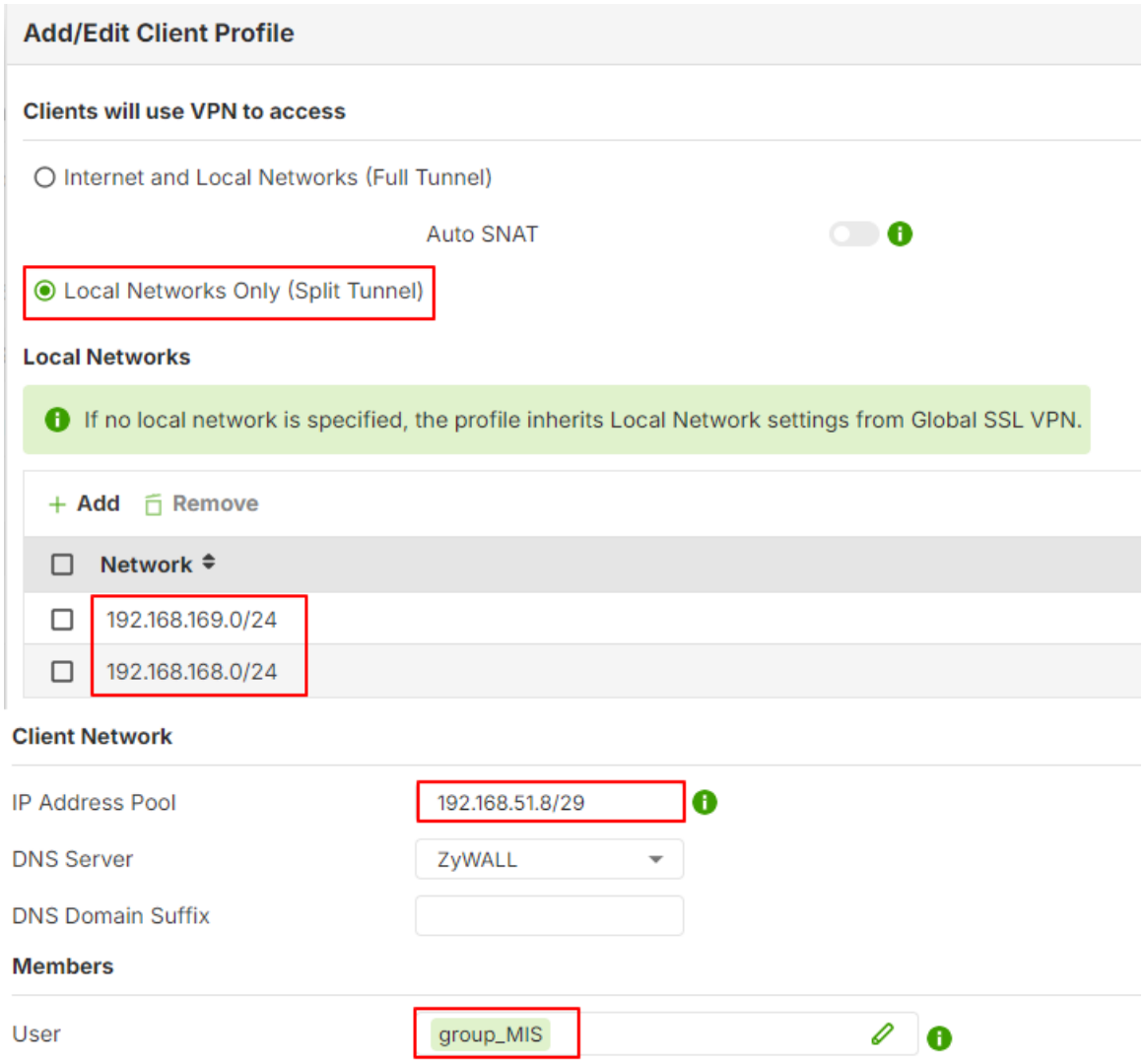
With multiple SSL VPN client profiles, you can create one or more profiles to apply its own settings such as IP pool, DNS and tunnel type to specific users. This example illustrates how to create multiple SSL VPN client profiles for different groups.



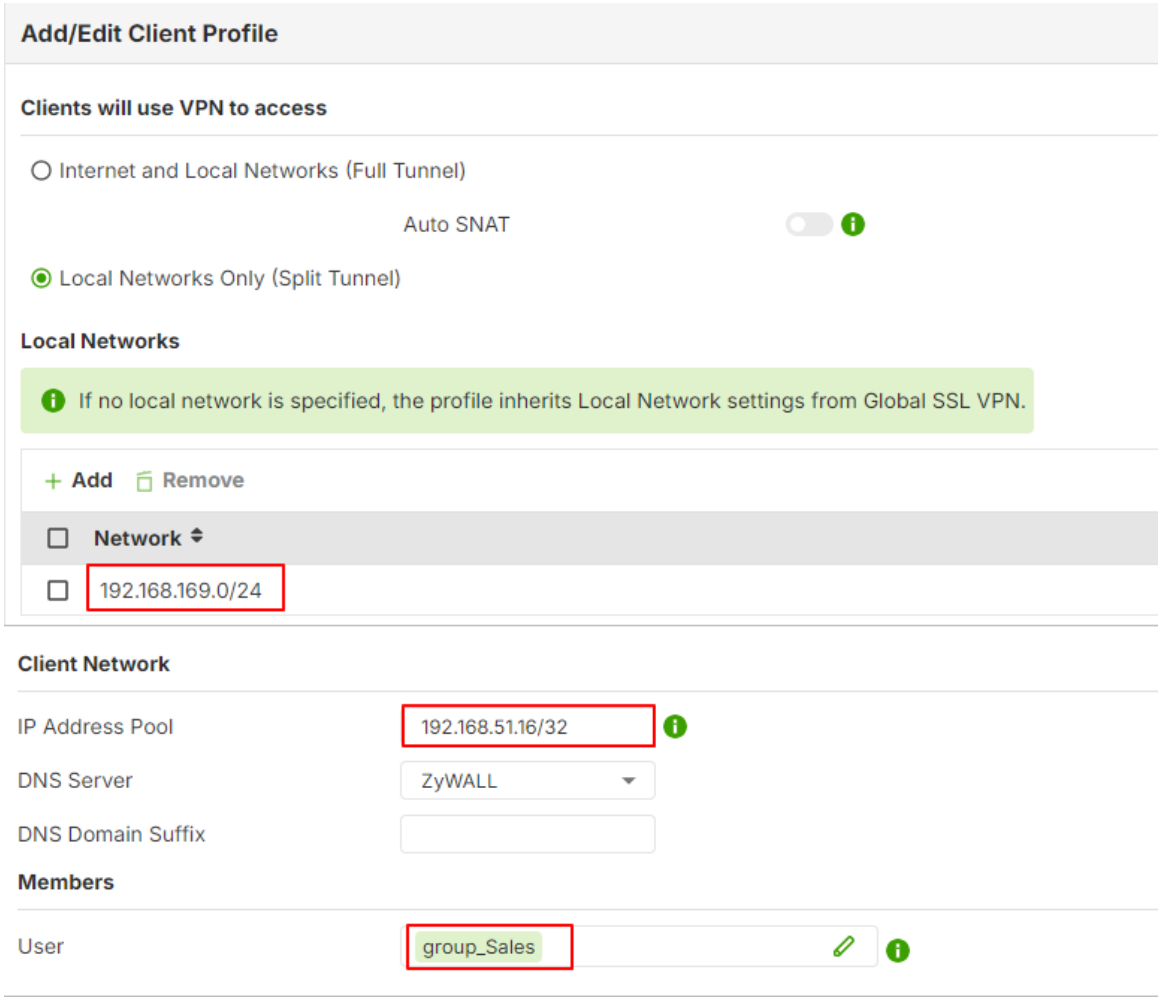
Note: This feature is supported from firmware version uOS 1.38.

Add Client Profiles

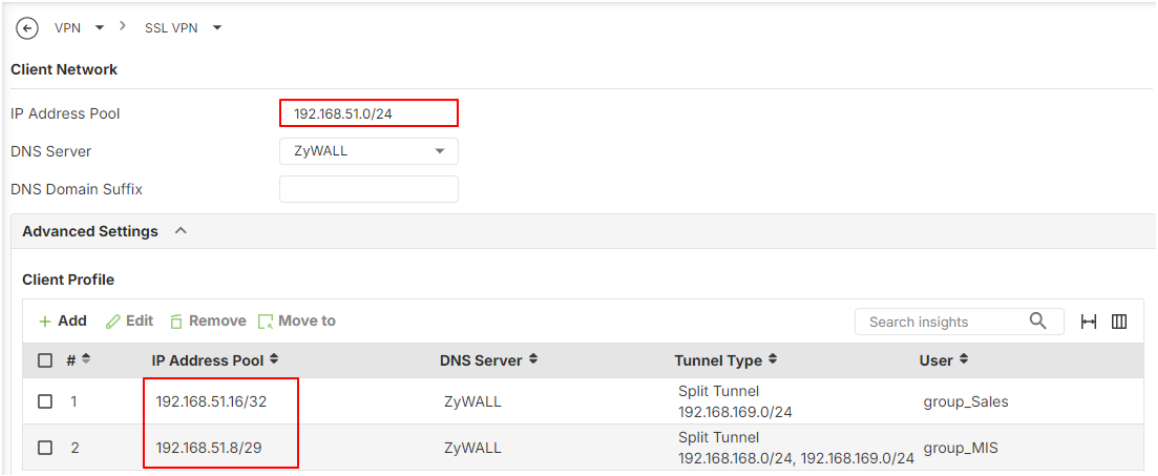
1. Go to VPN > SSL VPN > Advanced Settings > Client Profile and click +Add to add a client profile for MIS. In this example, users in group_MIS can access the network 192.168.168.0/24 and 168.168.169.0/24 after establishing SSL VPN.



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

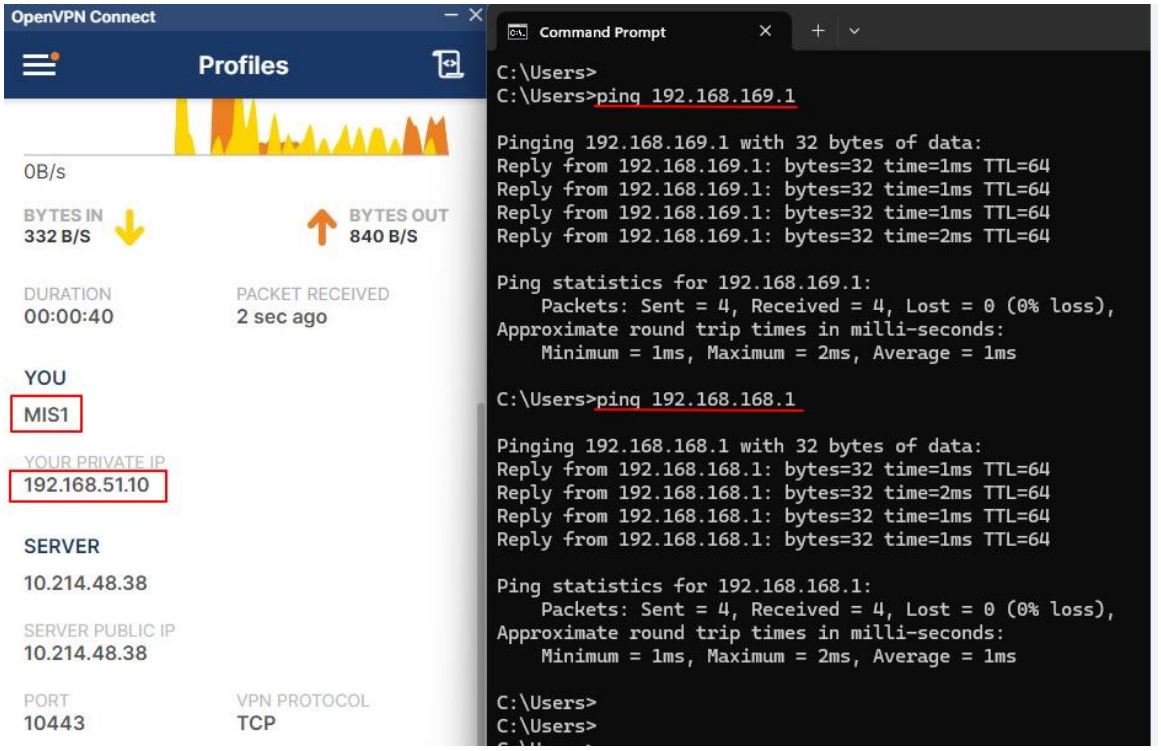


3. Check the client profiles.
   - The IP Address Pool of a client profile must be within the global SSL VPN IP Address Pool range. In this example, the global IP address Pool is 192.168.51.0/24, and the IP address Pool of client profiles are 192.168.51.16/29 and 192.168.51.8/29.
   - The IP Address 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



Verification

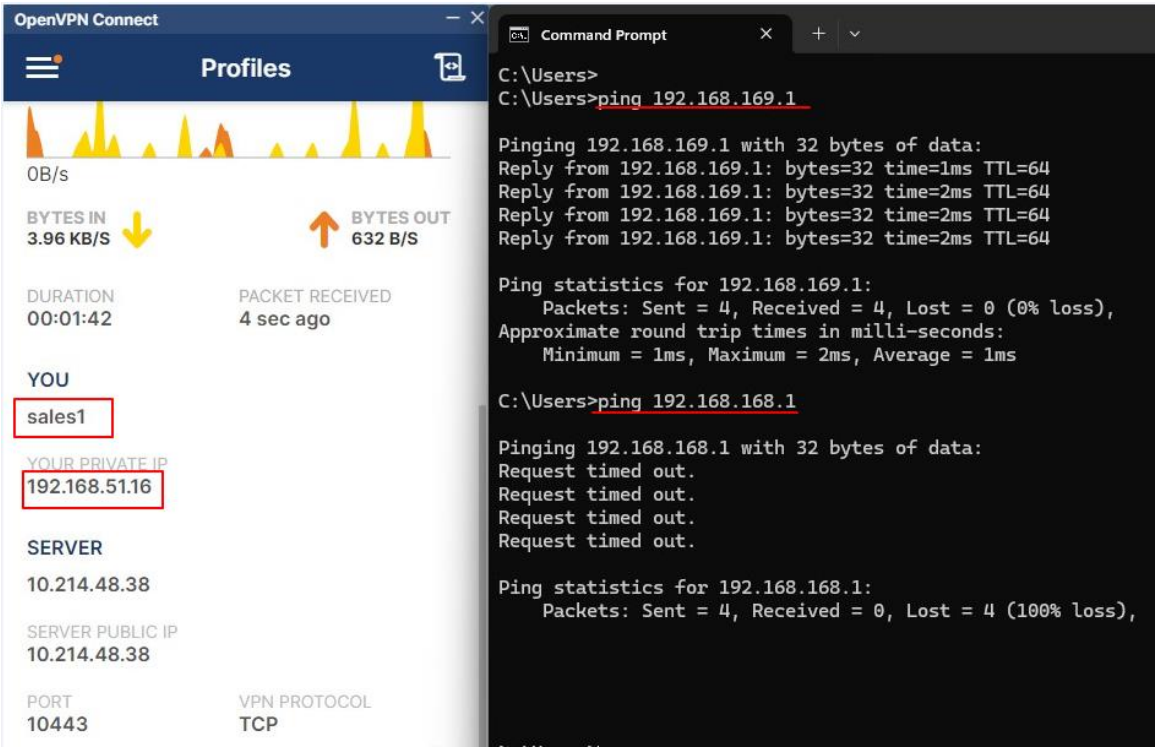
1. Go to VPN > SSL VPN. Download SSL VPN configuration file and import the file to OpenVPN client.
2. Enter the username “MIS1” and the password to connect SSL VPN. The user “MIS1” receives the IP address 192.168.51.10 and can access both 192.168.168.0/24 and 192.168.169.0/24.



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

3. 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.



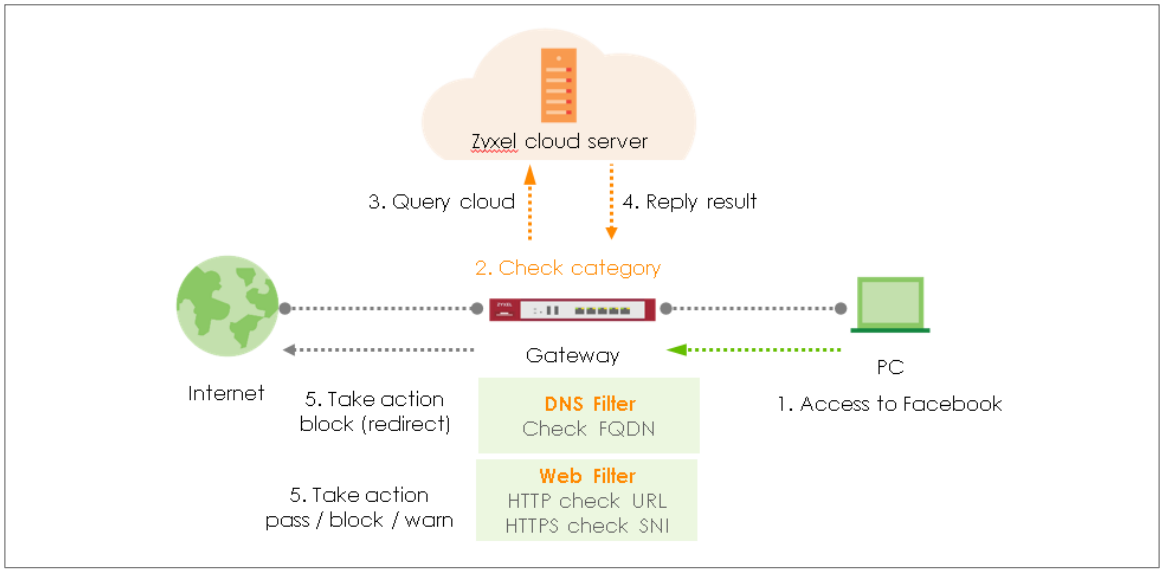
Verify the SSL VPN status in Log & Report > System.

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.

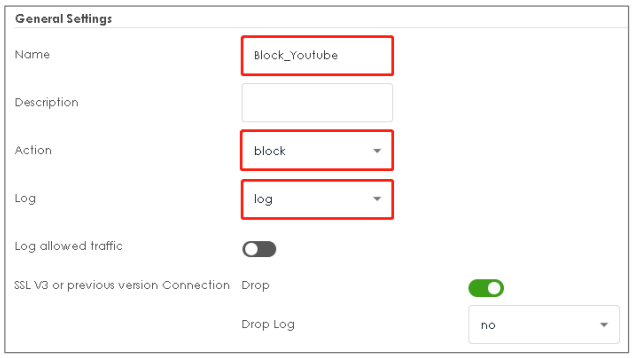


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

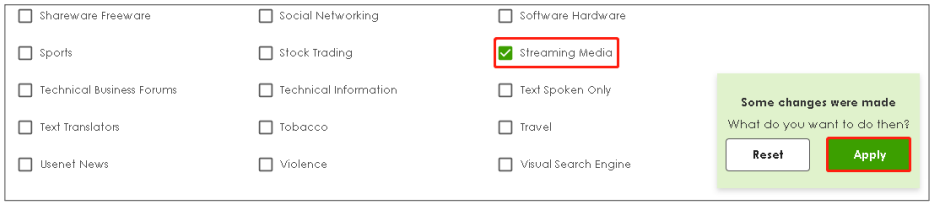
Set Up Content Filter

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

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

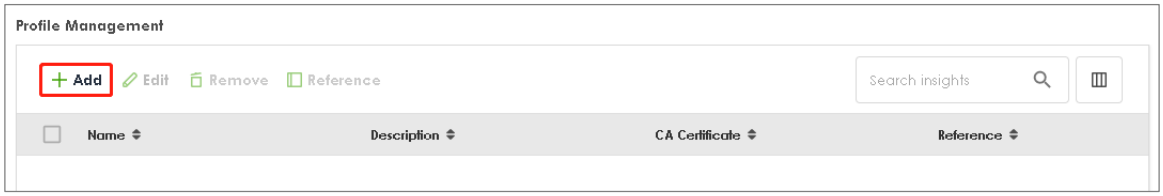


Tick Streaming Media category in Managed Categories, and click Apply.

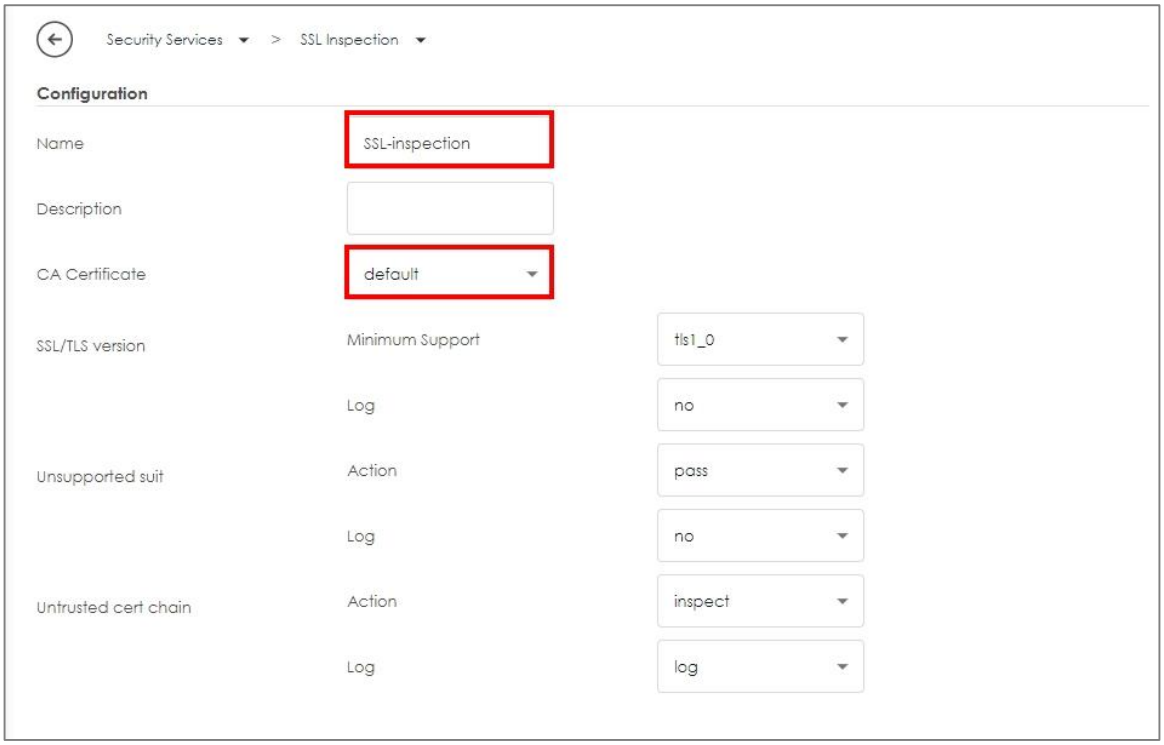


Set Up SSL Inspection

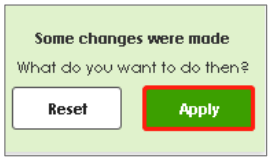
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



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



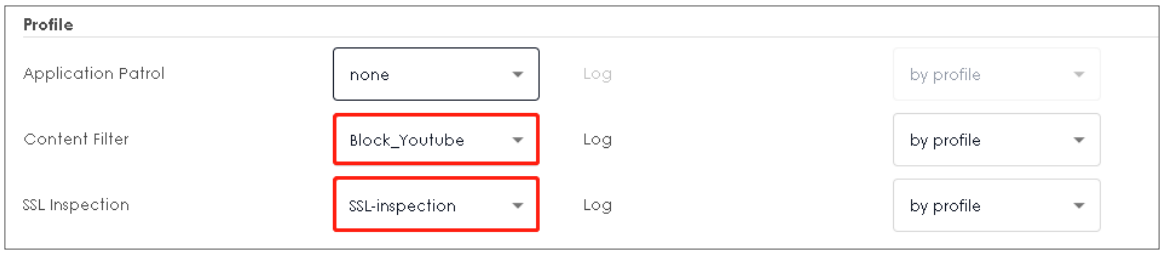
Click Apply to add SSL Inspection profile.



Set Up the Security Policy

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

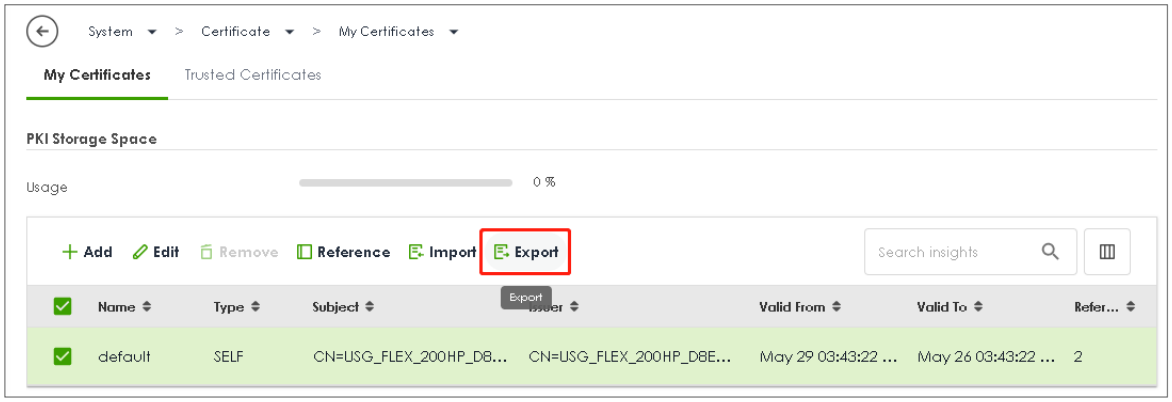
Select Content Filtering, and SSL Inspection. Click Apply to save.



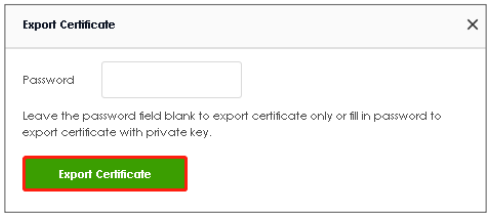
Export Certificate from FLEX and Import it to Windows

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.

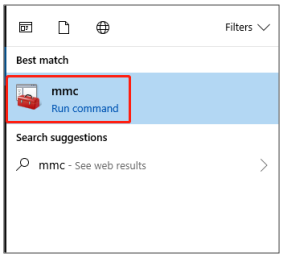
Go to System > Certificate > My Certificates to export default certificate from FLEX.



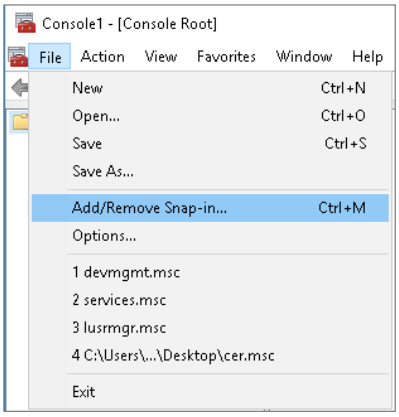
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



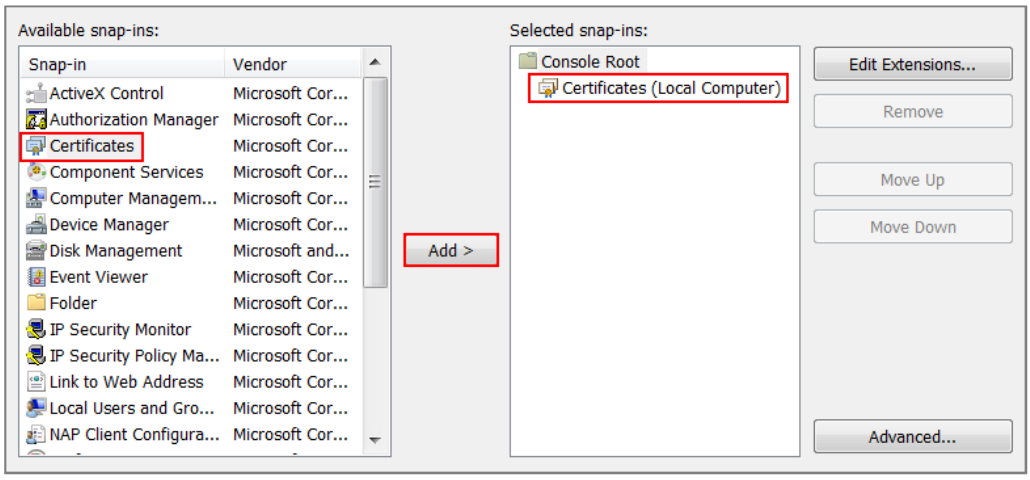
In Windows Start Menu > Search Box, type MMC and press Enter.



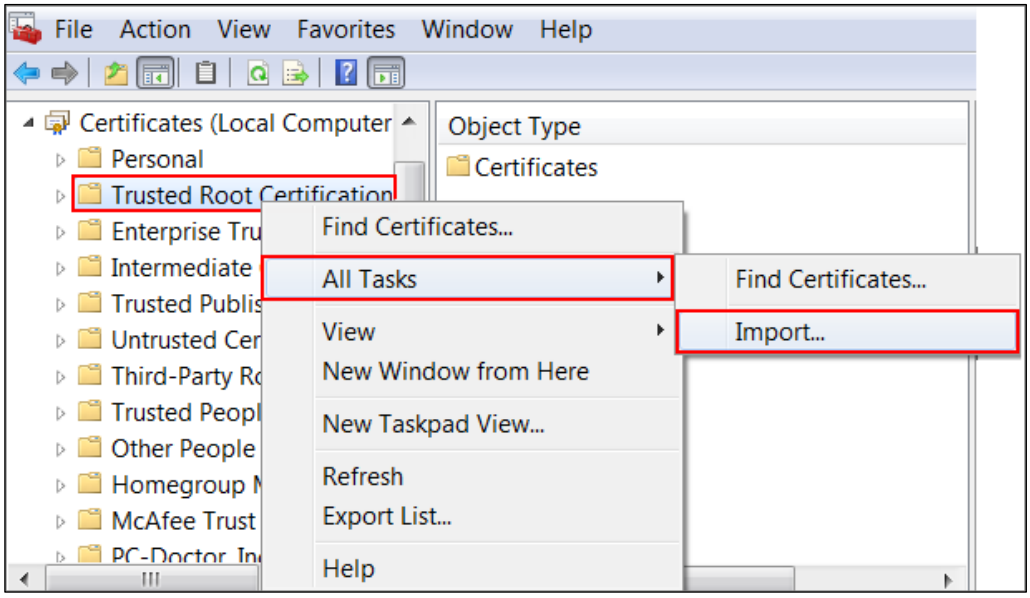
In the mmc console window, click File > Add/Remove Snap-in...



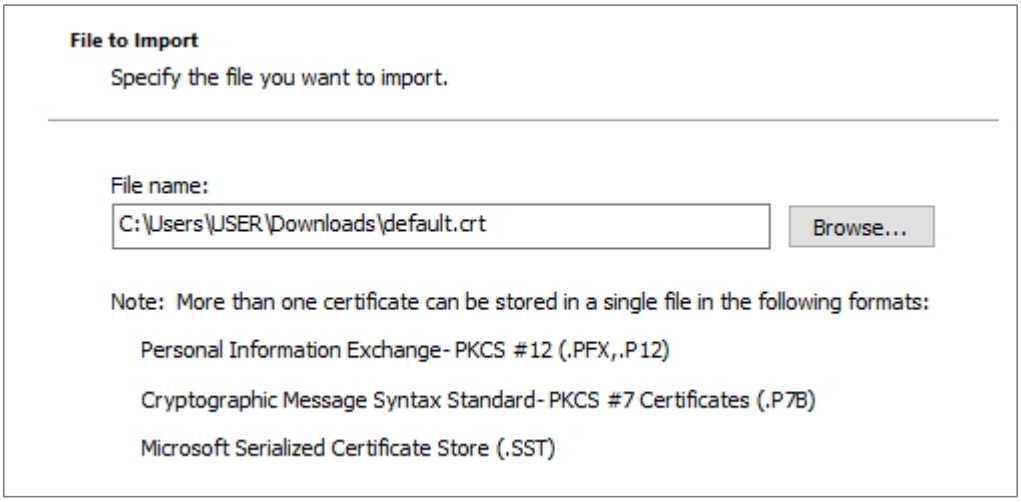
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



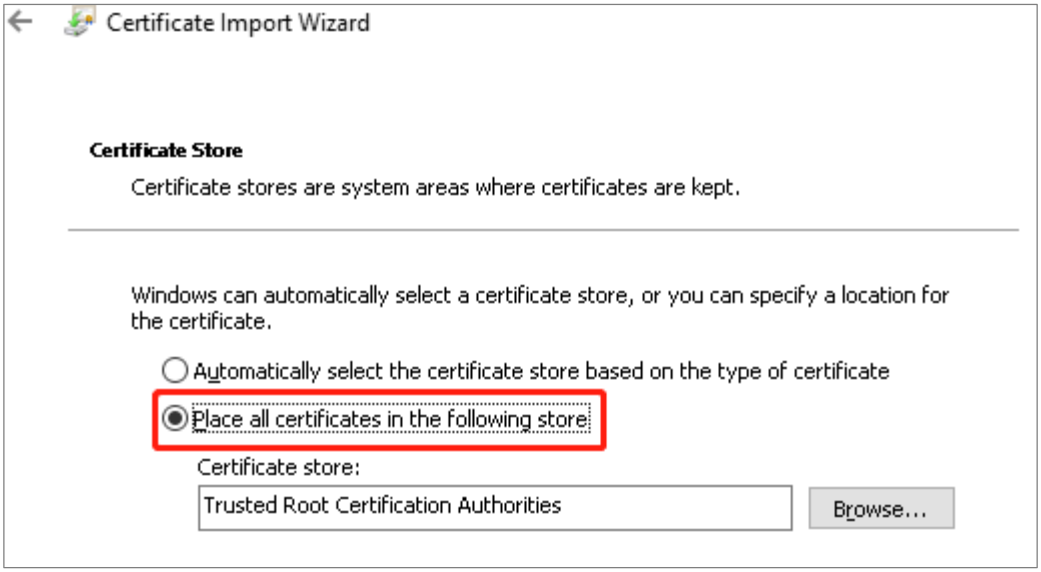
In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import...



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

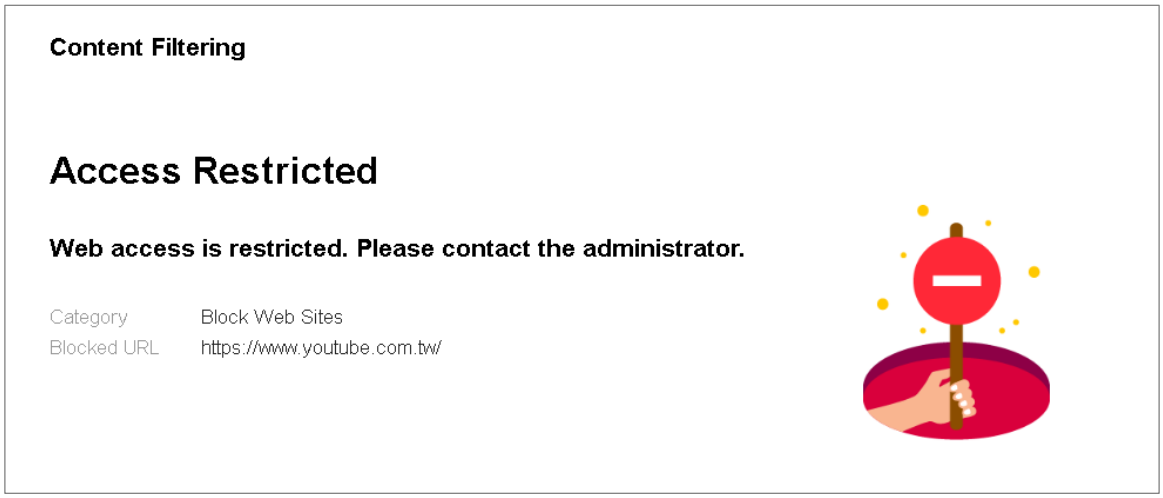


Select Place all certificates in the following store and then click Browse and find Trusted Root Certification Authorities. Click Next, then click Finish.

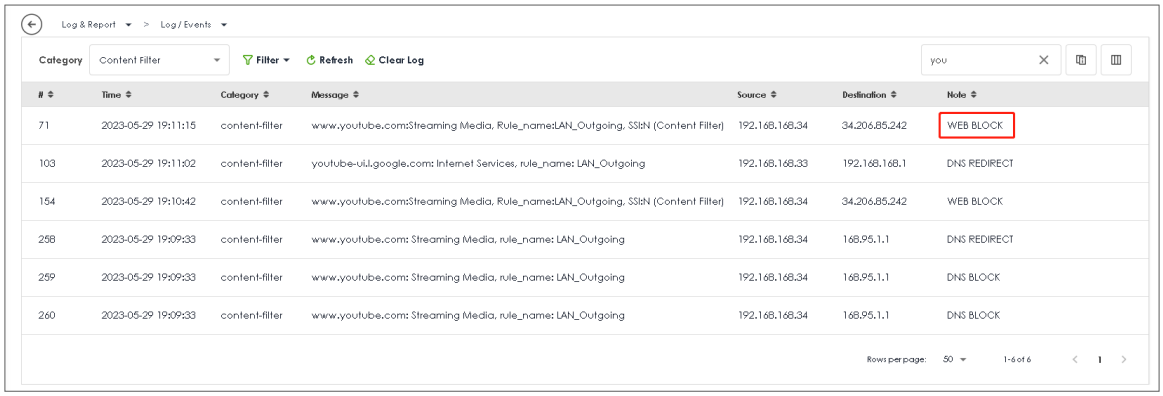


Test the Result

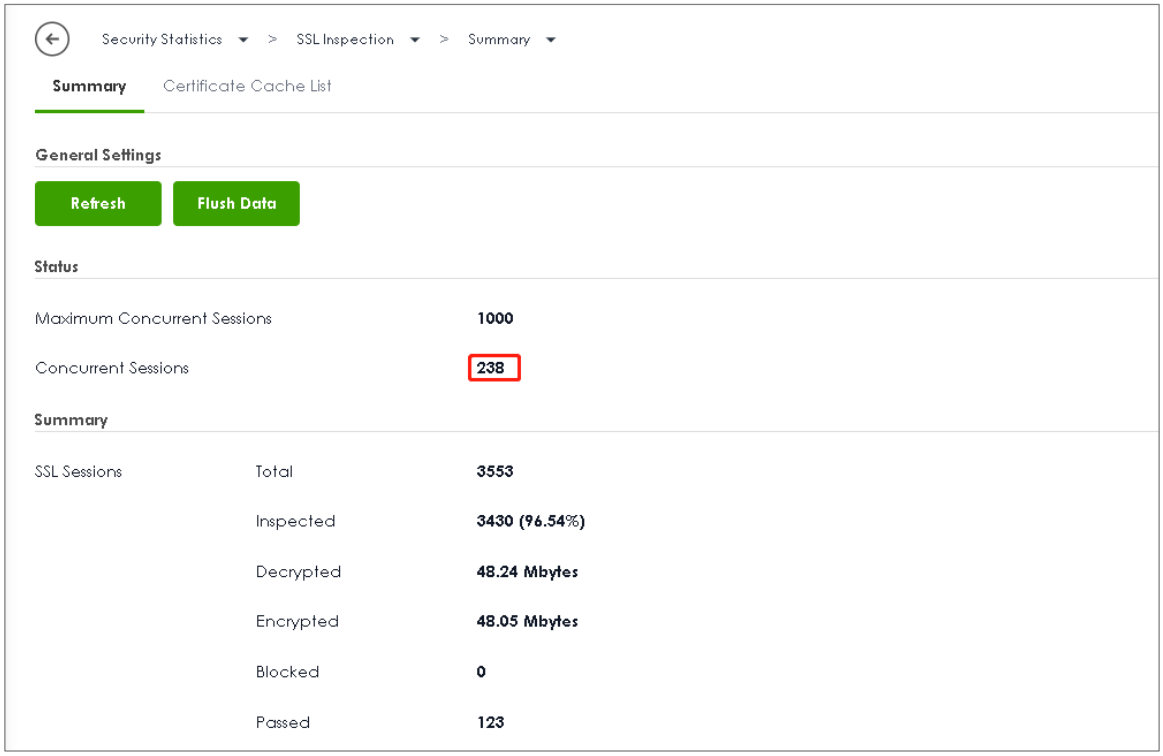
Using Web Browser to access the YouTube. The gateway will redirect you to a blocked page.



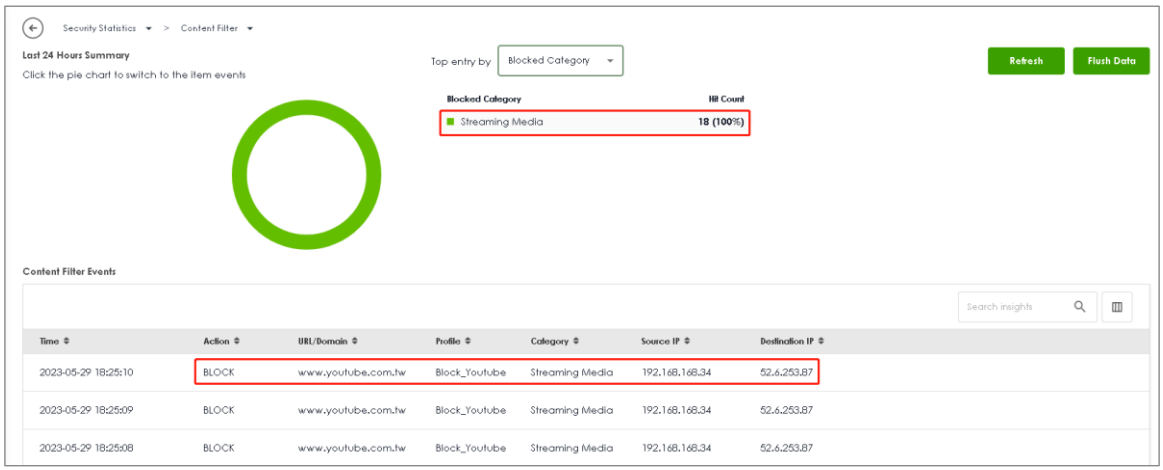
Go to Log & Report > Log/Events and select Content Filtering to check the logs.



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



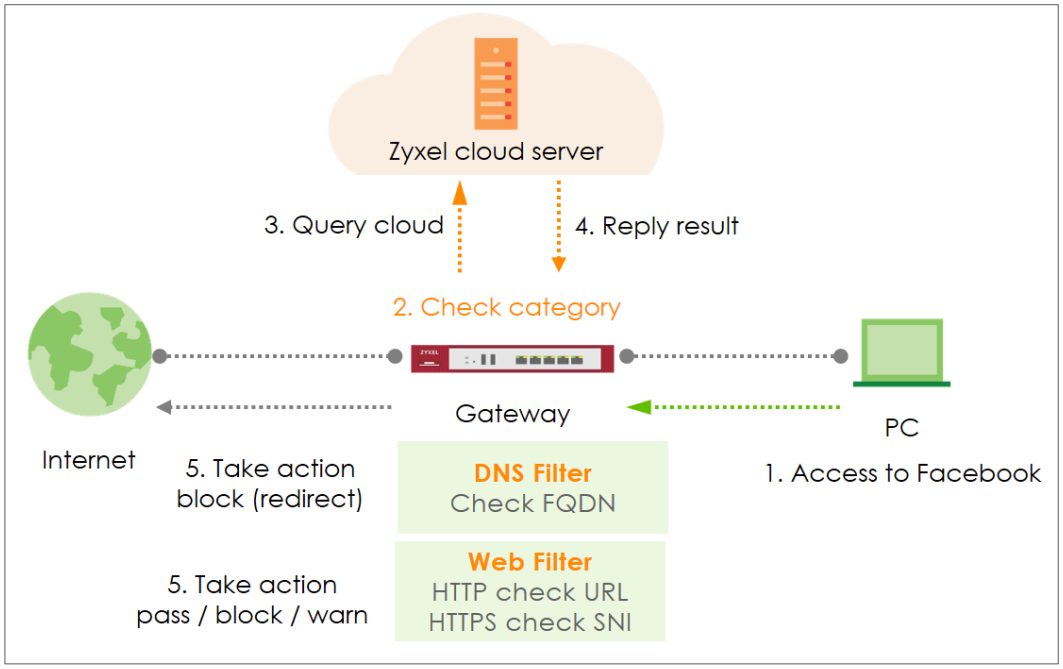
Go to Security Statistics > Content Filter to check summary of all events.



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.

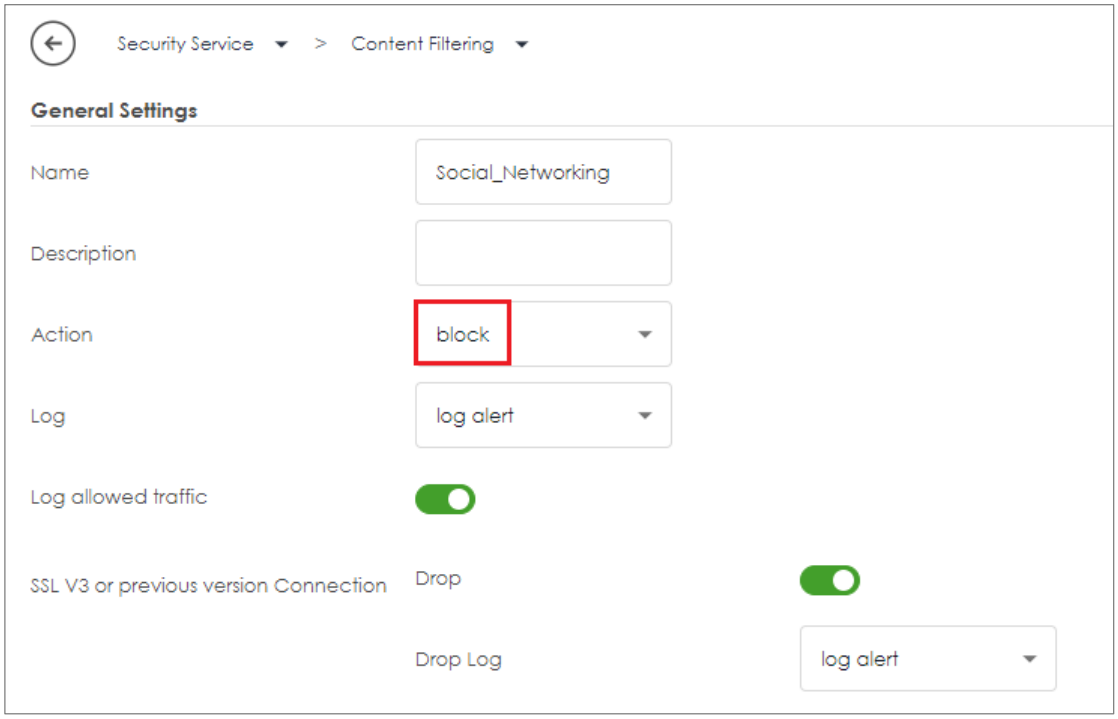
When the user makes an HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then the cloud database, then take action when it matches the block category in the Content Filter profile.



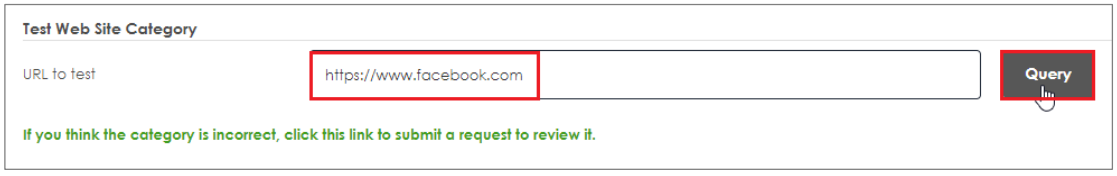
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Content Filter

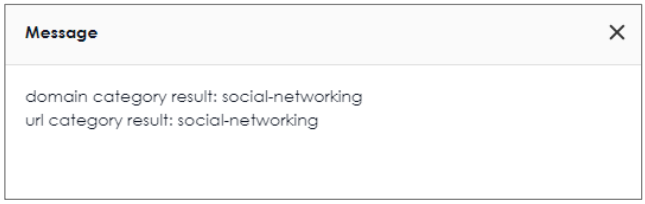
Go to **Security Service > Content Filtering > Profile Management > Add a Content Filter profile**. Configure a **Name** for you to identify the **Content Filter profile** such as "Social_Networking". Configure the **Action** to block when the Content Filter detects events.



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



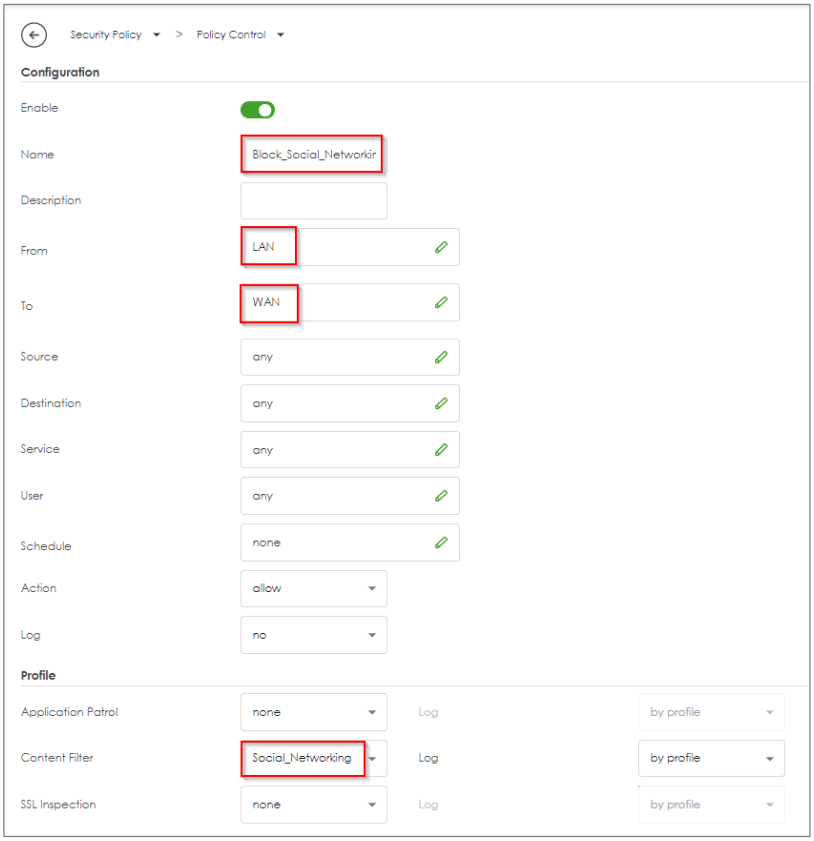
You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



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

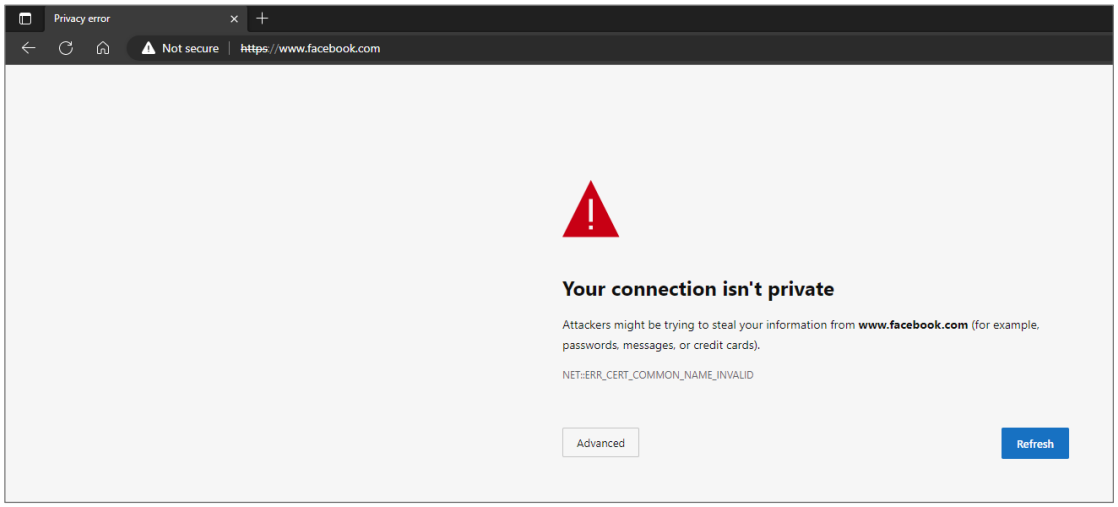
Set Up the Security Policy

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.



Test Result

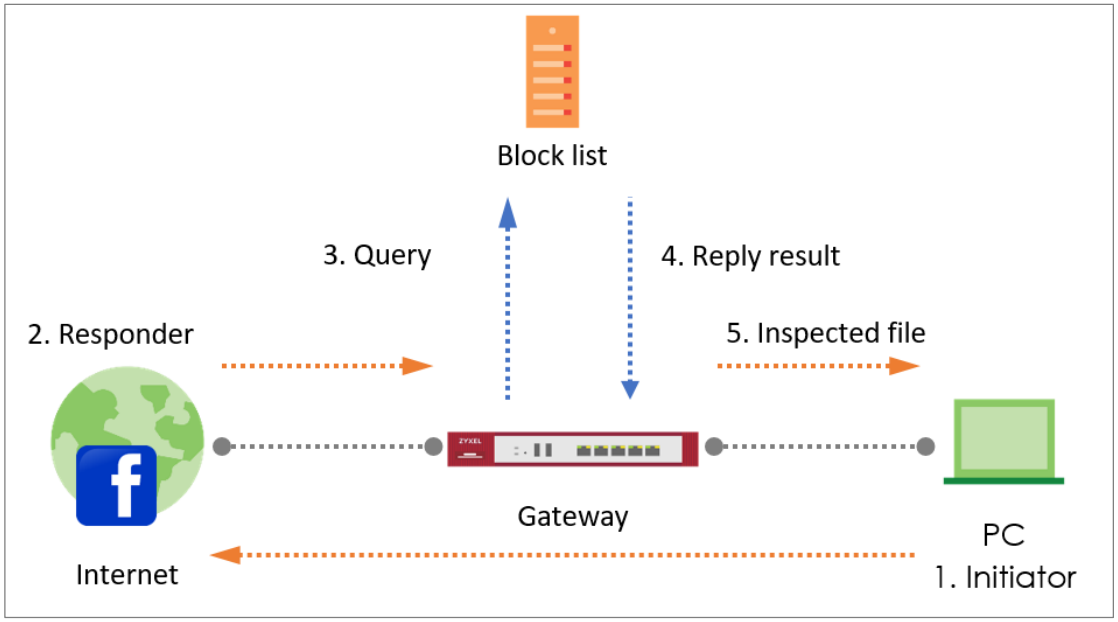
Type the URL http://www.facebook.com/ or https://www. facebook.com/ onto the browser and cannot browse facebook.



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

How to Block Facebook Using a Content Filter Block List

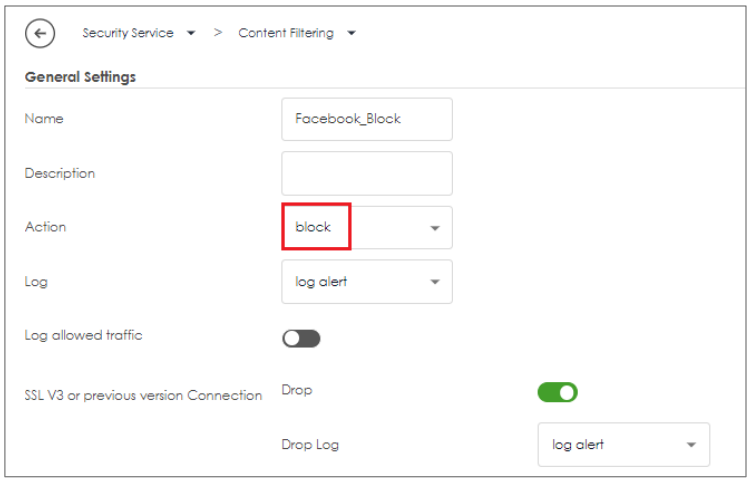
This is an example of using USG Flex H UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.



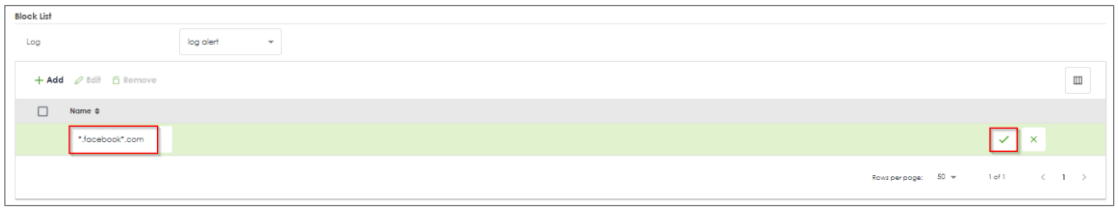
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

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.

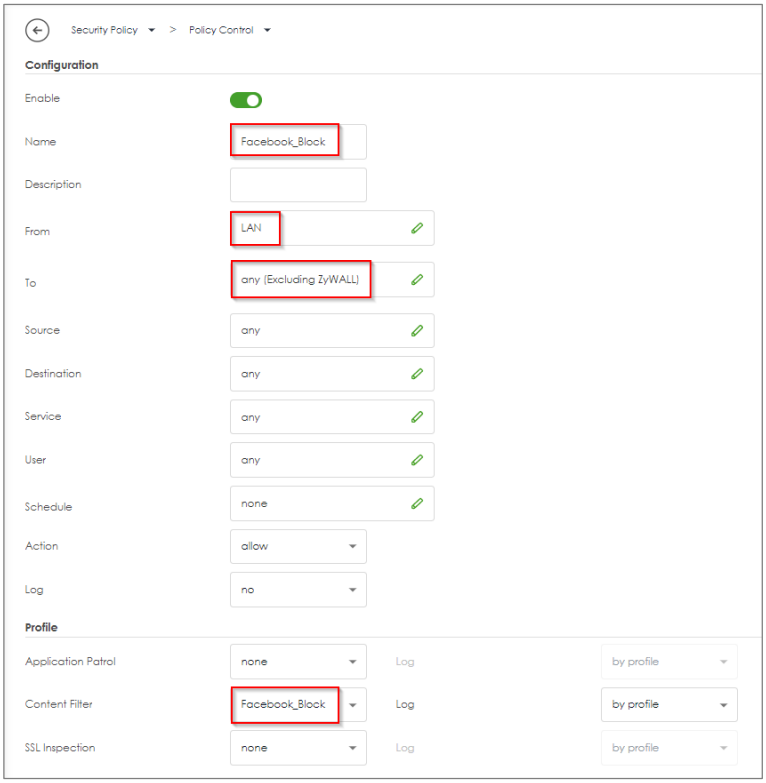


Go to **Block List** and type URL “*.facebook*.com” to add the URL that you want to block.



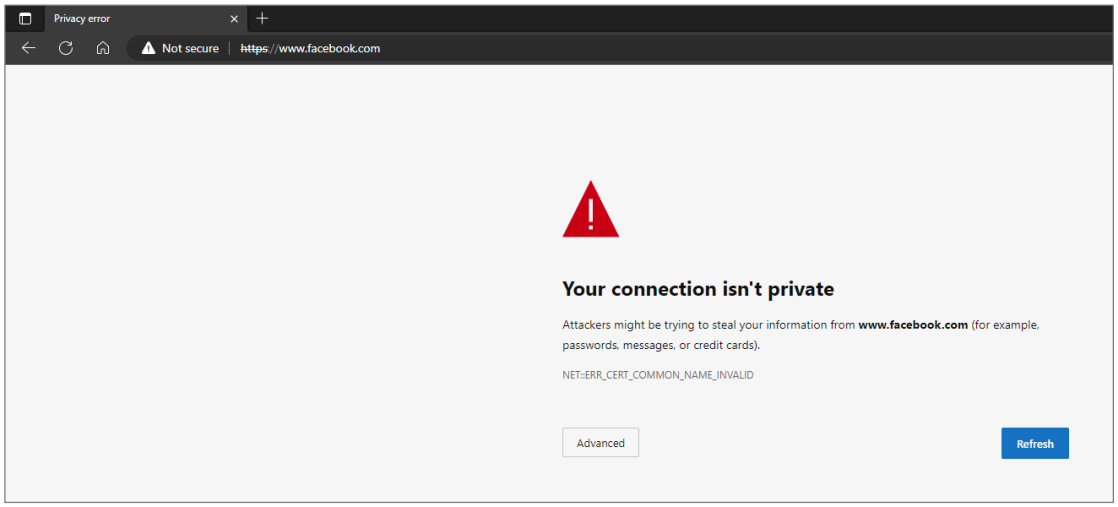
Set Up the Security Policy

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.



Test the Result

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

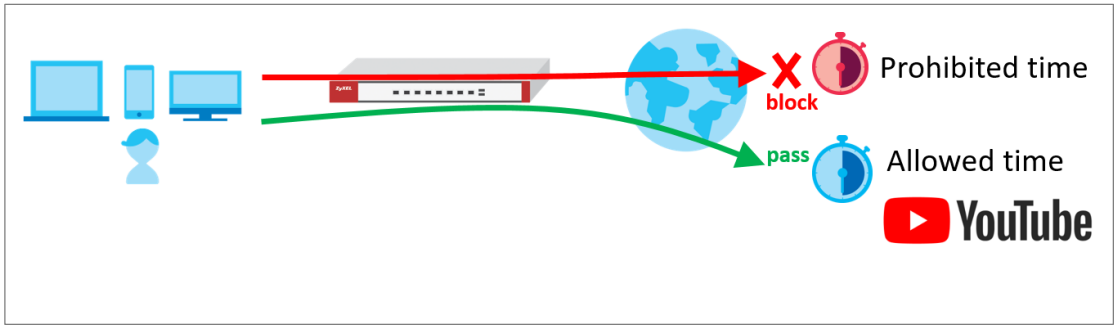


Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

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

How to block YouTube access by Schedule

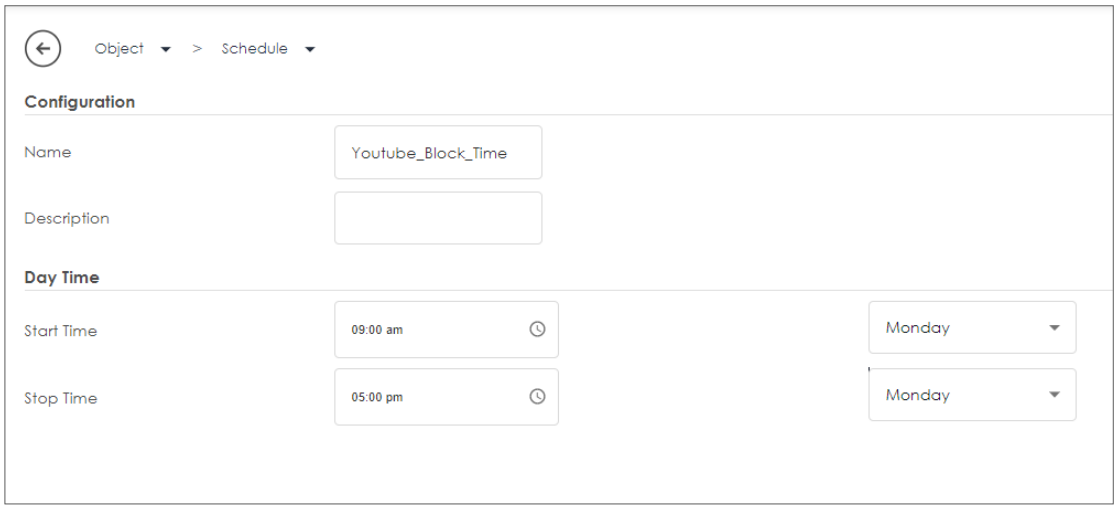
This is an example of using the USG Flex H to block access YouTube access by schedule. You can use Application Patrol and security policy with schedule settings to make sure that YouTube cannot be accessed in your network at a specific prohibited time. This article will guide you on how to deploy it.



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).

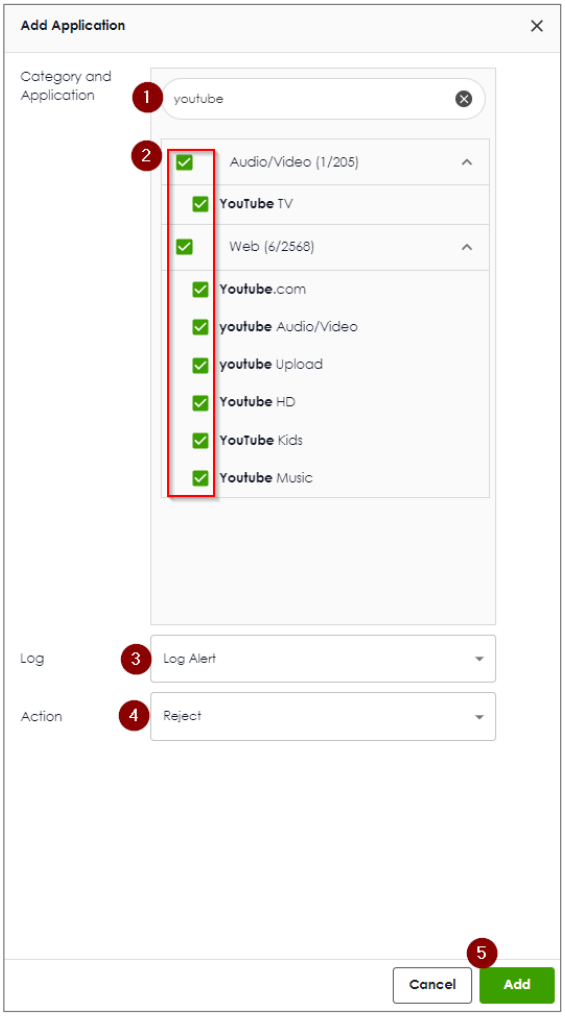
Set Up the Schedule

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.



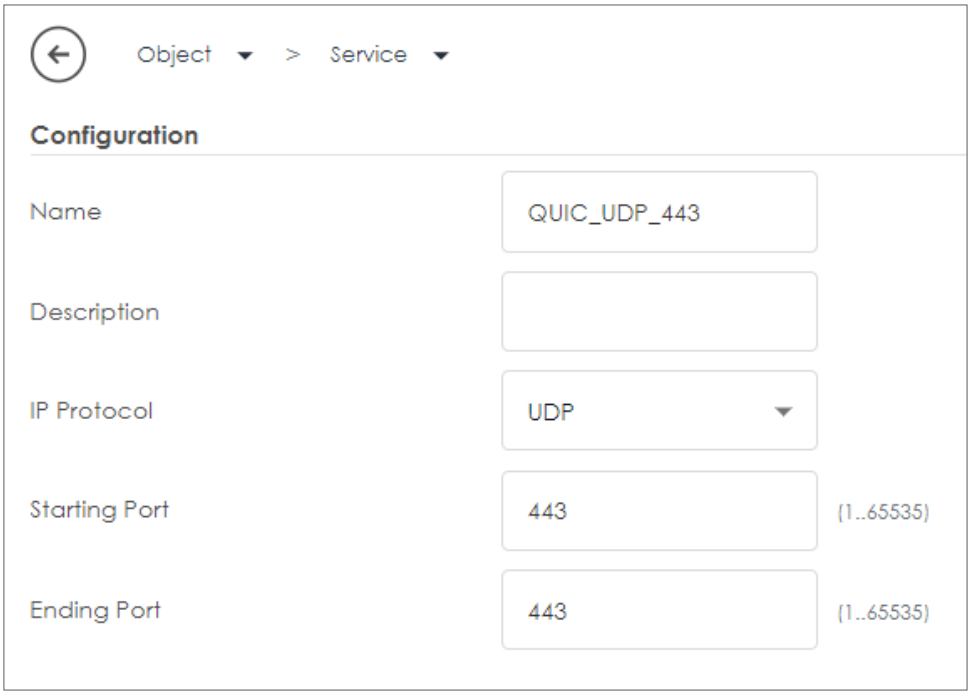
Create the Application Patrol profile

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.**



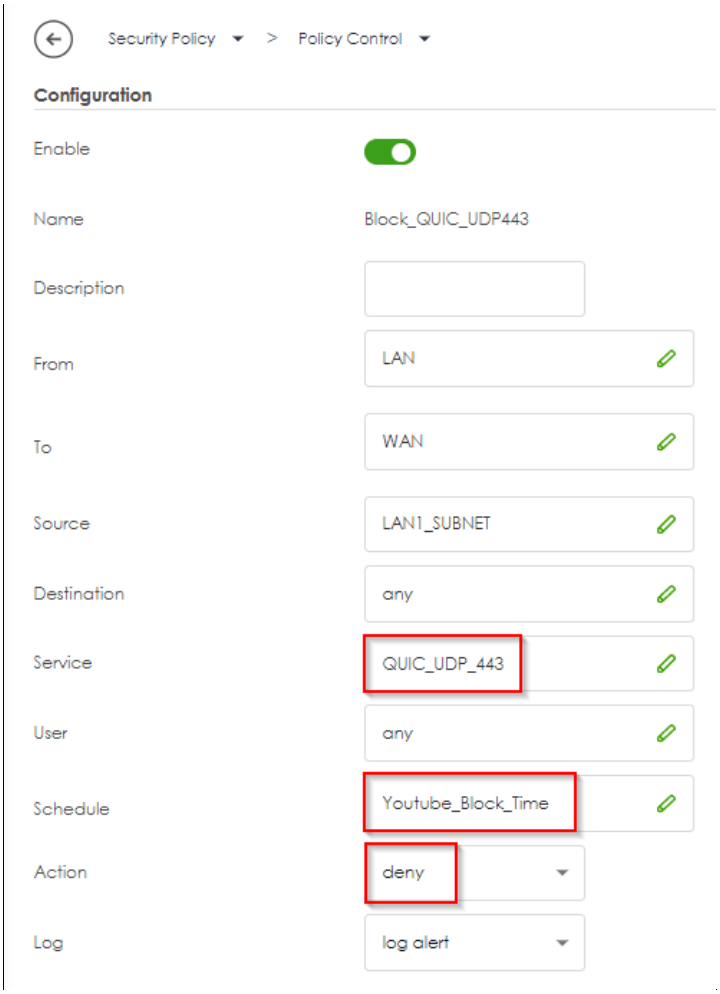
Set Up the Security Policy

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

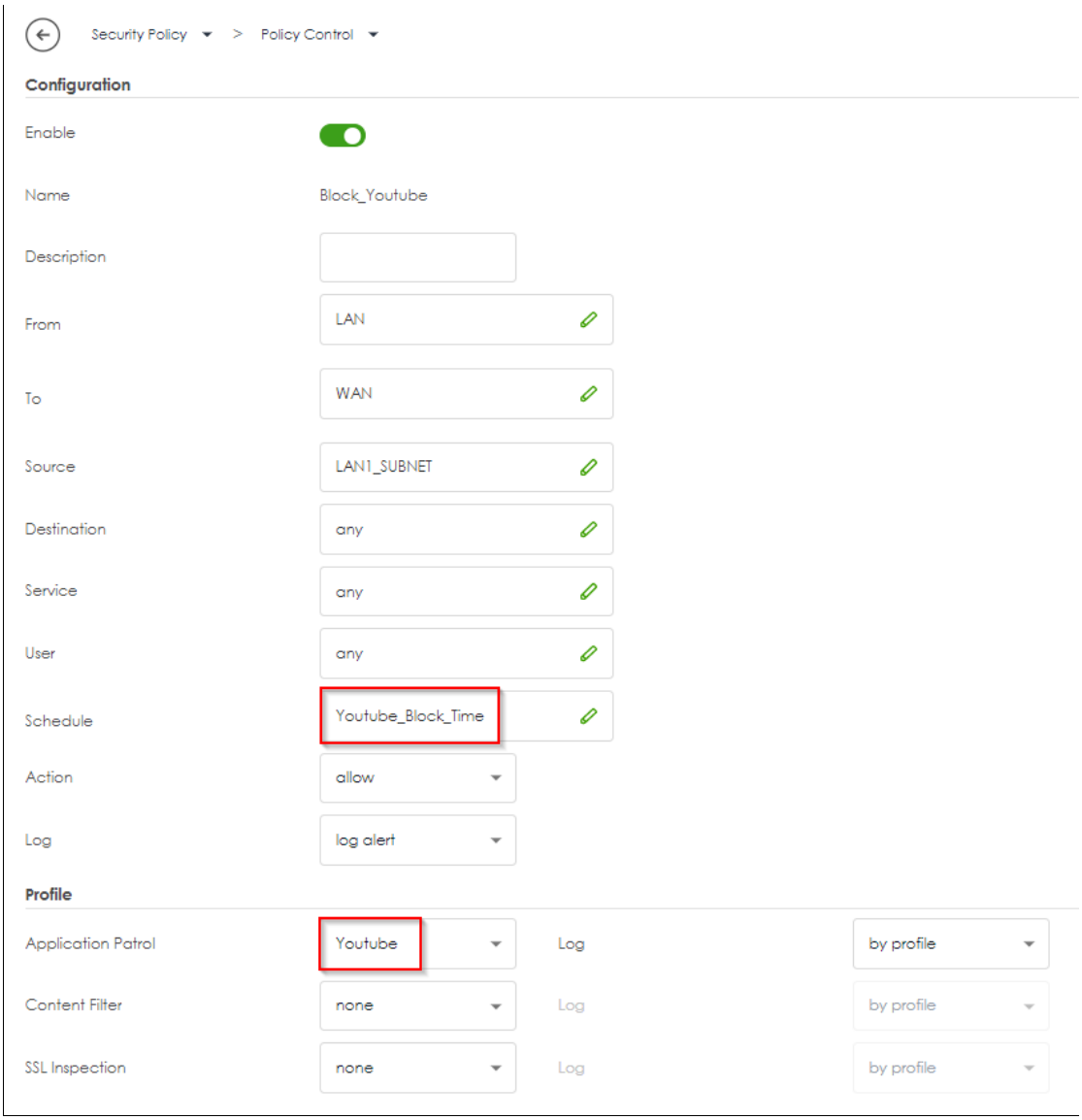


Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **service** QUIC_UDP443 and select the **Schedule** that defines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

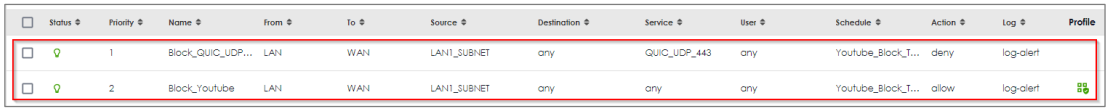
In this example, select “Youtube_Blocked_Time”.



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.



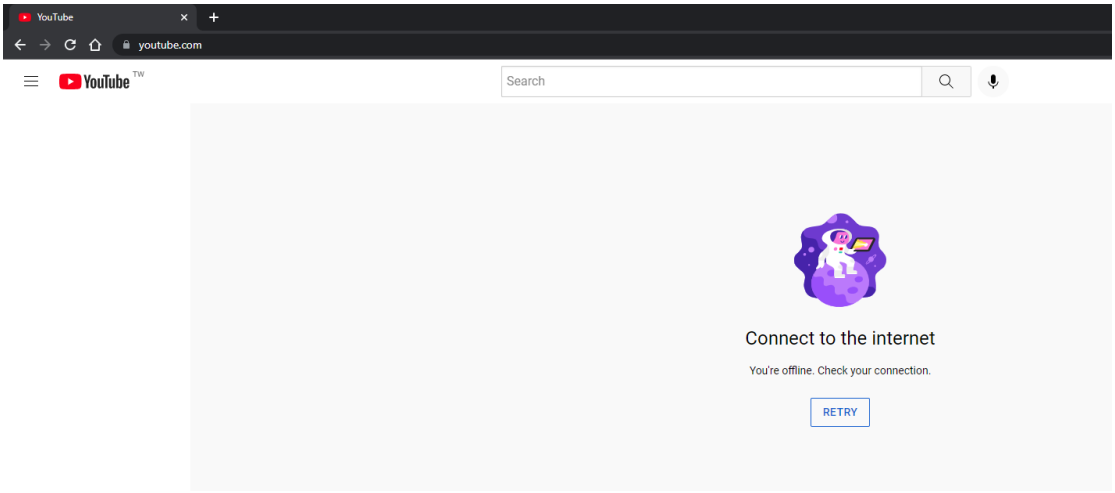
Then go back to the security policy page and move the security priority of block UDP 443 is higher than block YouTube by schedule.



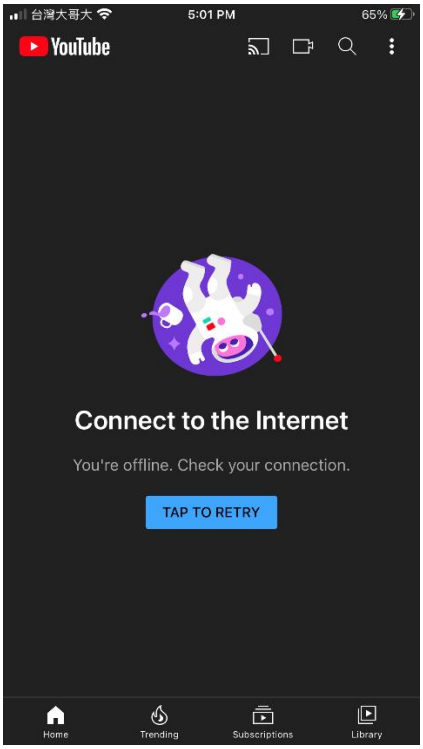
	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
☐		1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
☐		2	Block_Youtube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log-alert	

Test the Result

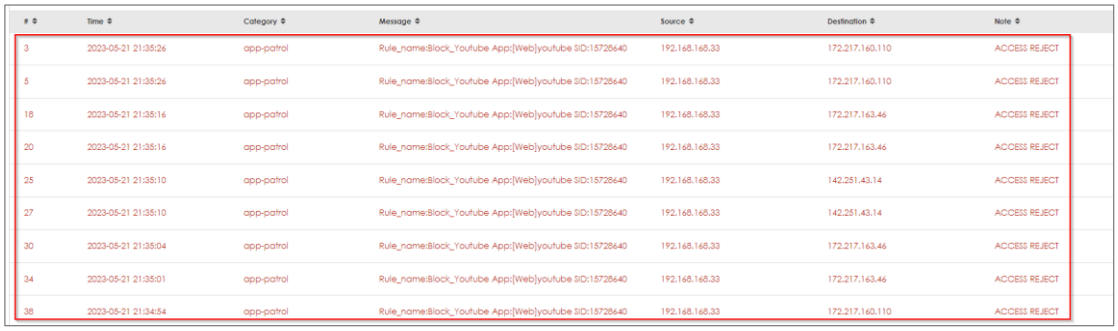
Type the URL http://www.youtube.com/ or https://www.youtube.com/ onto the browser and cannot browse YouTube.



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



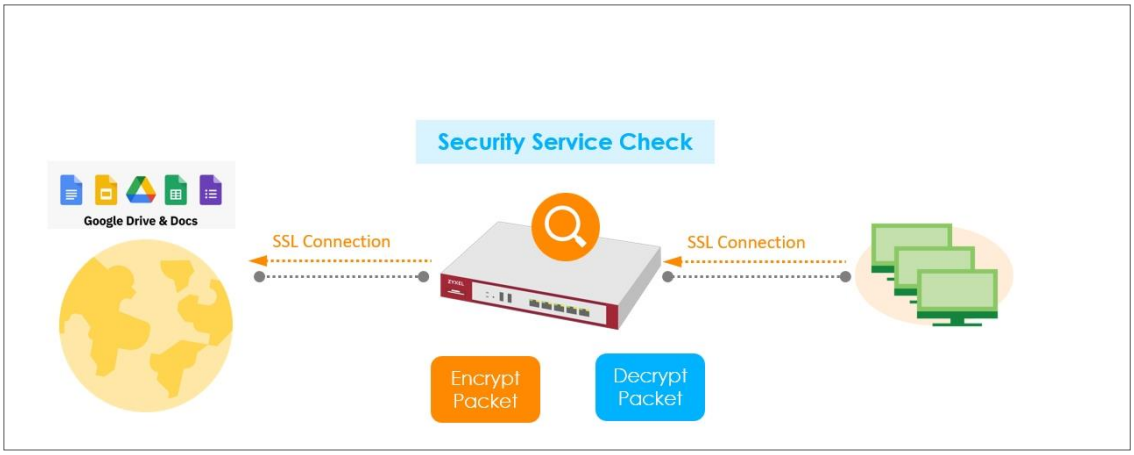
Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.



#	Time	Category	Message	Source	Destination	Note
3	2023-05-21 21:35:26	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT
5	2023-05-21 21:35:26	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT
18	2023-05-21 21:35:16	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
20	2023-05-21 21:35:16	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
25	2023-05-21 21:35:10	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	142.251.43.14	ACCESS REJECT
27	2023-05-21 21:35:10	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	142.251.43.14	ACCESS REJECT
30	2023-05-21 21:35:04	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
34	2023-05-21 21:35:01	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
38	2023-05-21 21:34:54	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT

How to Control Access to Google Drive

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



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

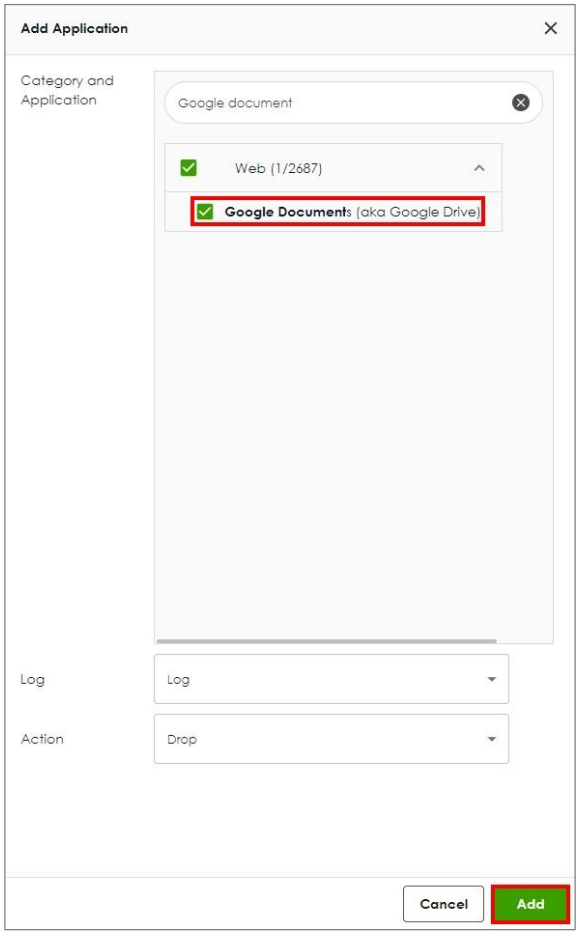
Create app patrol profile

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

Click add to add application in this profile.

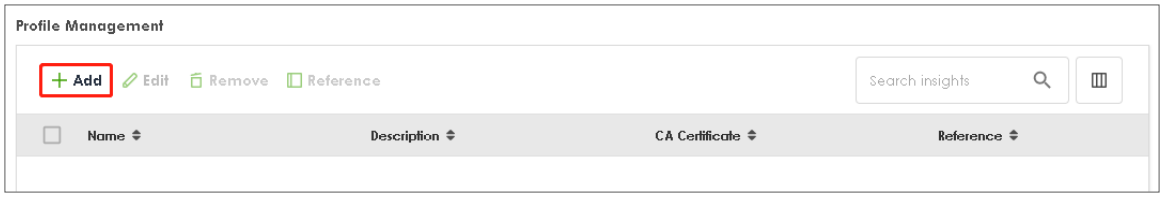
Search **Google Documents(aka Google Drive)**, and select this Application.

Action set to Drop, and click Add.

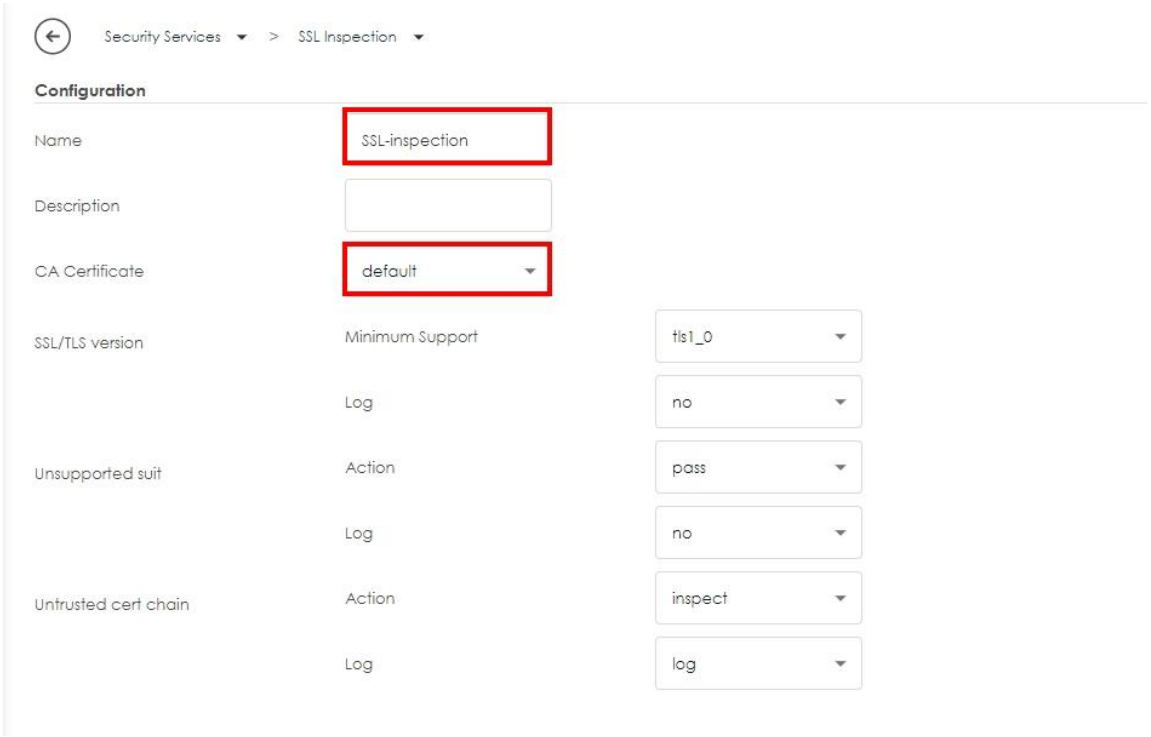


Set Up SSL Inspection on the FLEX

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



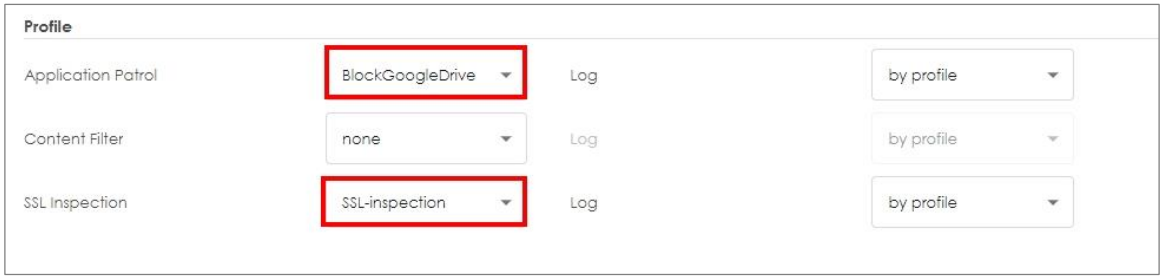
Type profile Name, and select the CA Certificate to be the certificate used in this profile. Leave other actions as default settings.



Apply profile to security policy

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

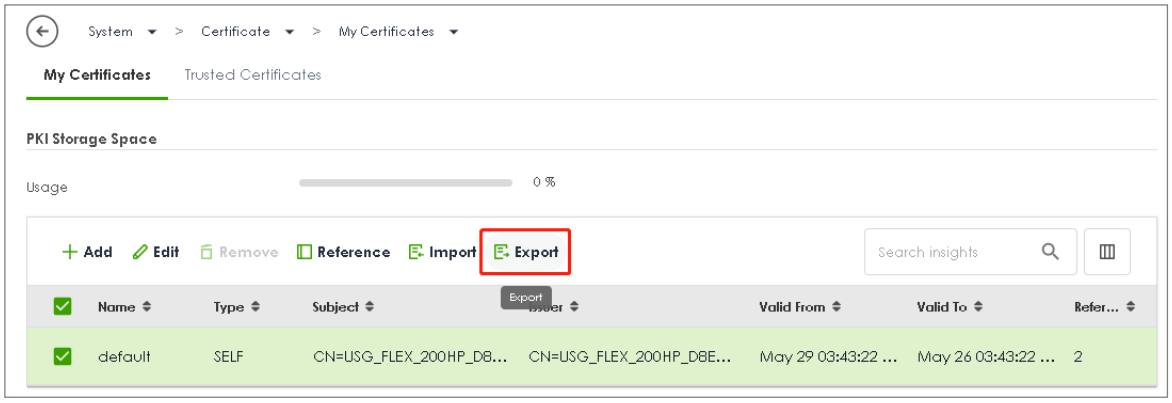
Select Application Patrol, and SSL Inspection.



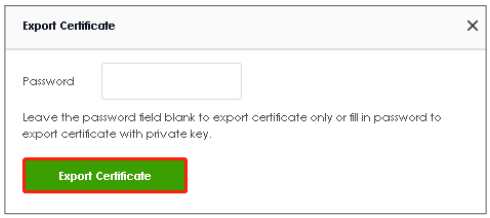
Export Certificate from FLEX and import to Lan hosts

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.

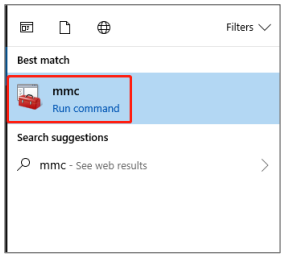
Go to System > Certificate > My Certificates to export default certificate from FLEX.



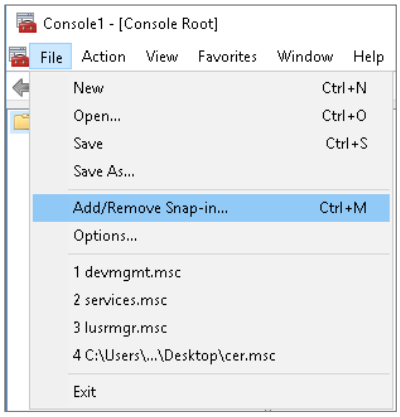
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



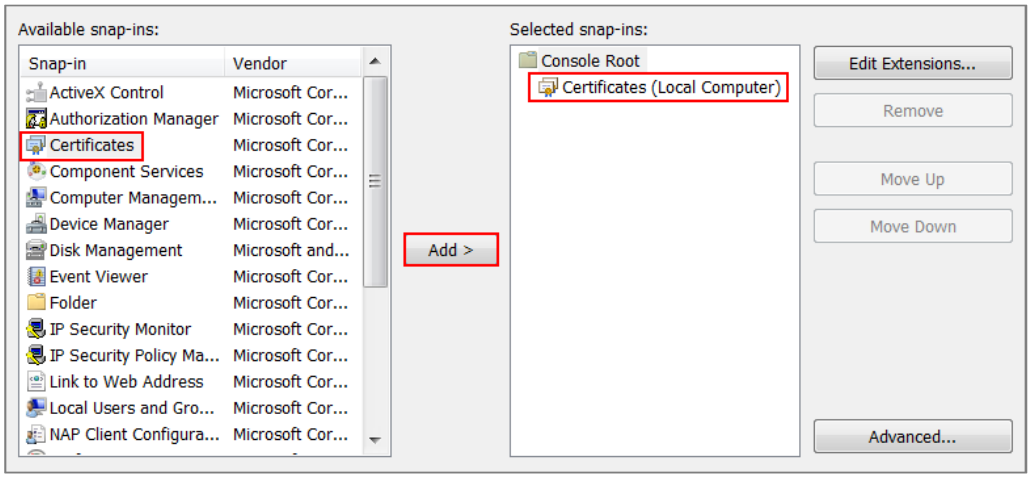
In Windows Start Menu > Search Box, type MMC and press Enter.



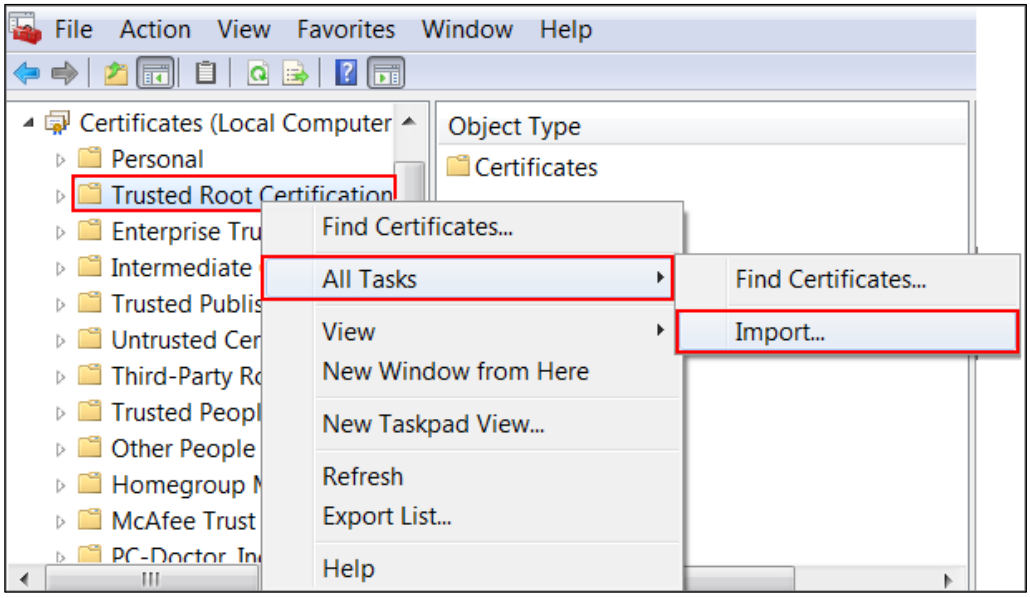
In the mmc console window, click File > Add/Remove Snap-in...



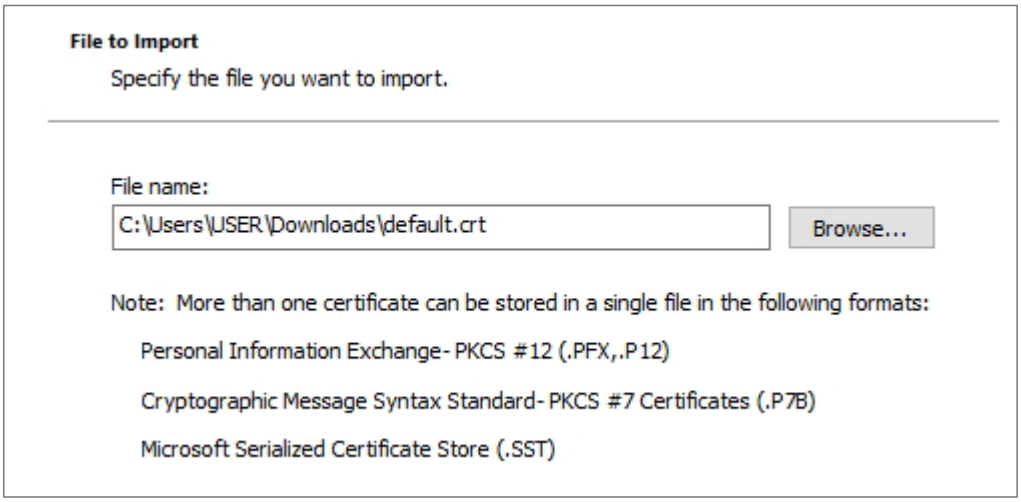
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



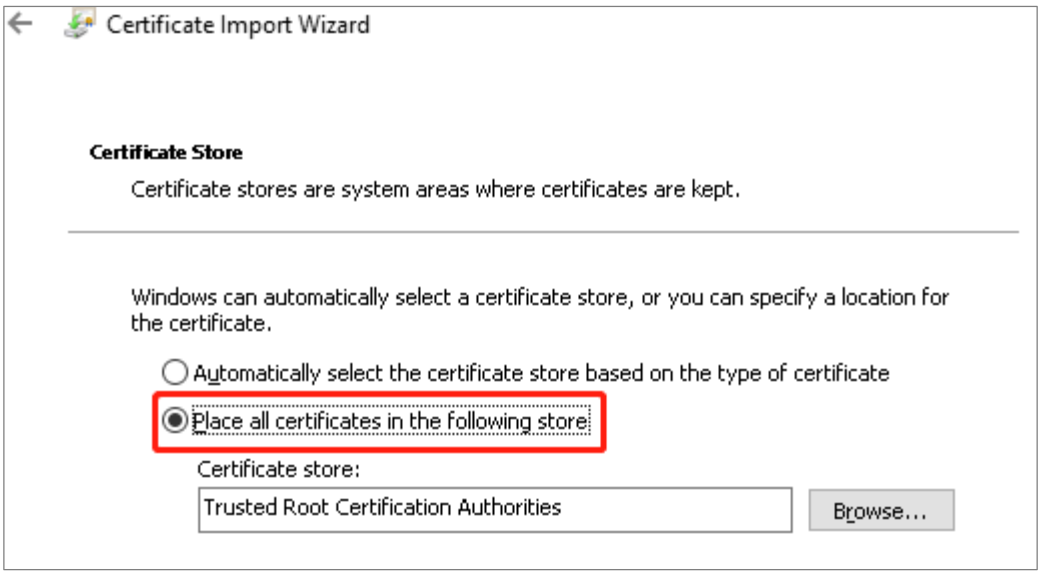
In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import...



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.



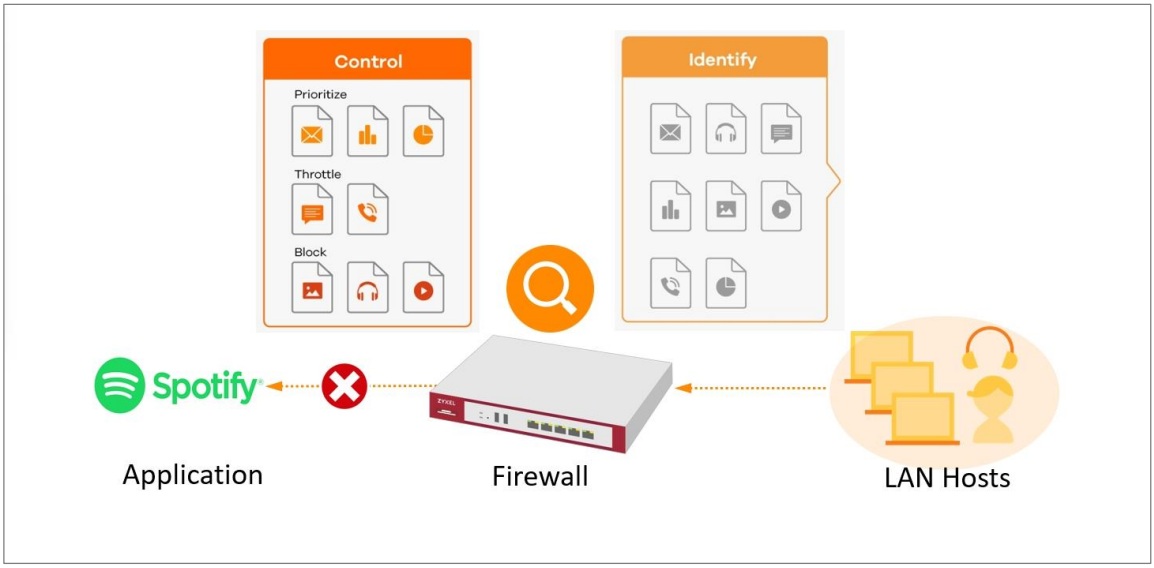
Test the Result

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.

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.



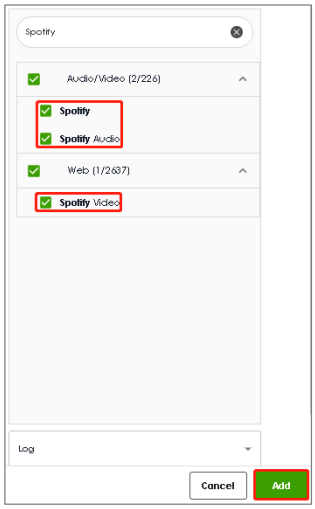
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

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.

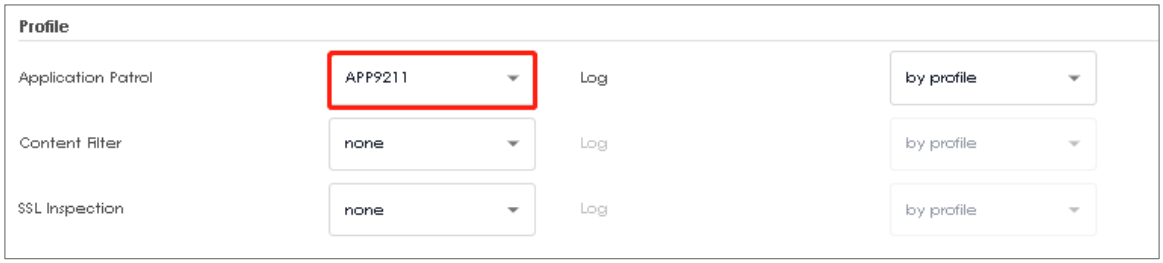
Search Spotify, and select this Application. Action set to Drop, and click Add.



Apply profile to security policy

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

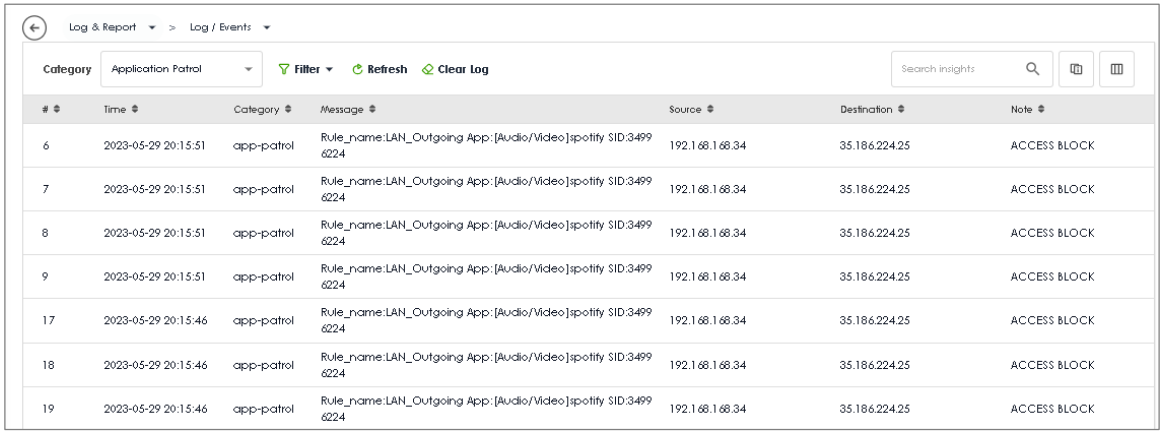
Apply Application Patrol profile to Security policy.



Test the Result

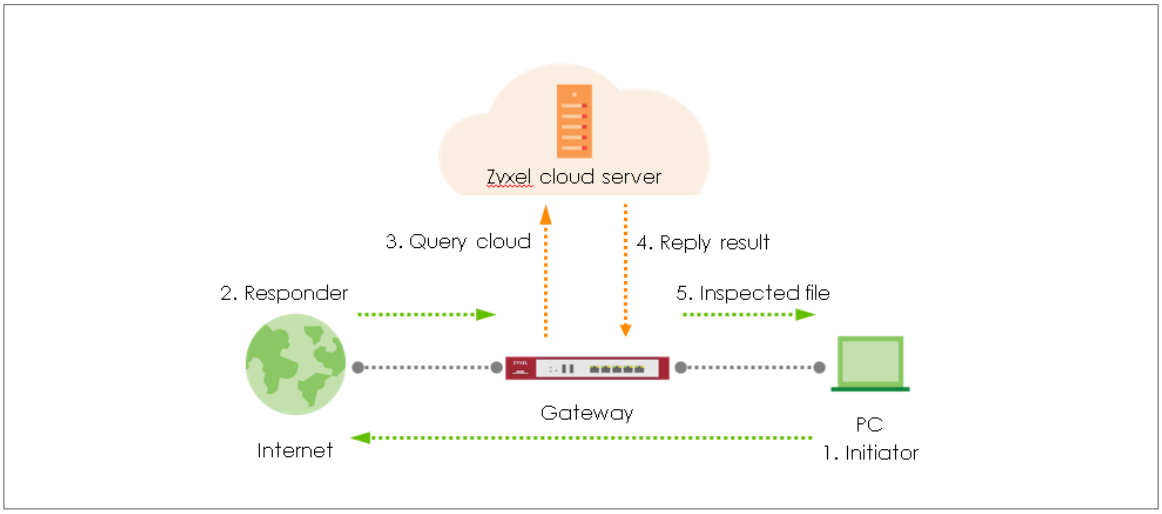
Access to Spotify from Lan host to verify if it is blocked by firewall Application patrol.

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



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

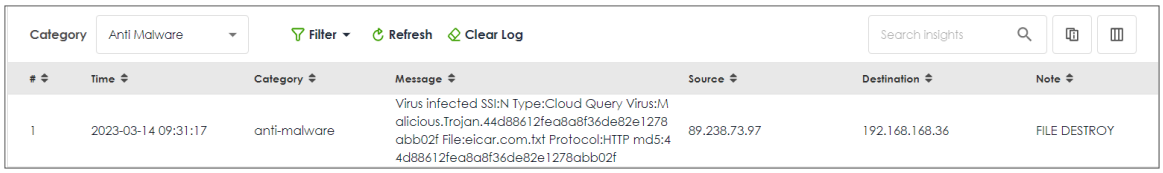
Go to Security Service > Anti-Malware. Turn on this feature. Select Collect Statistics and Scan and detect EICAR test virus.

Select Destroy infected file and log in Actions When Matched

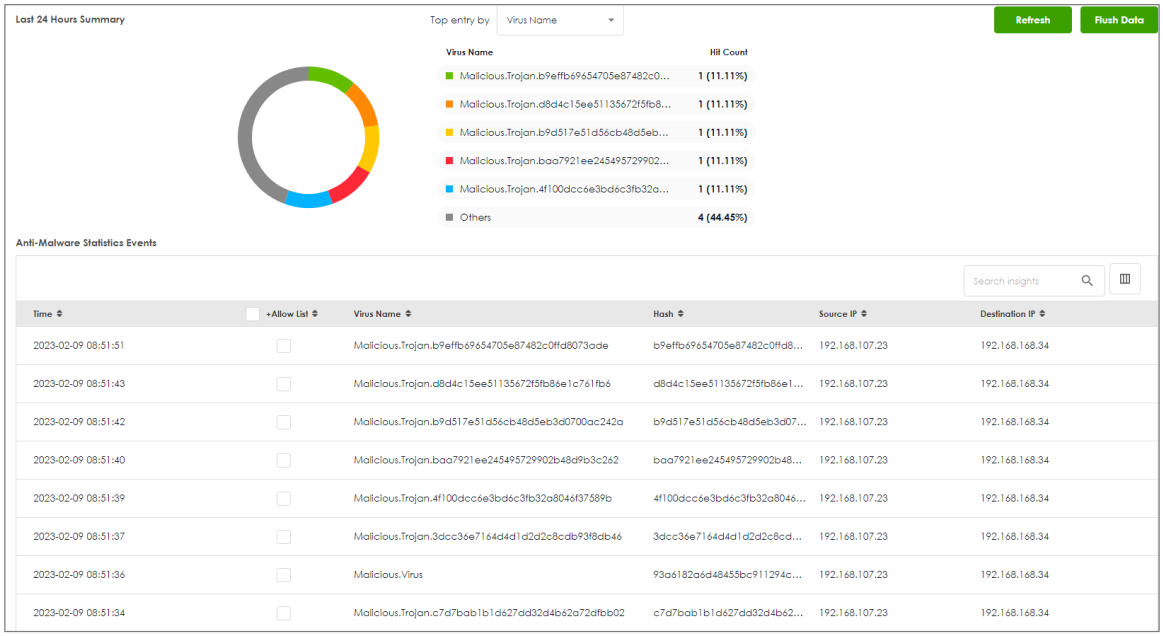
Test the Result

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.

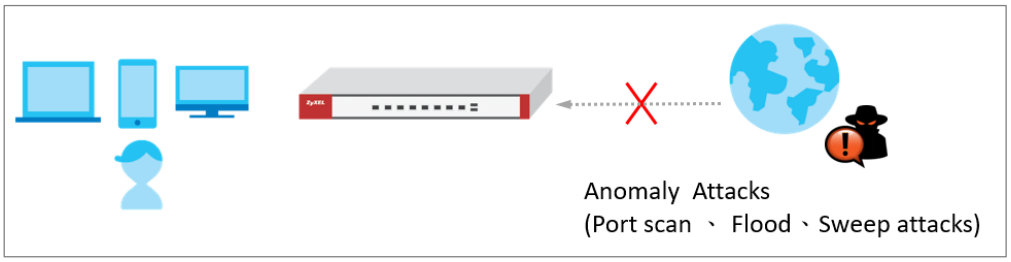


Go to Security Statistics > Anti-Malware to check summary of all events.



How to Detect and Prevent TCP Port Scanning with DoS Prevention

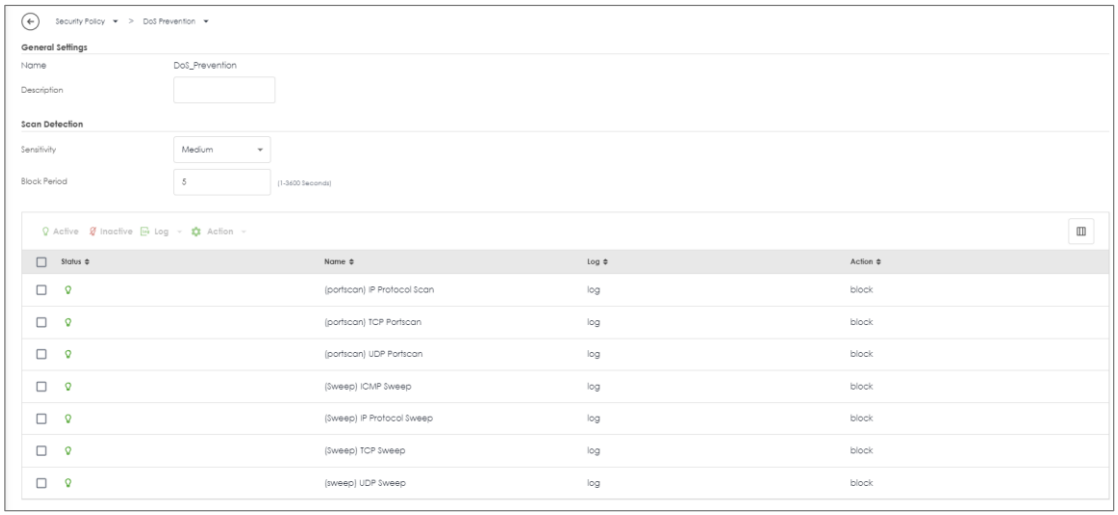
This is an example of using a USG Flex H DoS Prevention Profile to protect against anomalies based on violations of protocol standards (RFCs Requests for Comments) and abnormal traffic flows such as port scans.

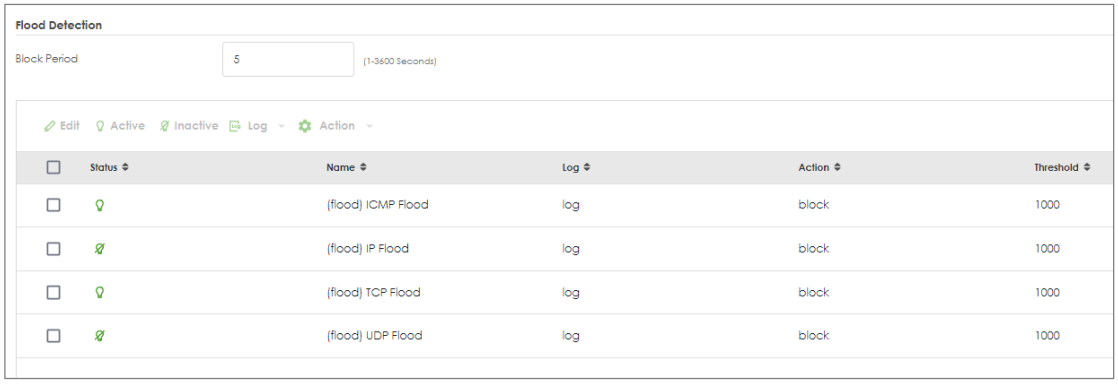


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the DoS Prevention

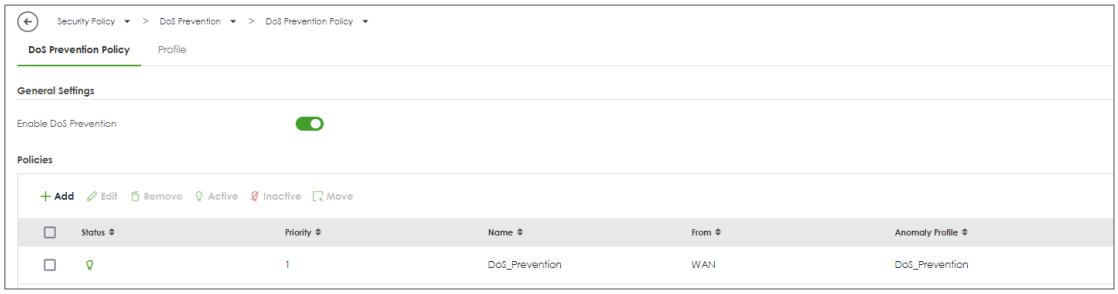
In the USG Flex H, go to **Security Policy > Dos Prevention > Add a profile**. Configure a **Name** for you to identify the **profile** such as “DoS_Prevention”. Configure the **Scan Detection** and **Flood Detection** to block when the Dos prevention events were detected.





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.

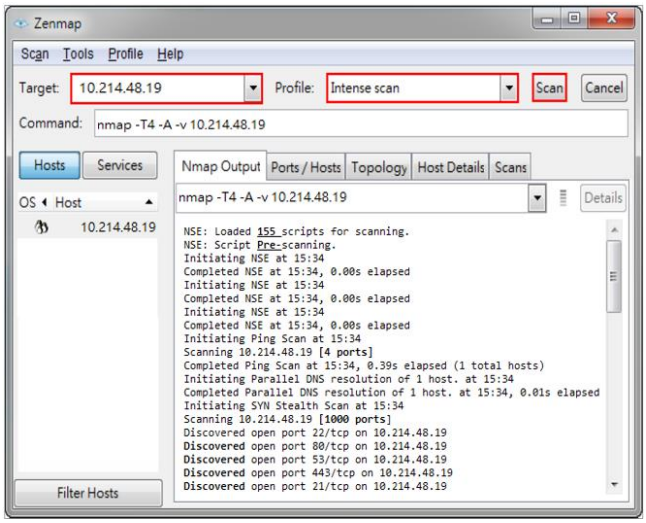


Test the Result

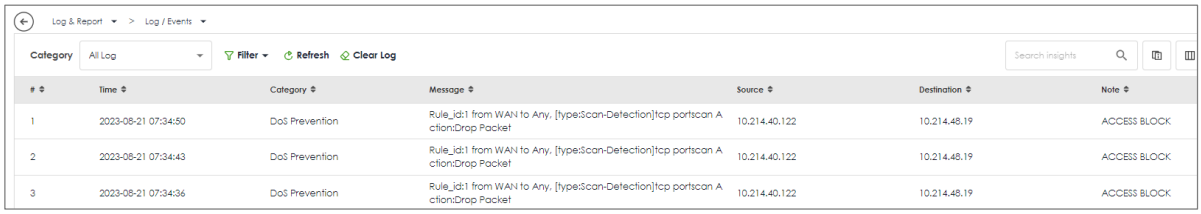
Using the port scan tool Nmap or hping3 to scan the wan interface.

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.



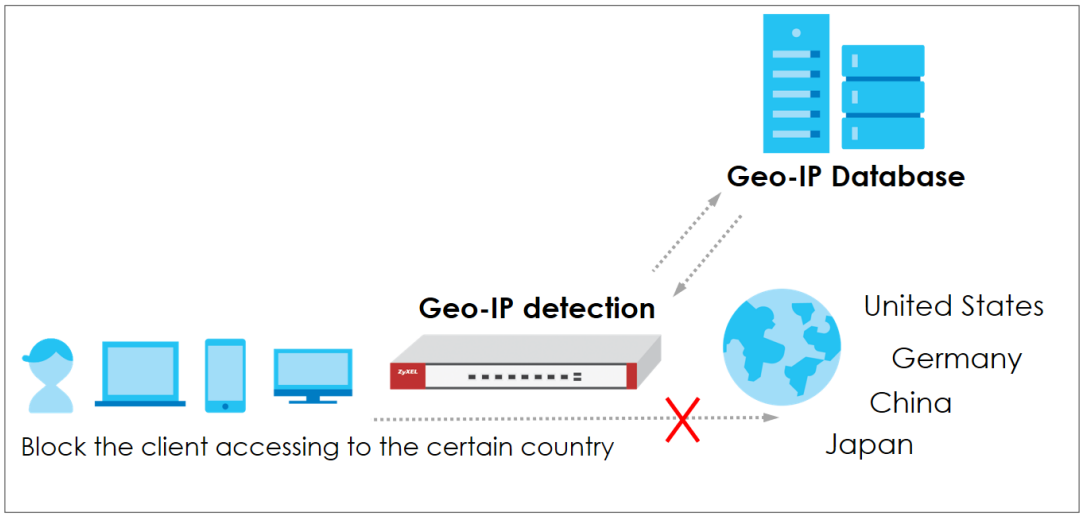
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.



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.

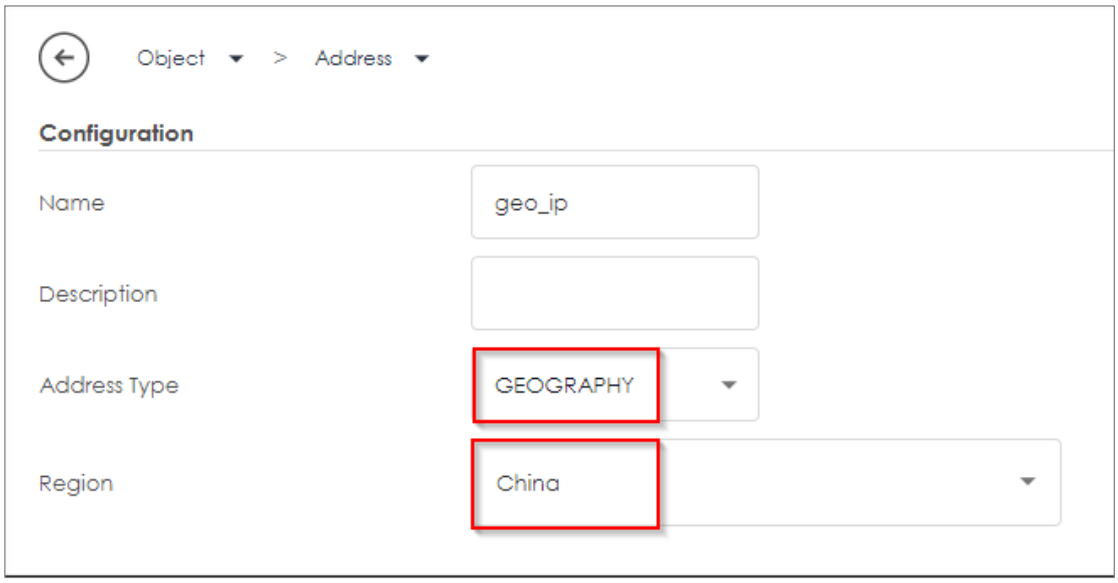
When the user makes HTTP or HTTPS request, USG Flex H queries the IP address from the cloud database, then takes action when it matches the block country in the security policy.

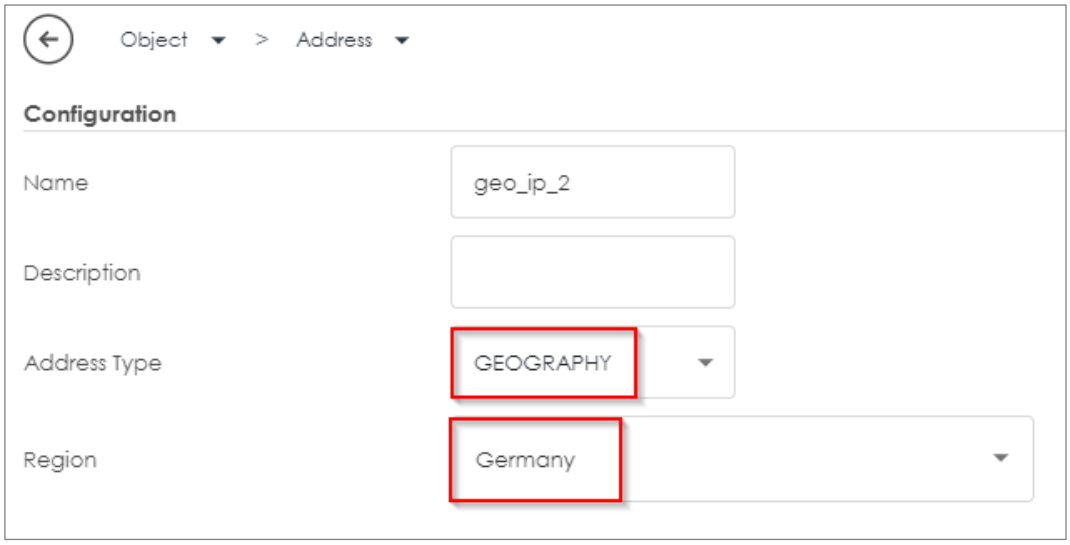


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500H (Firmware Version: uOS 1.10)

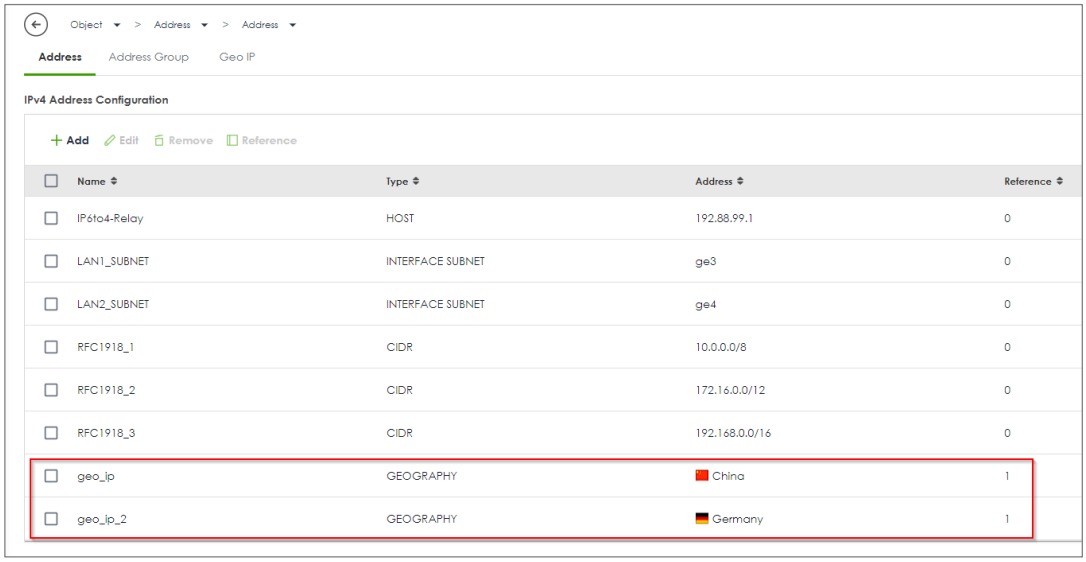
Set Up the Address Objet with Geo IP

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

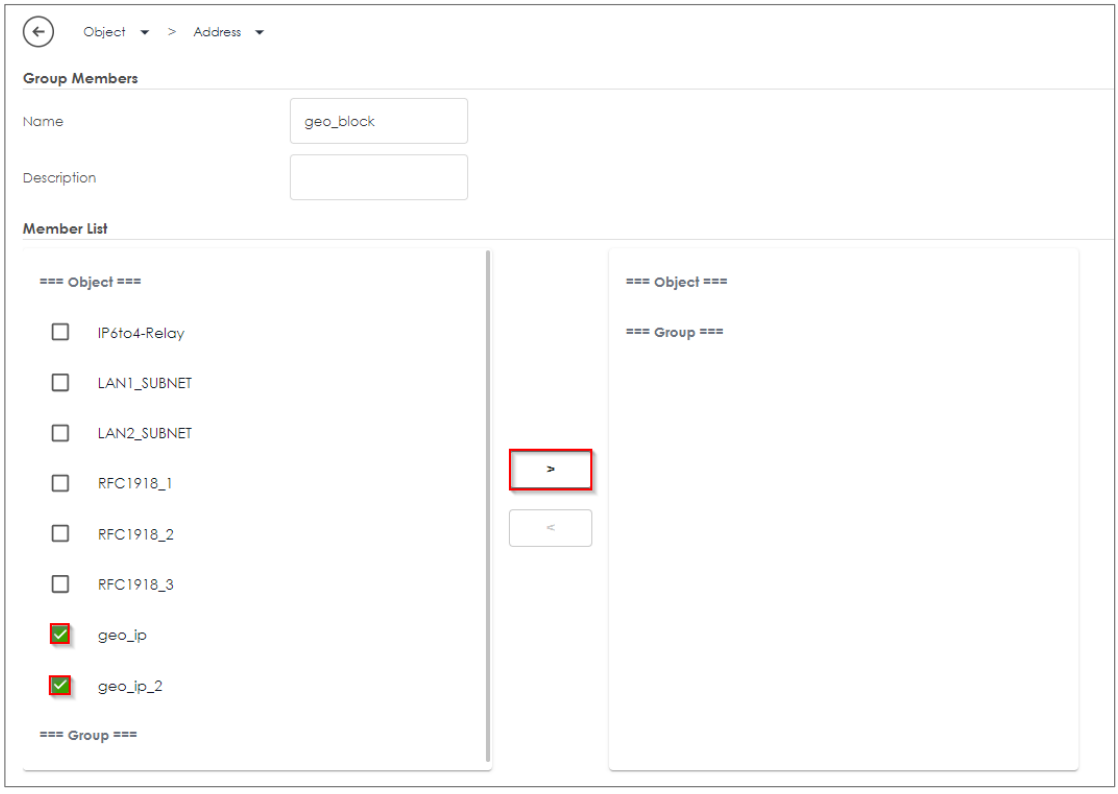




Navigate to **Object > Address > Address**, you can see the customized GEOGRAPHY address object.

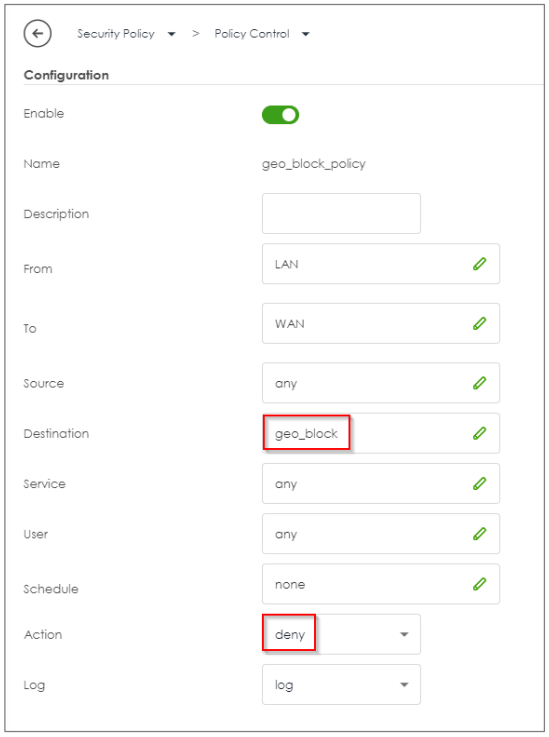


Go to **Object > Address > Address Group> Add Address Group Rule**, add all customized GEOGRAPHY addresses into the same **Member** object.



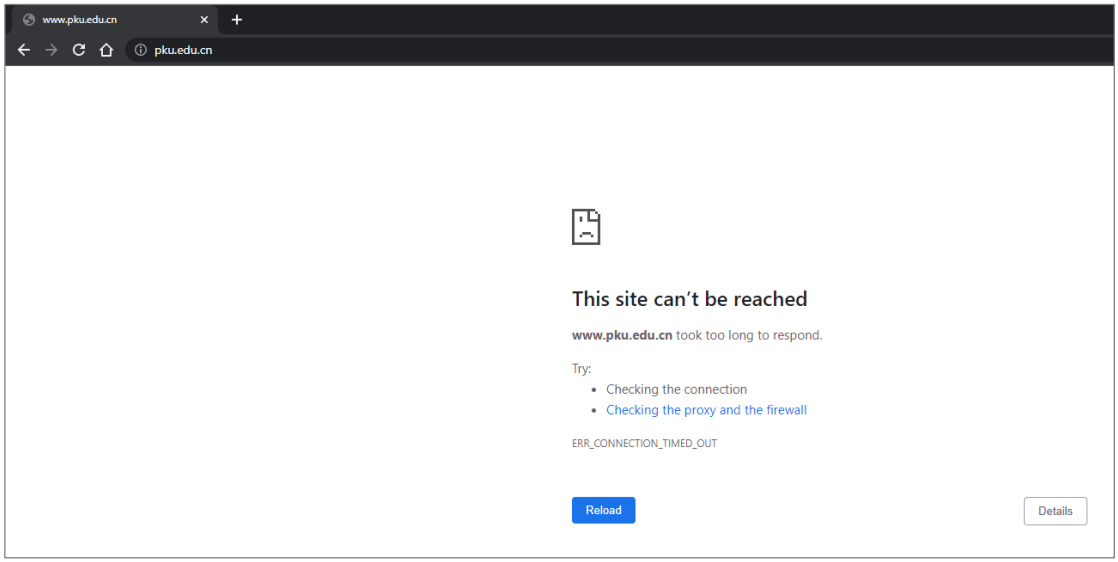
Set Up the Security Policy

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).

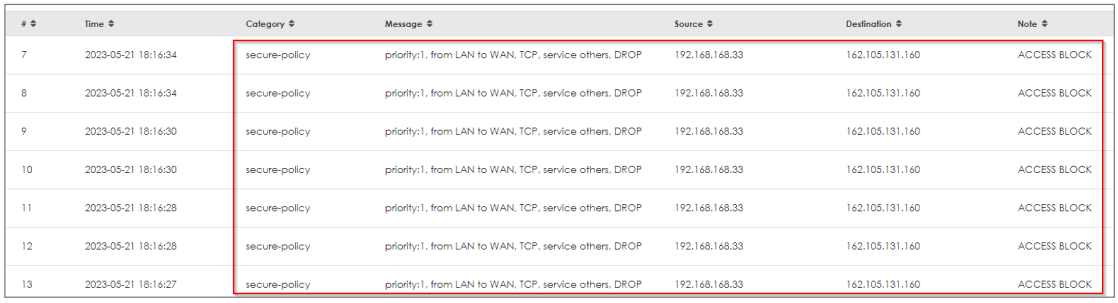


Test the Result

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



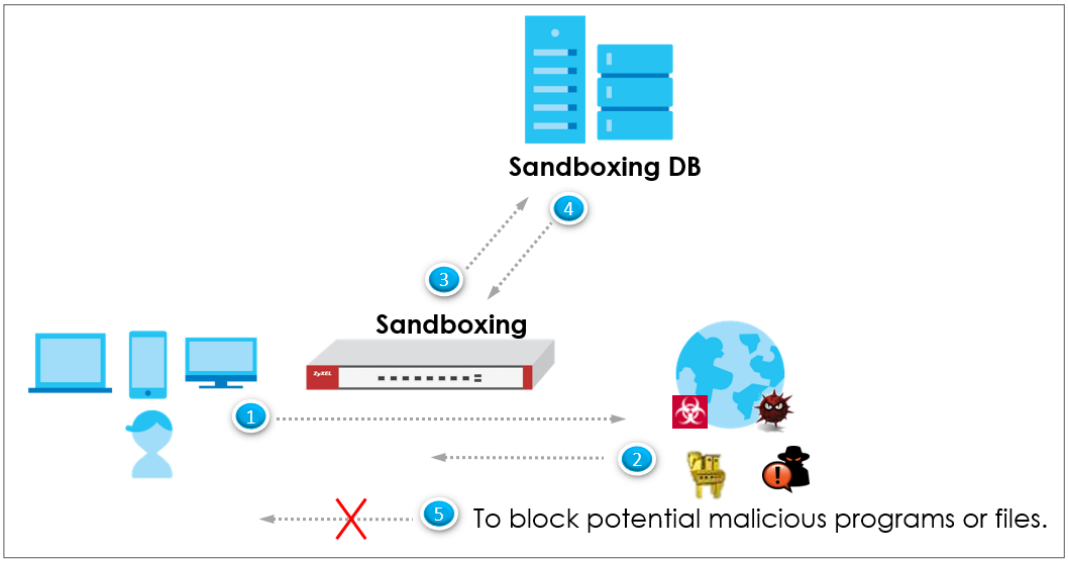
To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.



#	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?

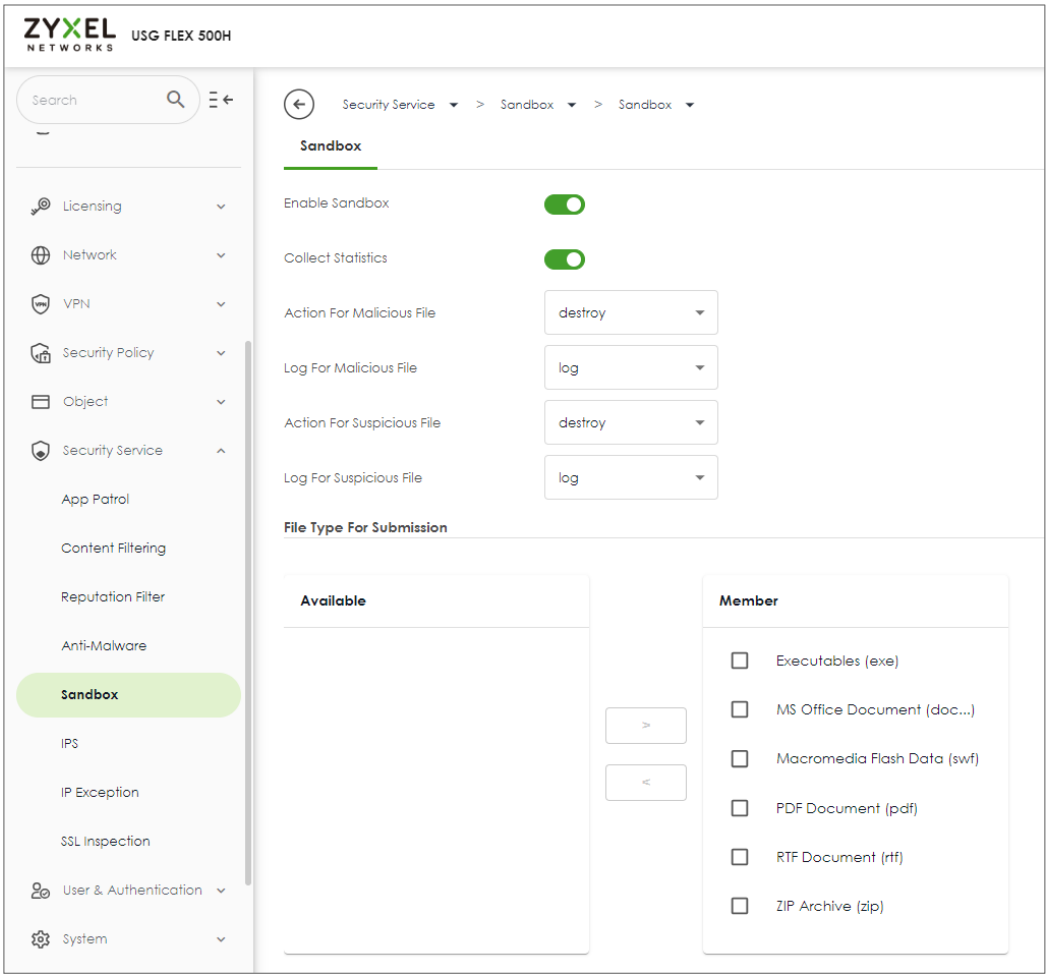
This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



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.

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.

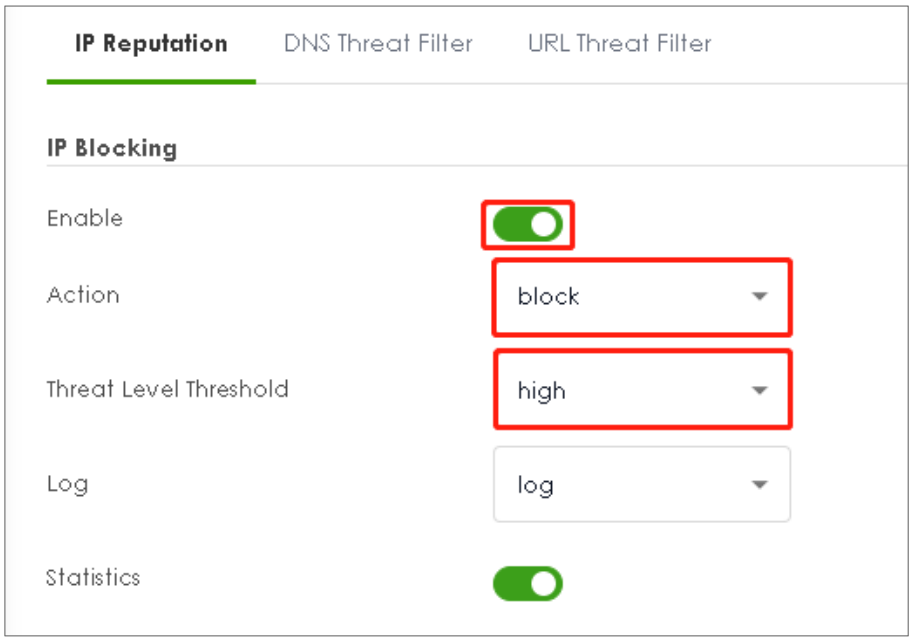
With regularly updated IP database, FLEX prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

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

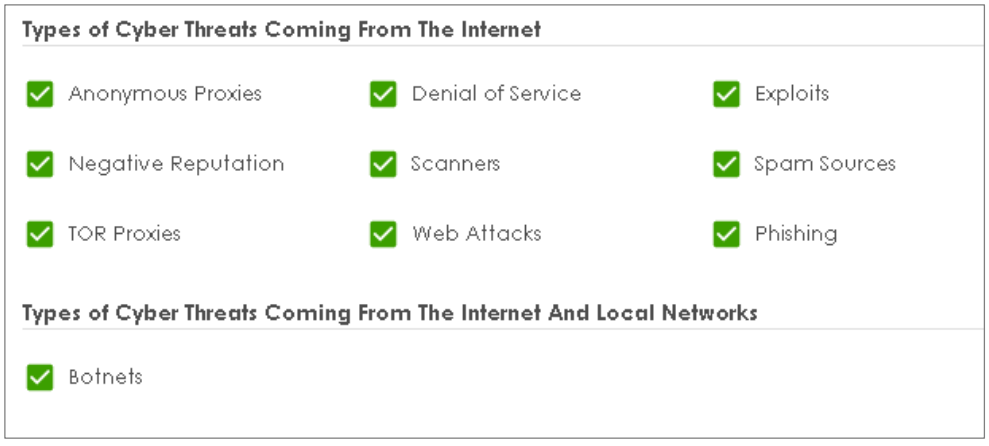
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the IP reputation filter

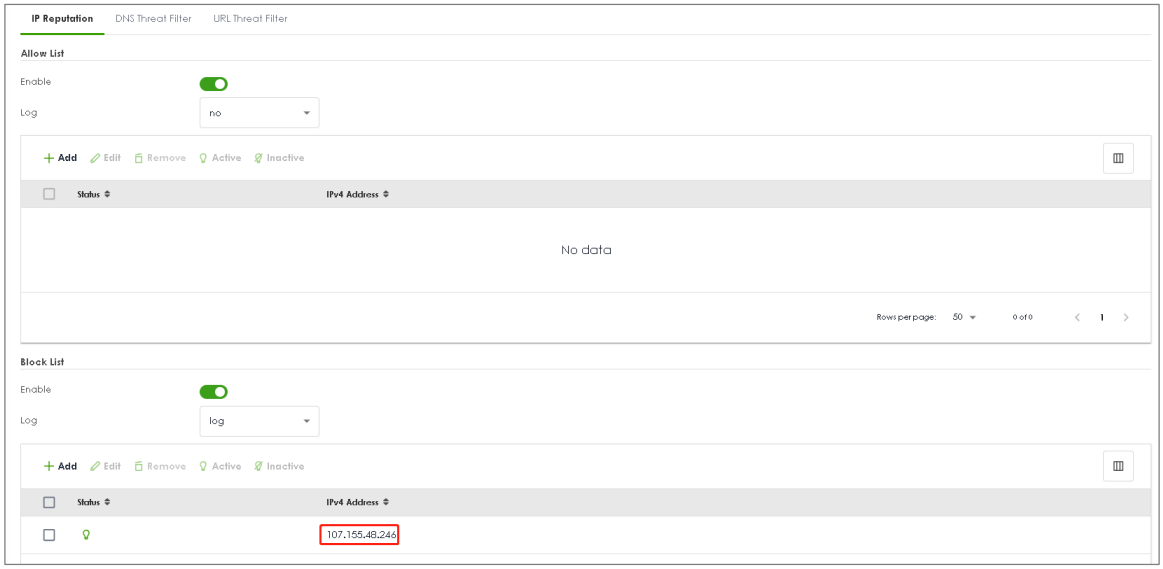
Go to Security Service > Reputation Filter > IP reputation. Turn on this feature. Select Block on Action field. The threat level threshold is measured by the query score of IP signature database.



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



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

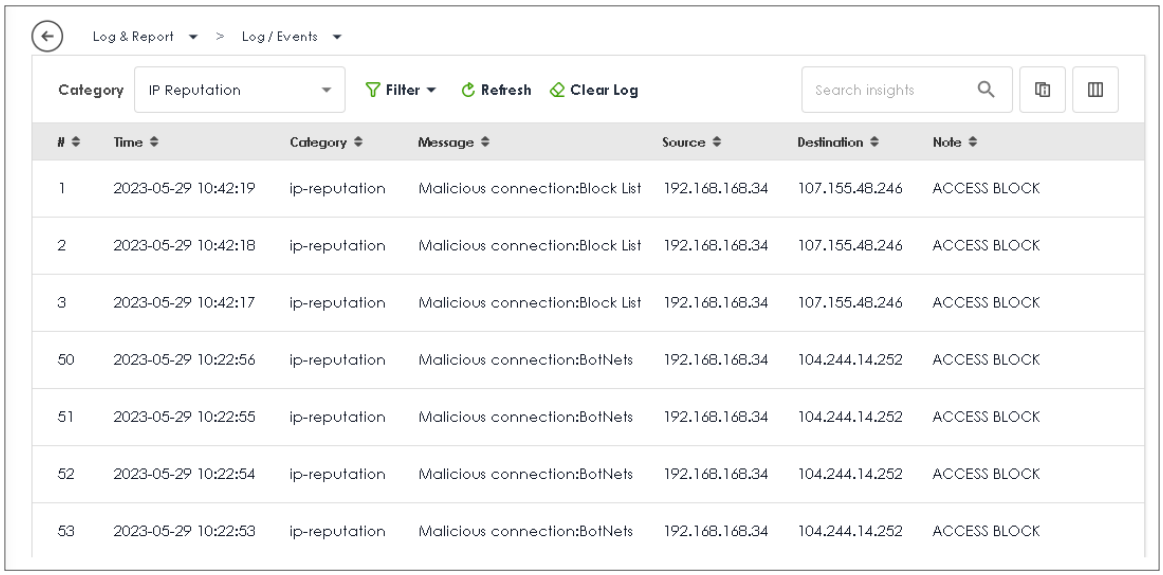


Test the Result

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

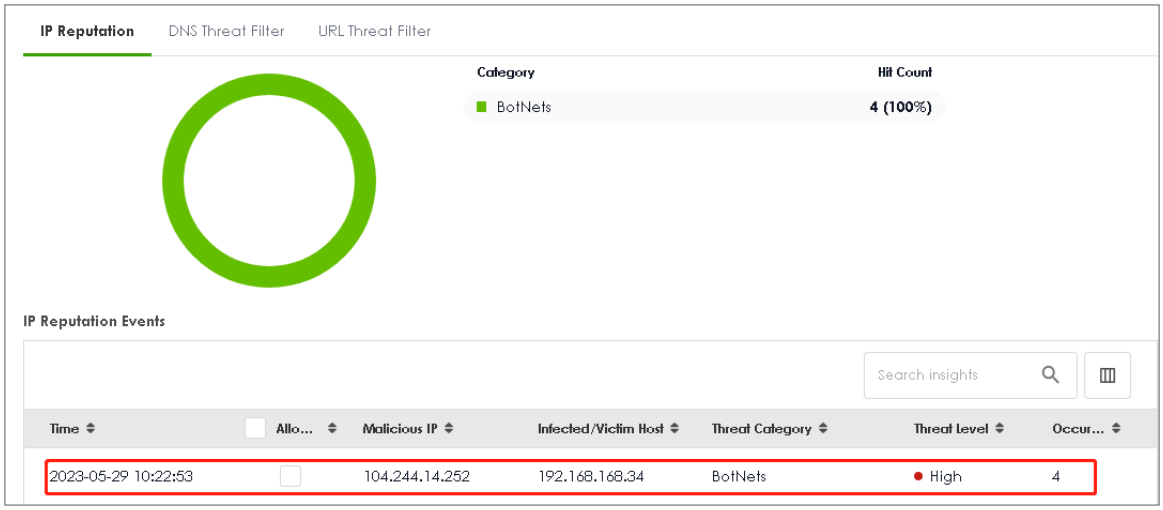
Try to generate ICMP packet from LAN to destination IP 107.155.48.246, and 104.244.14.252

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



#	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

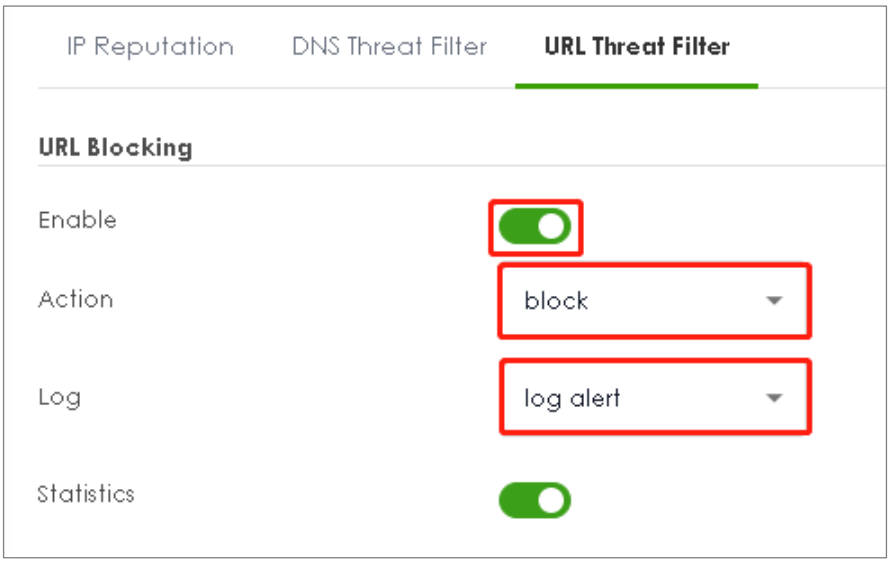
URL Threat Filter can avoid users to browse some malicious URLs (such as anonymizers, browser exploits, phishing sites, spam URLs, spyware) and allows administrator to manage which URLs can be browsed or not.

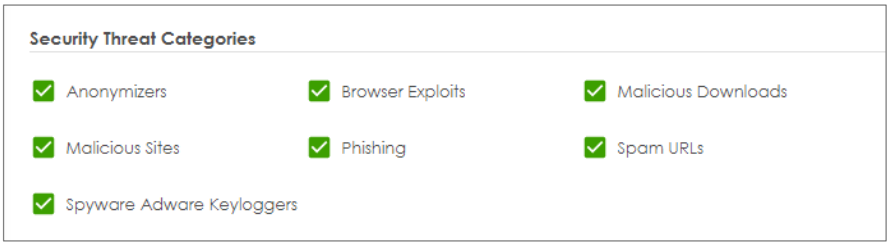
This example demonstrates how to configure the URL Threat Filter to redirect web access after the client hits the URL Threat Filter categories.

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.

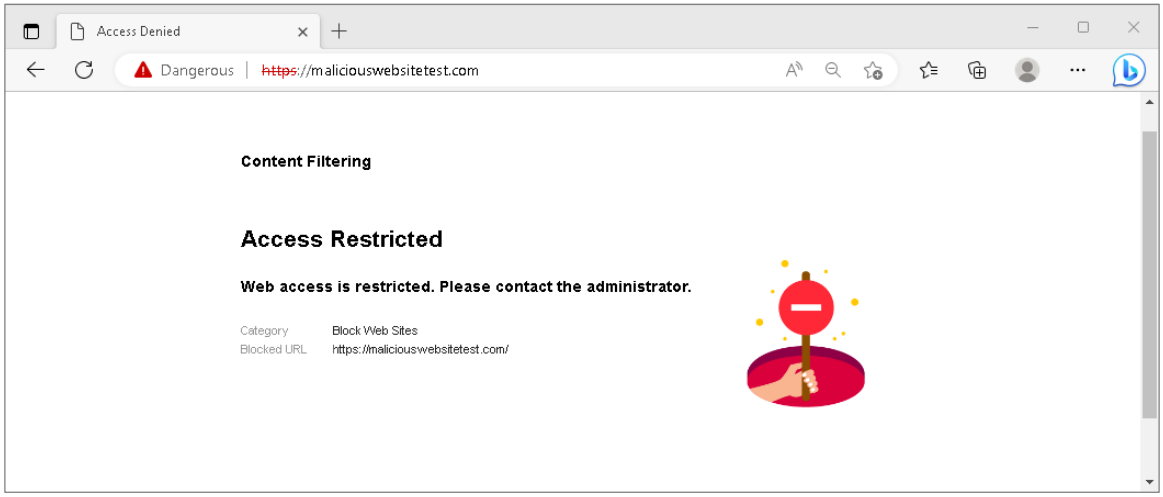




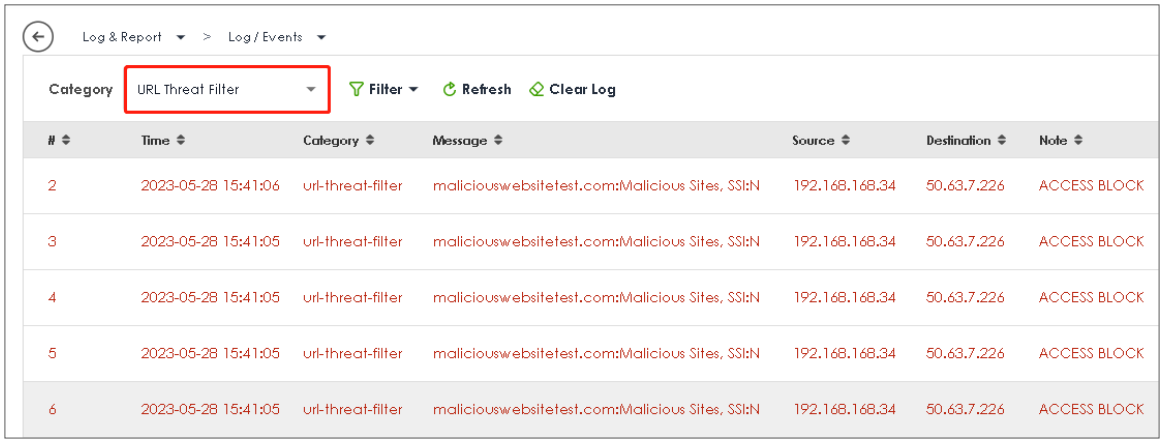
Test the Result

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

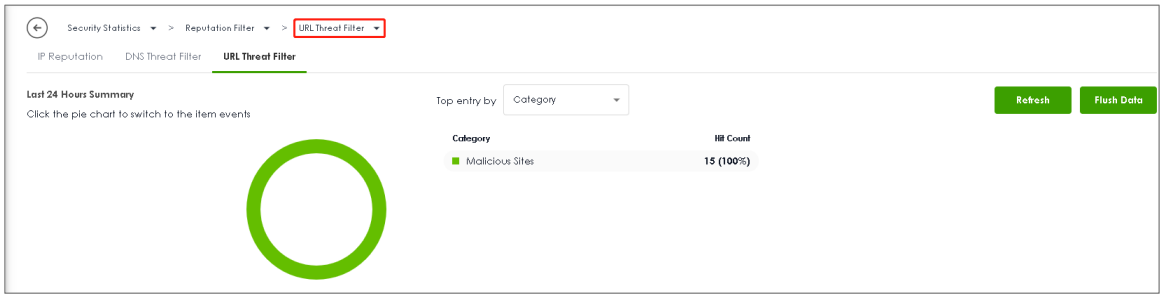
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.

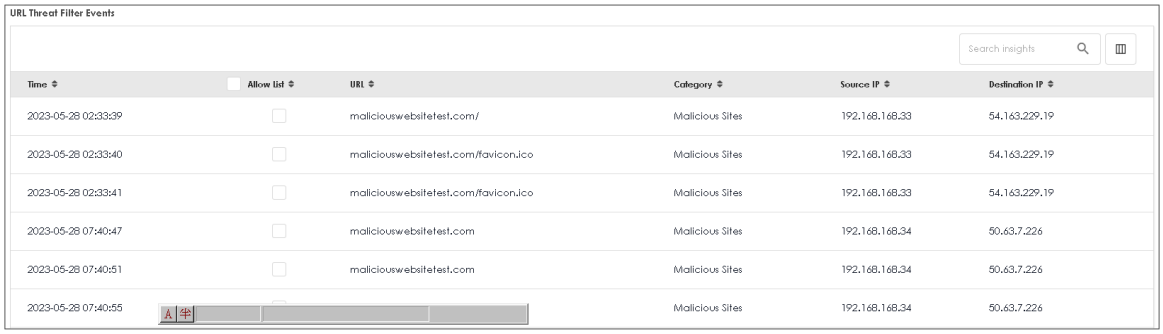


Go to Log & Report > Log/Events and select URL Threat Filter to check the logs.



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





How to Configure Reputation Filter- DNS Threat Filter

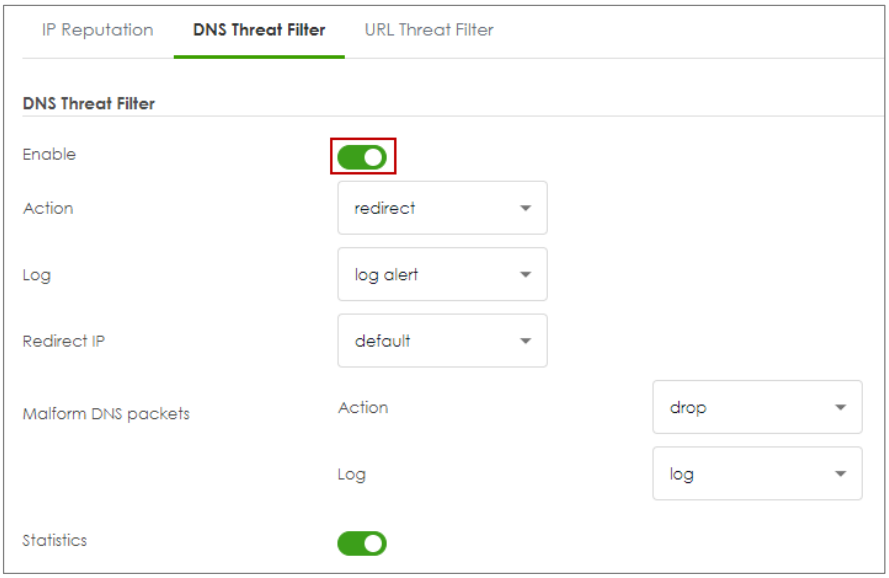
DNS Threat Filter is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the administrator.

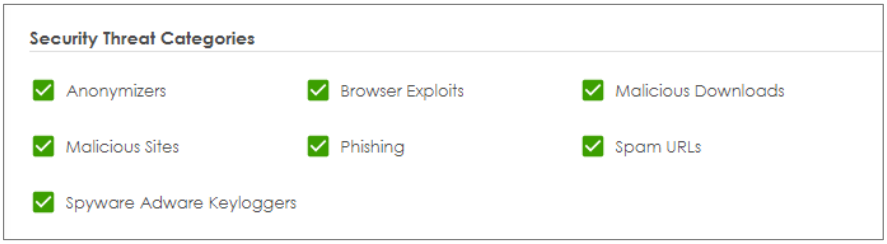
When a client wants to access a malicious domain, the query is sent to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. The cloud server identifies that this is bad site. What gateway can do here is send the redirect IP address 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.





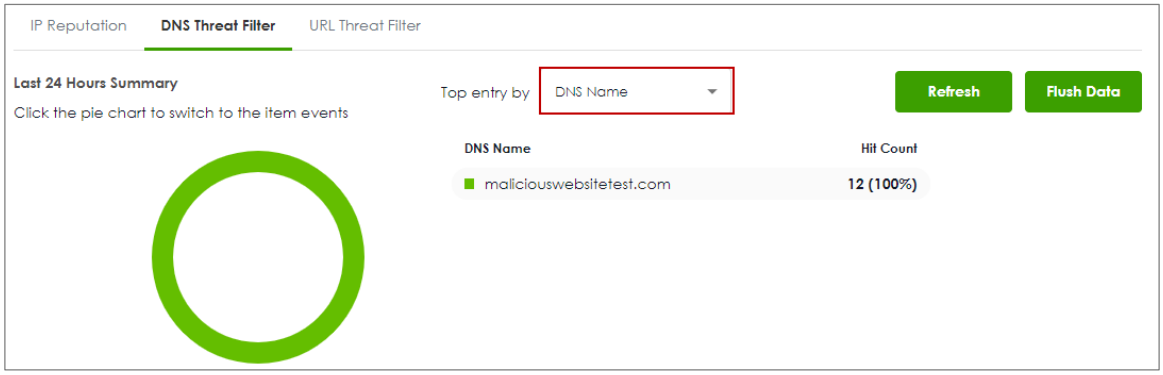
Test the Result

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

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.

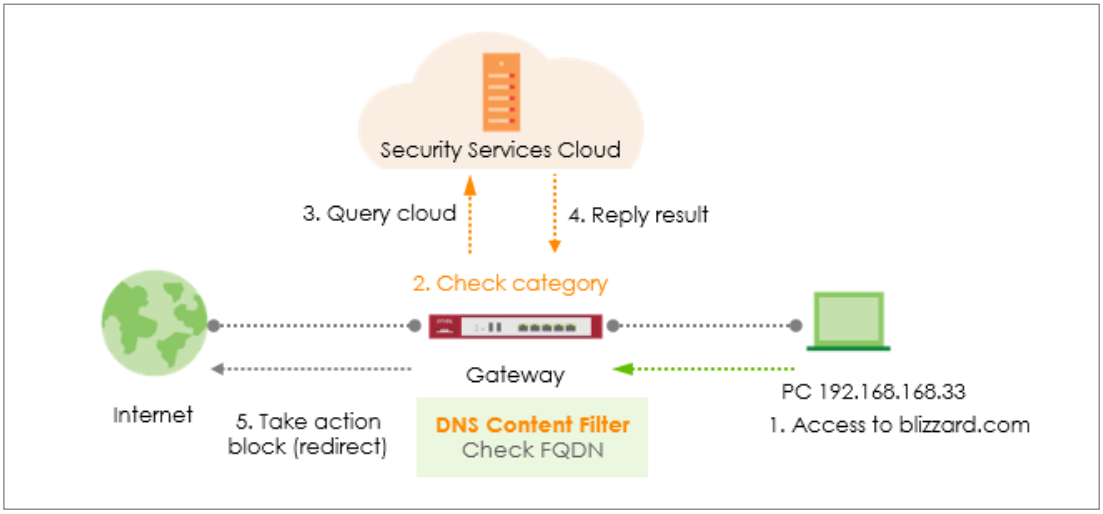
Go to Security Statistics > Reputation Filter > DNS Threat Filter to check summary of all events.



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.

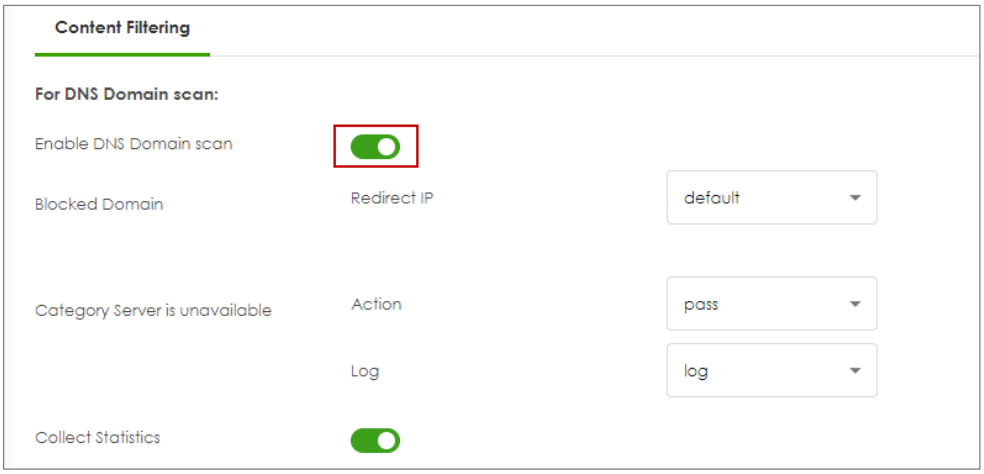
DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those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



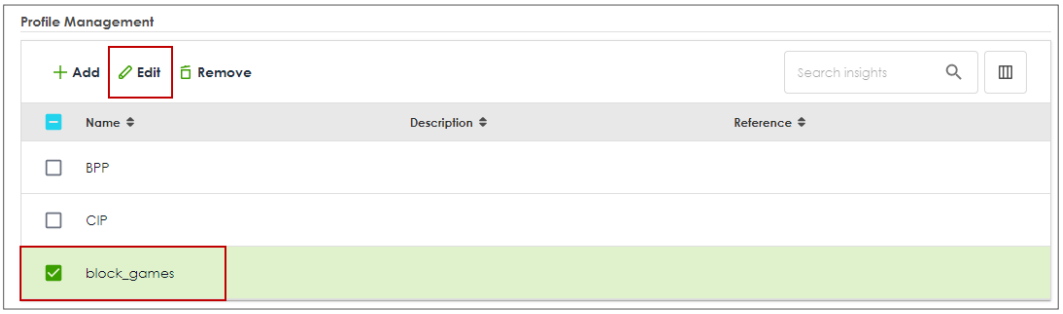
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

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/.

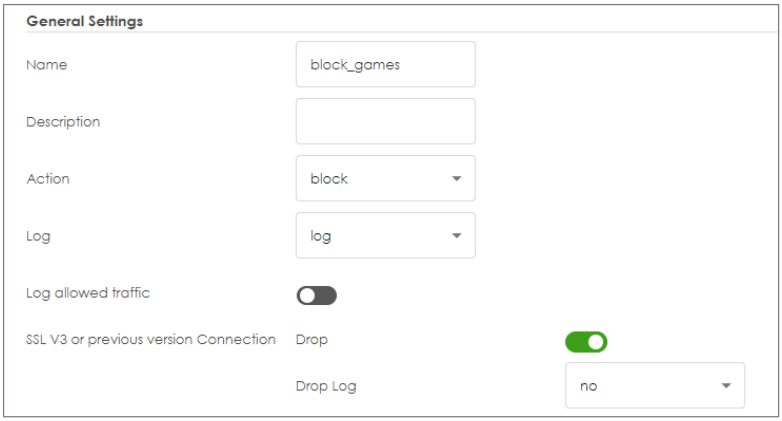


Add a new profile in Profile Management to block gaming websites.

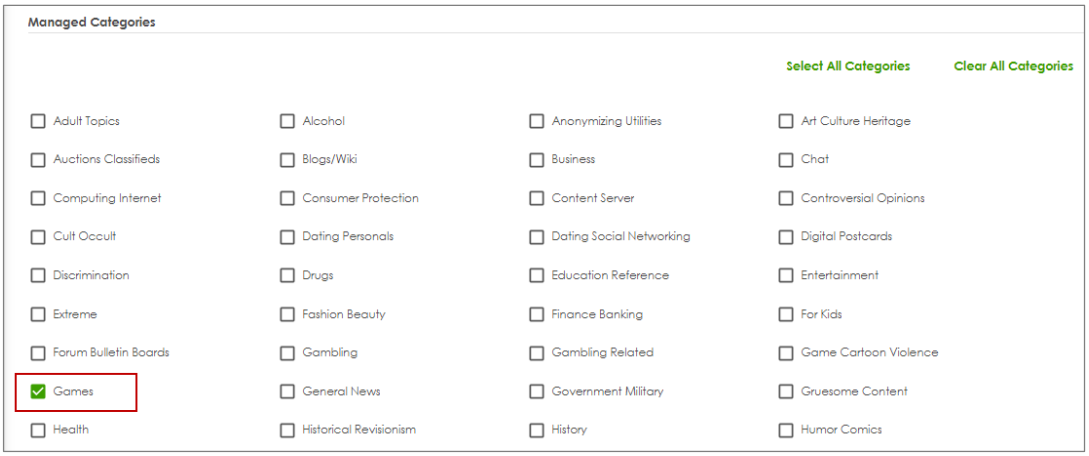


Action: block

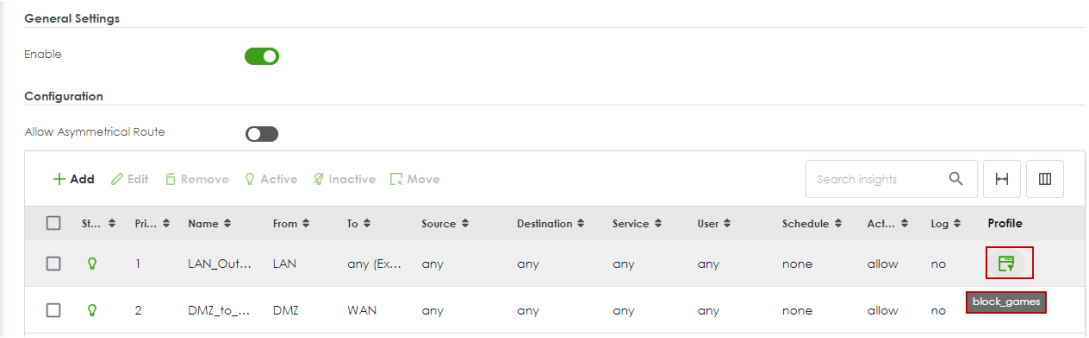
Log: log or log alert



Enable the checkbox of "Games" in managed categories.



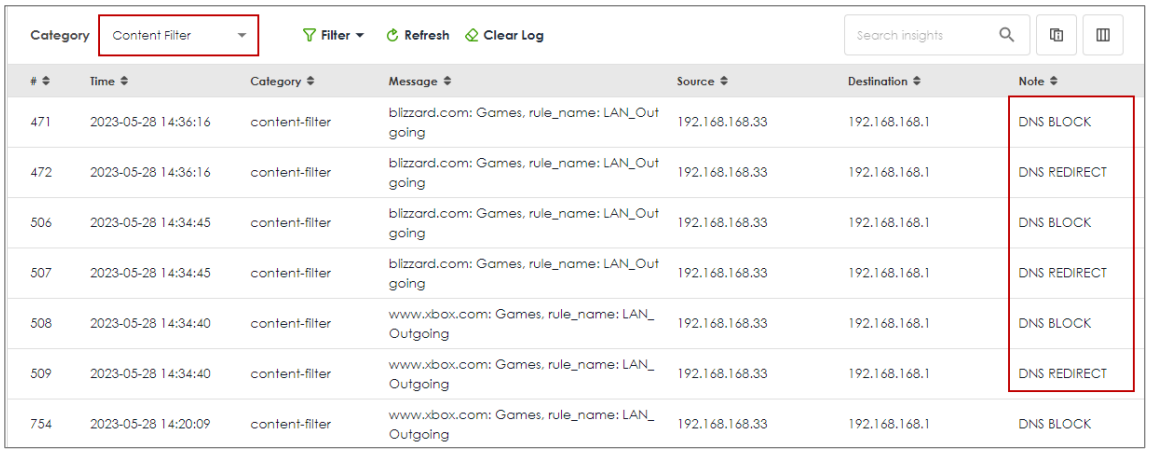
Apply the profile to security policy. In this example, the profile is applied to security policy rule “LAN_Outgoing”.



Test the Result

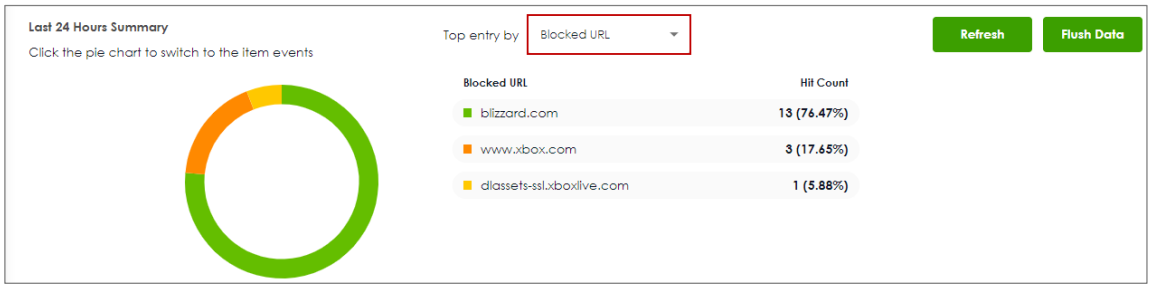
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.

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_Out going	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_Out going	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_Out going	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_Out going	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.



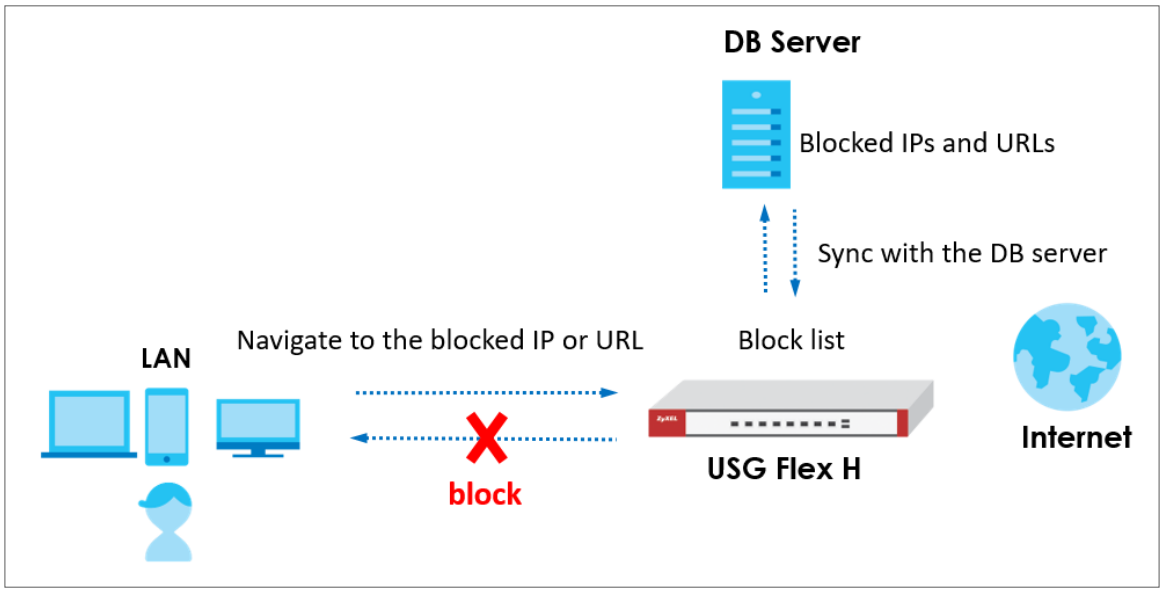
Content Filter Events

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	dlassets-ssl.xboxlive.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:55:13	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1

External Block List for Reputation Filter

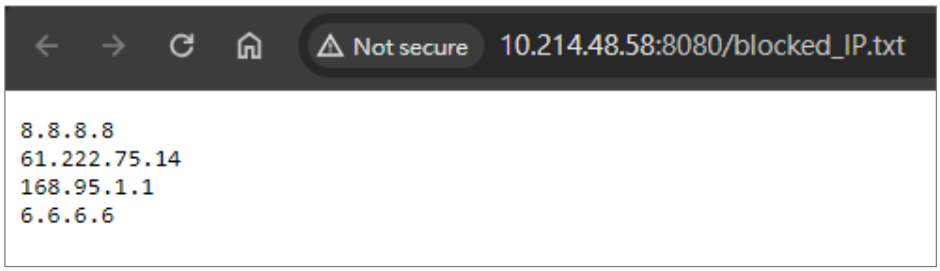
The administrator can configure an external block list for the Reputation Filter to expand its usage. This article will provide guidance on setting up the external block list for the IP Reputation and DNS Threat Filter/URL Threat Filter.



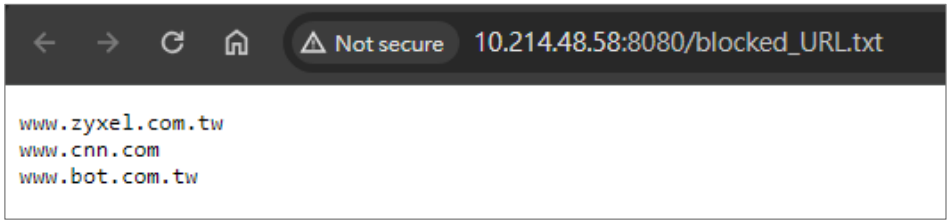
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Set Up the DB server

The administrator can set up websites to maintain external block lists. The USG Flex H firewall can update the external block list via a URL. For example,
http://10.214.48.58:8080/blocked_IP.txt

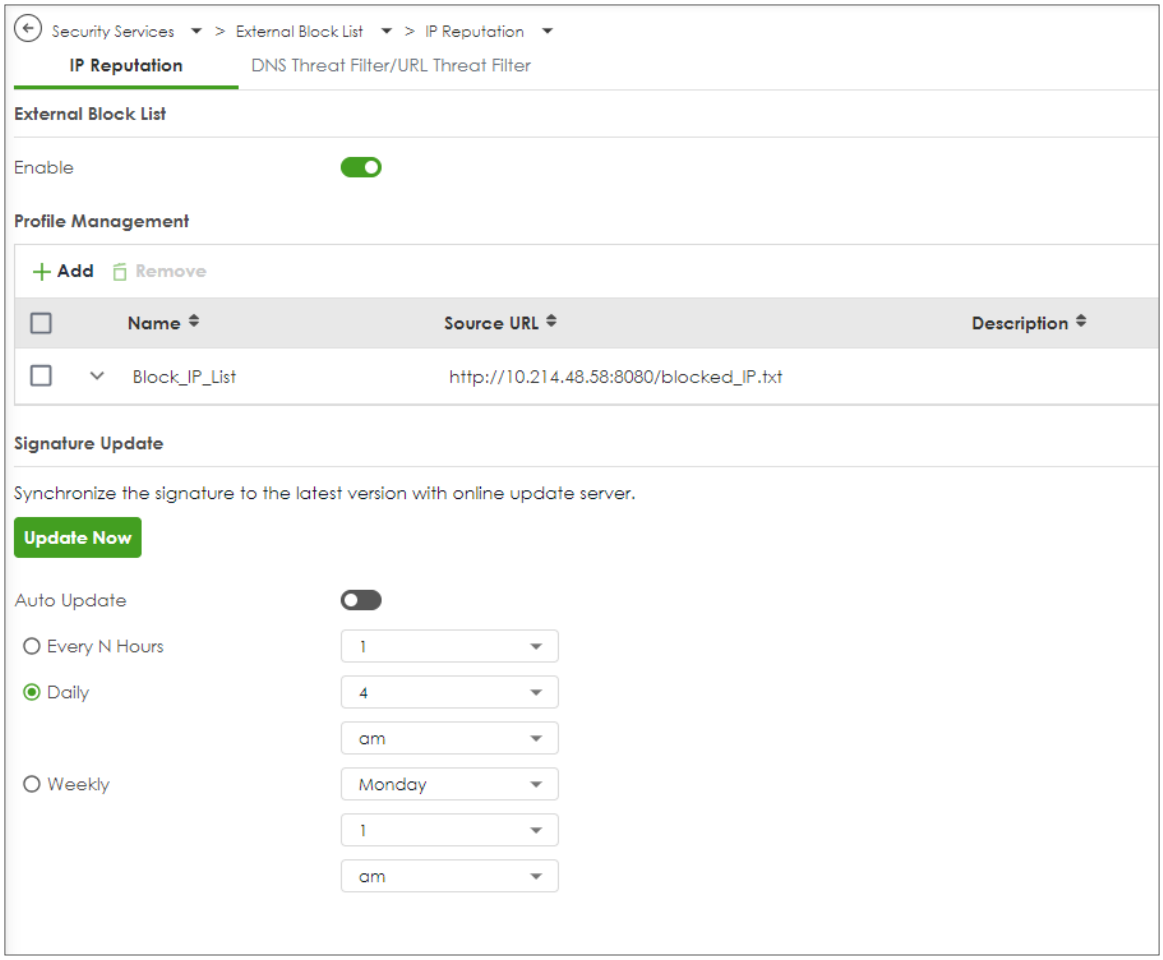


http://10.214.48.58:8080/blocked_URL.txt



Set Up the External Block List of IP Reputation

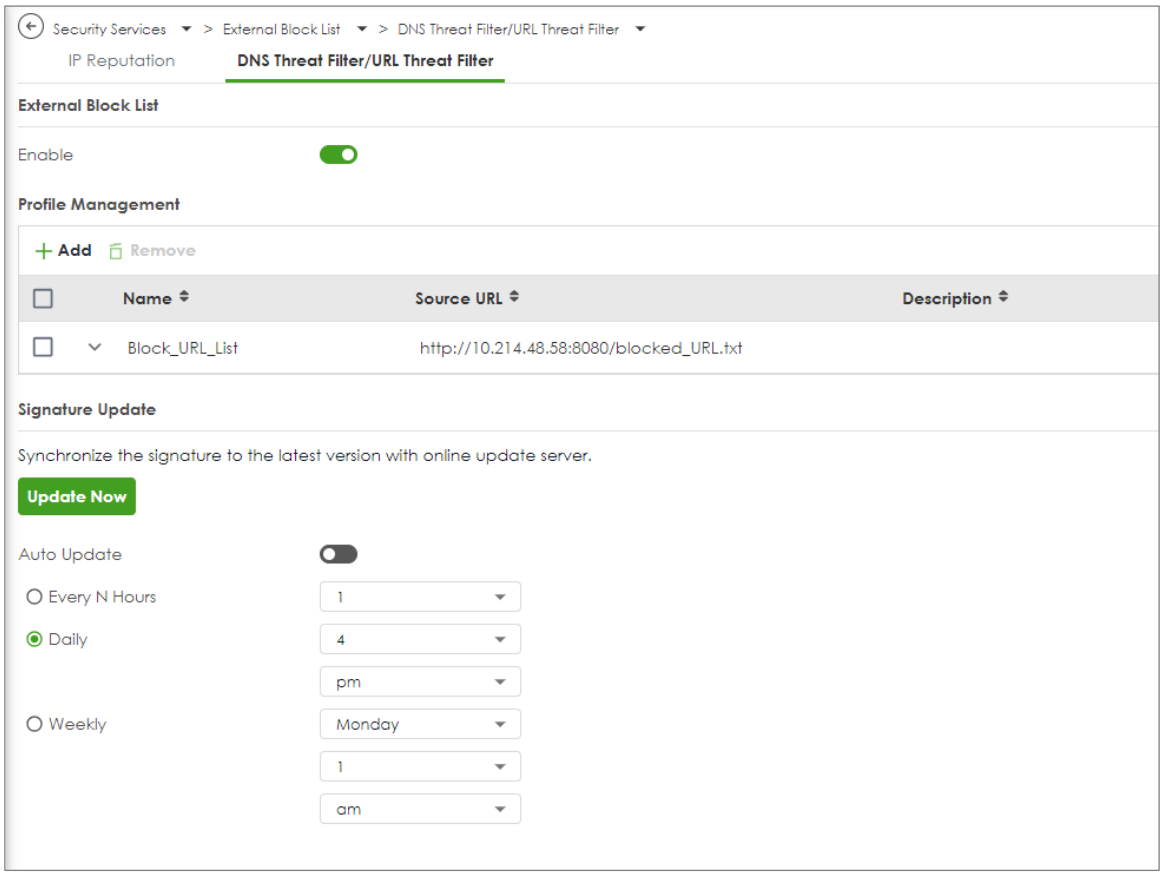
Navigate to Security Services > External Block List > IP Reputation and add a service URL such as http://10.214.48.58:8080/blocked_IP.txt and then click “Update Now” to update the block list.



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

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

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



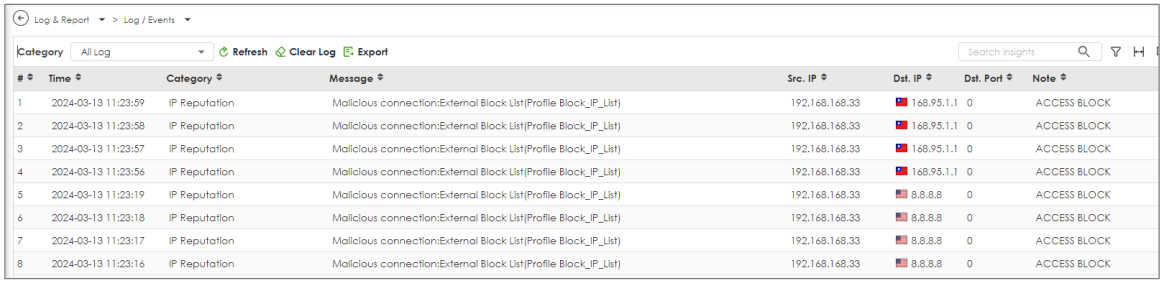
If the DNS/URL threat filter external block list is updated successfully and you can observe the corresponding log message.

Test the Result

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

```
C:\Users\[redacted]>ping 8.8.8.8

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

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

C:\Users\[redacted]>ping 168.95.1.1

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

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

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

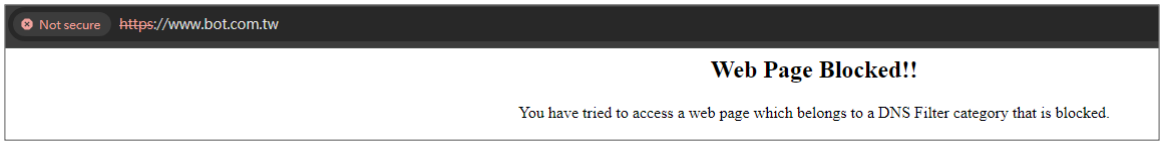


Log & Report > Log / Events

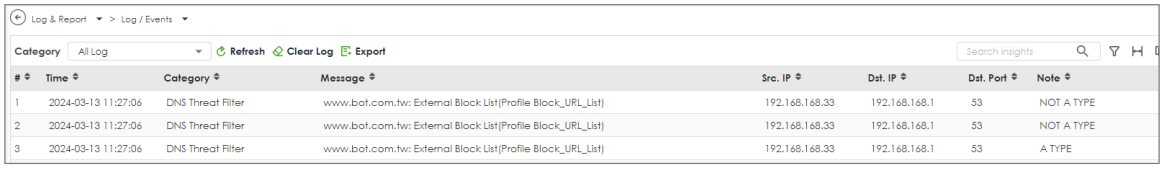
Category: All Log | Refresh | Clear Log | Export | Search insights

#	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.



Log & Report > Log / Events

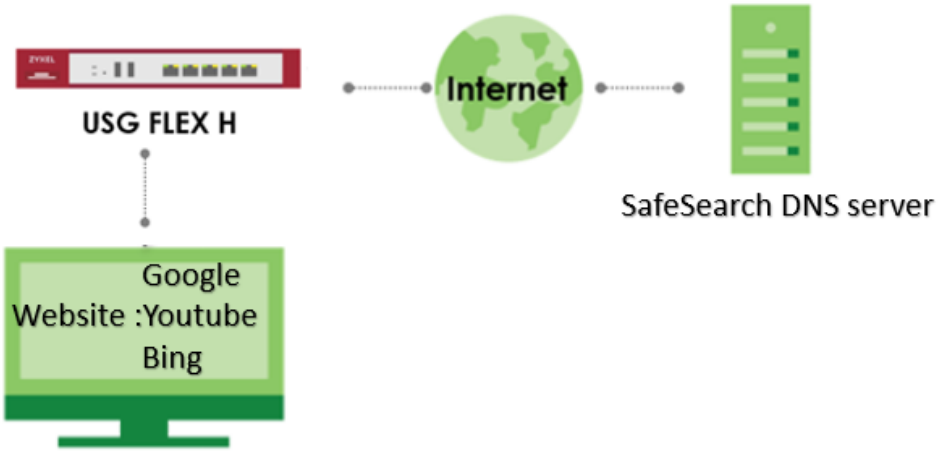
Category: All Log | Refresh | Clear Log | Export | Search insights

#	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.

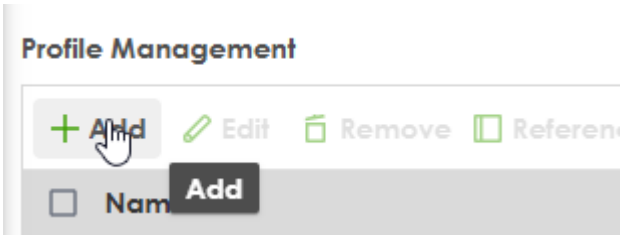
This guide explains how to configure your gateway to set up DNS Safe Search.



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.



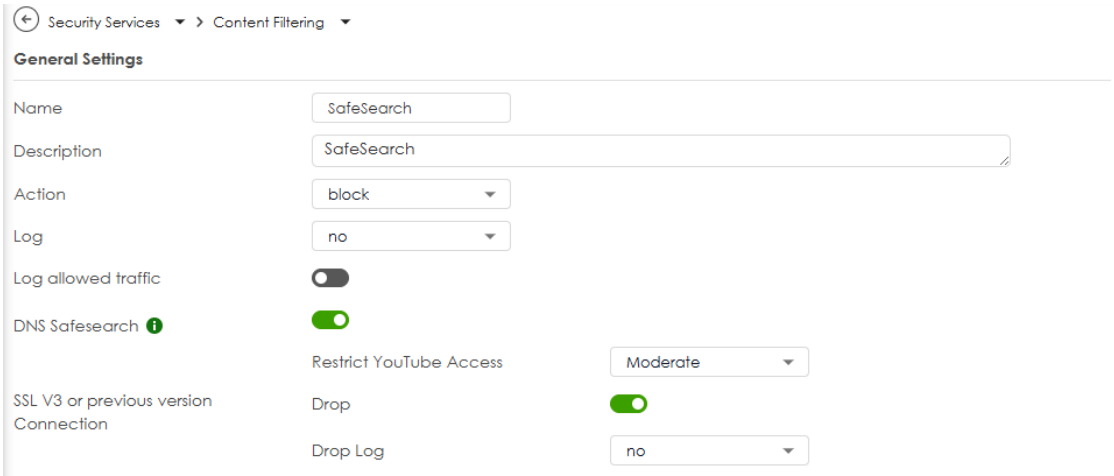
Configure the Profile

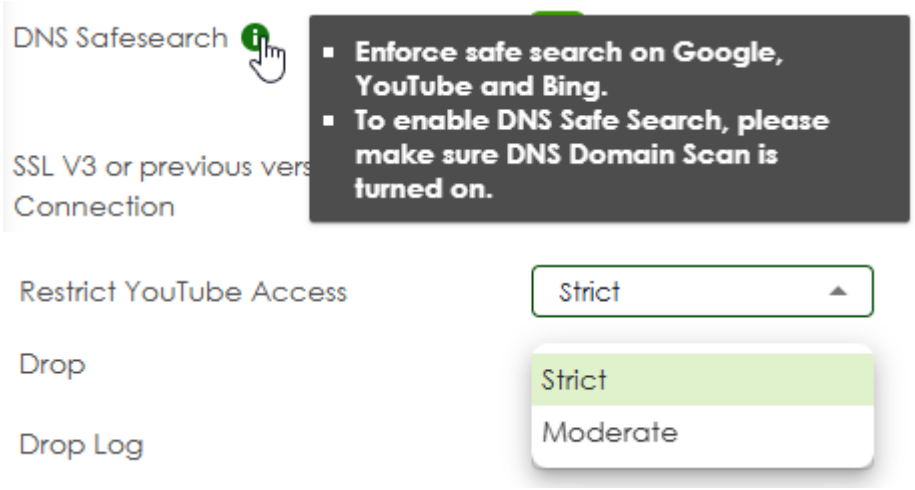
DNS Safesearch: Click the button to enable the function.

Enforce safe search on Google,Youtube,Bing.

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

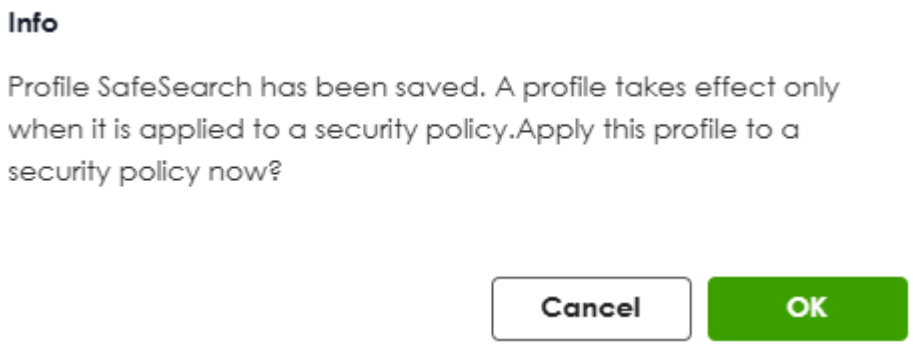
Restrict Youtube Access: The Restrict YouTube Access setting allows you to choose between Strict and Moderate modes.



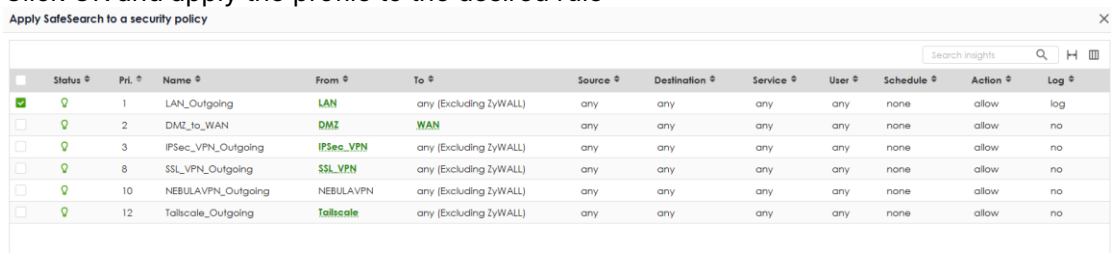


Step 2: Apply the safe search profile to Security Policy Rule

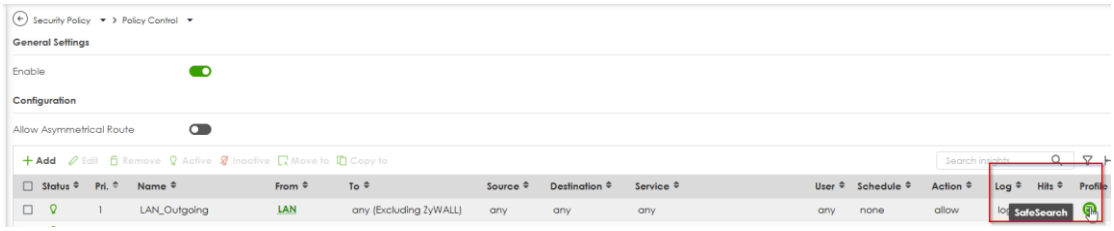
After completing the profile, a message will pop up to guide you in applying the profile to the Security Policy Rule



Click OK and apply the profile to the desired rule



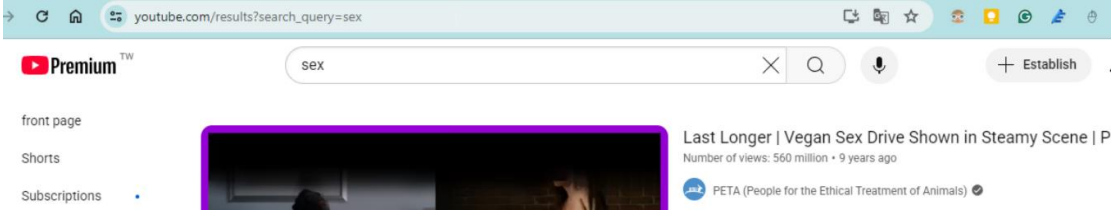
After implementation, please navigate to Security Policy > Policy Control to check if the rule has been correctly set up.



Step 3: Verified SafeSearch Function

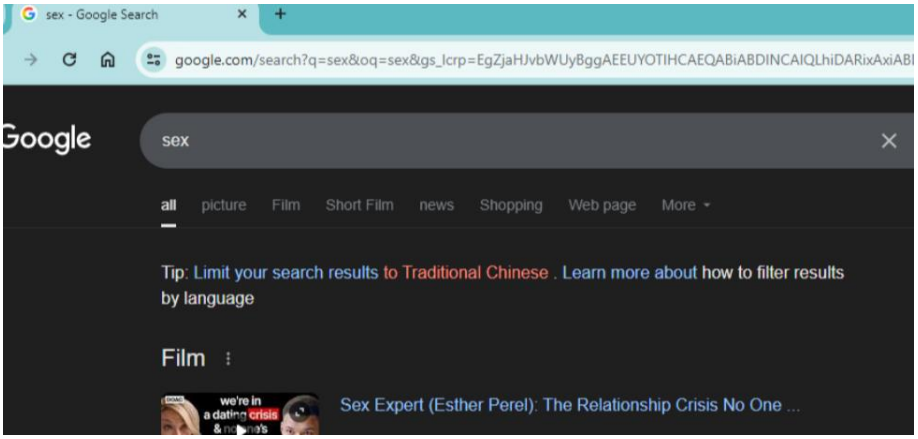
Before verified the SafeSearch, if there is no other setting on DNS, normally the query result will display as below.

www.youtube.com



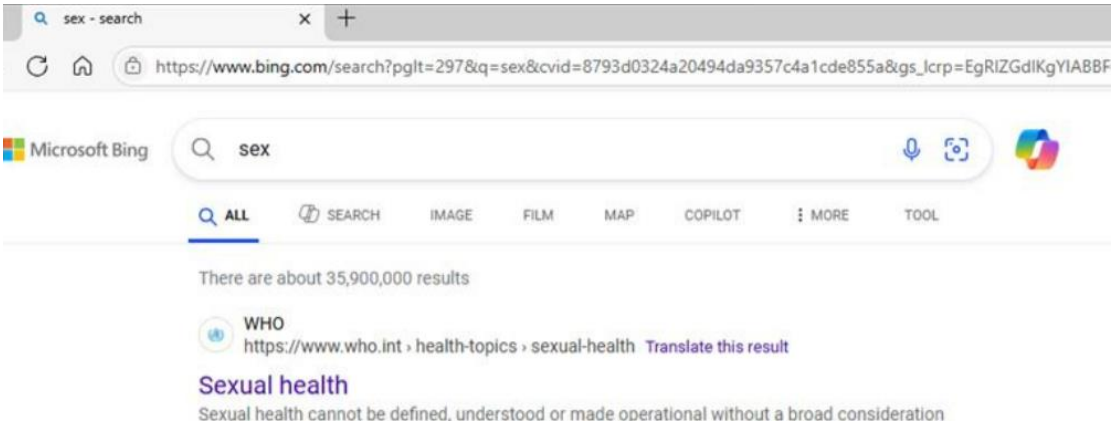
www.google.com

```
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
```

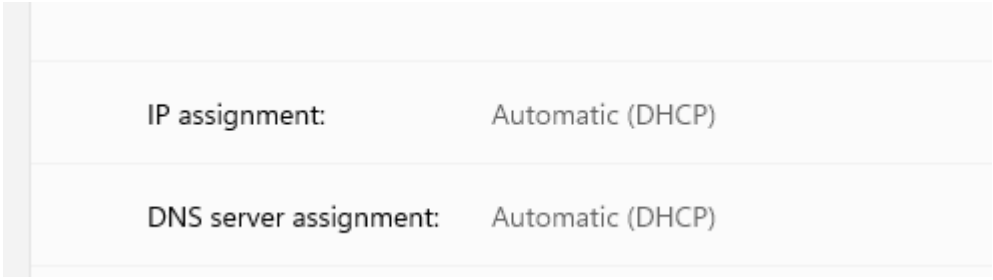


www.bing.com

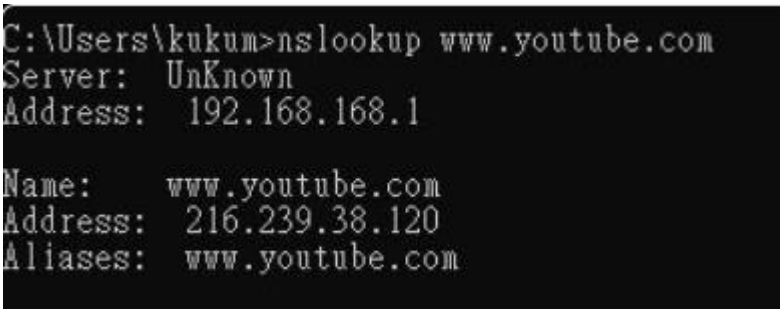
```
C:\Users\kukum>nslookup www.bing.com
Server:  UnKnown
Address:  192.168.168.1

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
```

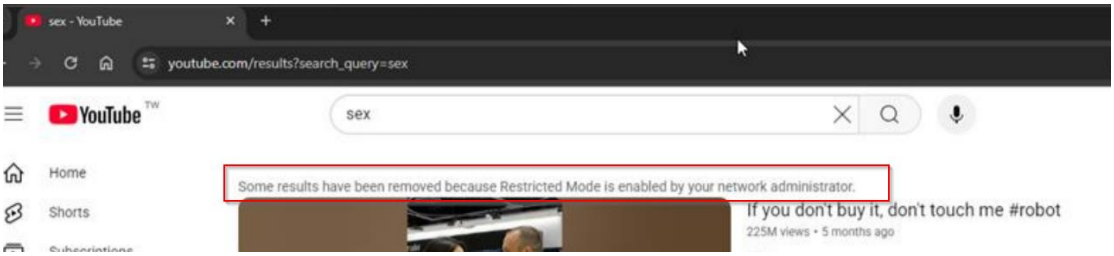



Ensure that the DNS server assignment is automatic get from the firewall.



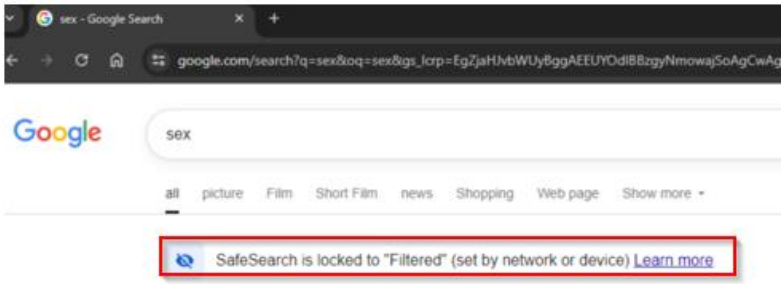
www.youtube.com





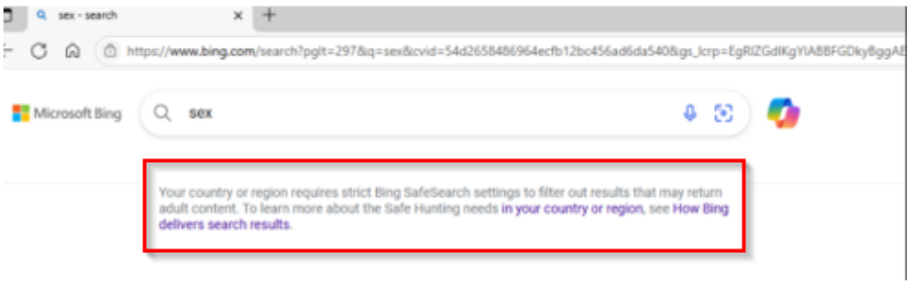
www.google.com

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

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



www.bing.com

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

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



Troubleshooting

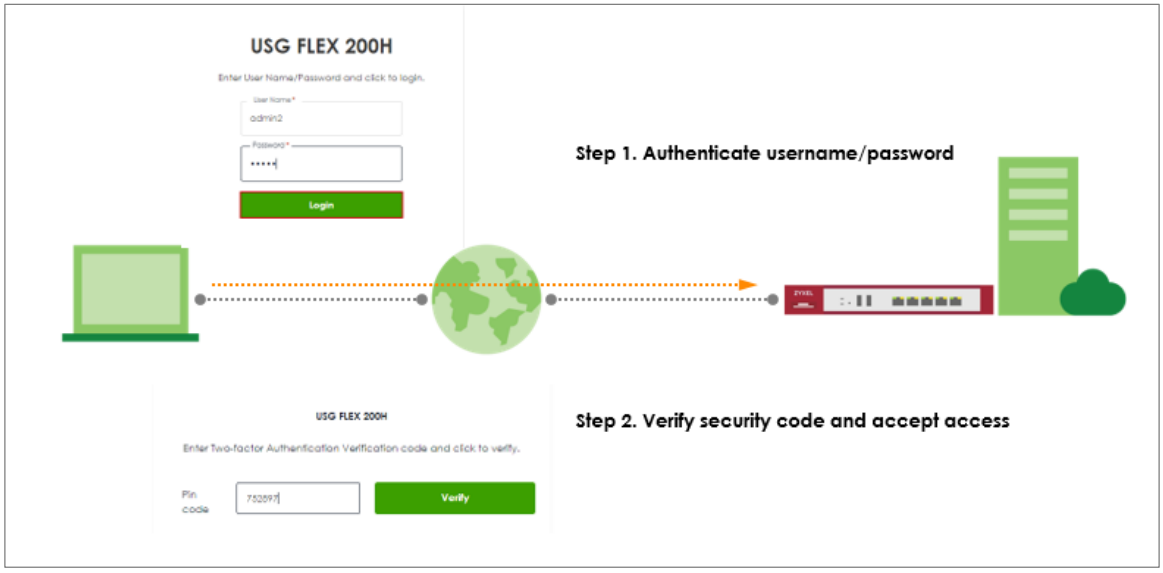
DNS Safe Search is not working

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

Chapter 3- Authentication

How to Use Two Factor with Google Authenticator for Admin Access

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



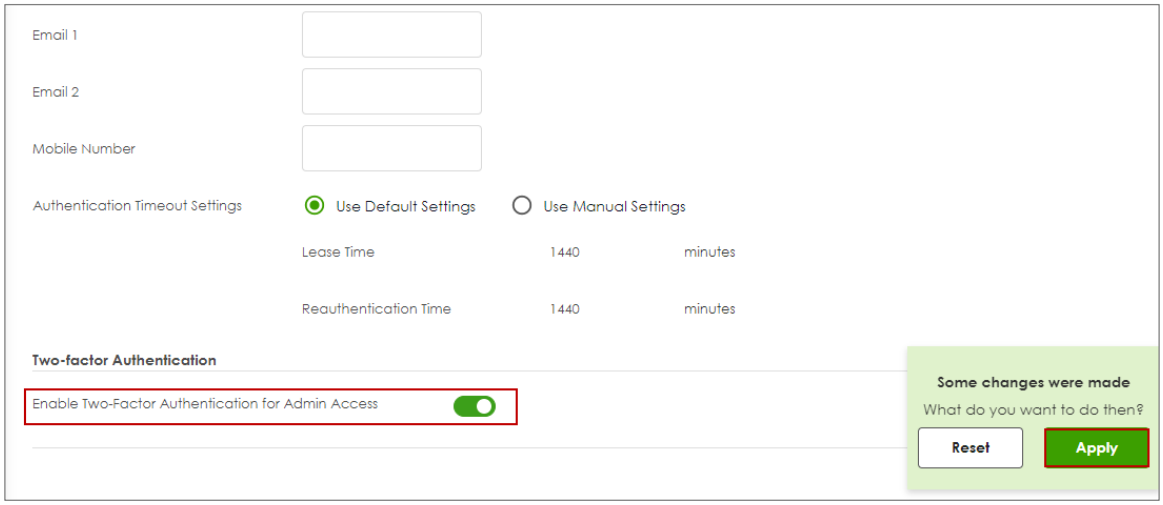
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Two Factor with Google Authenticator Flow

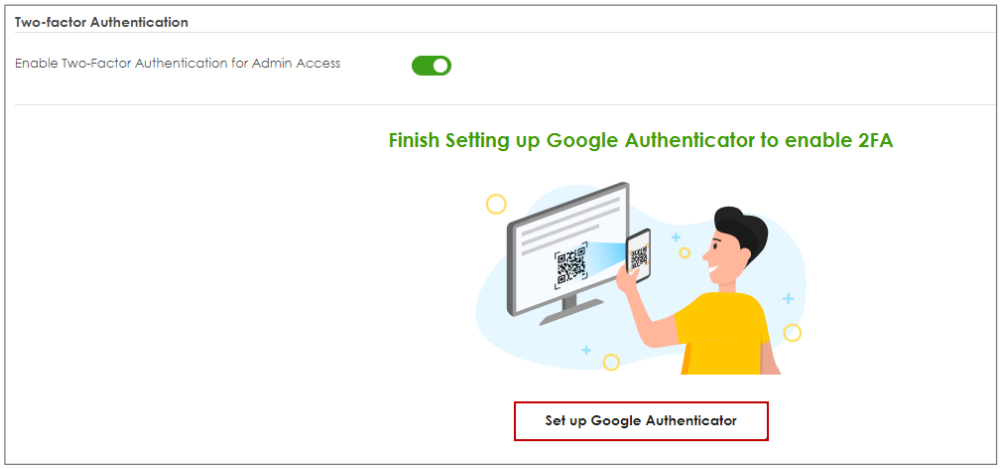
1. Enable Google Authentication on specific admin user.
2. Set up Google Authenticator.
3. Configure valid time and login service types.

Enable Google Authentication on specific admin user

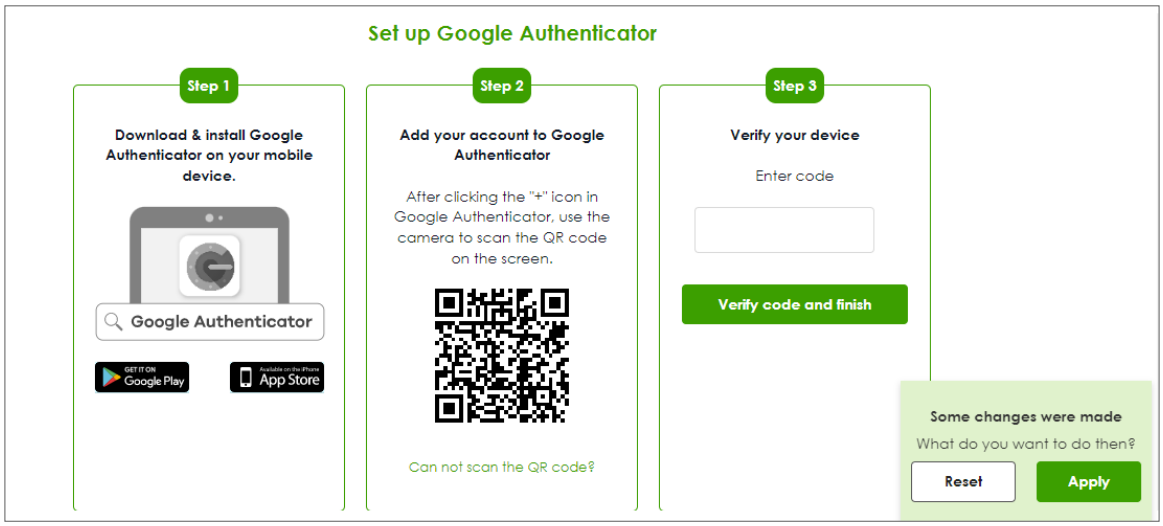
Go to User & Authentication > User/Group. Select a specific local administrator and enable Two-factor authentication.



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

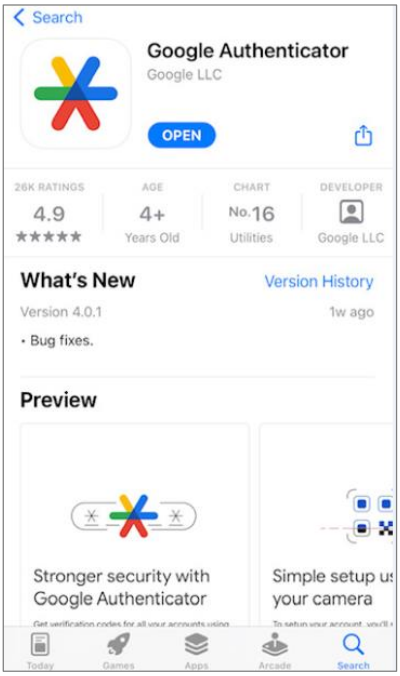


Set up Google Authenticator

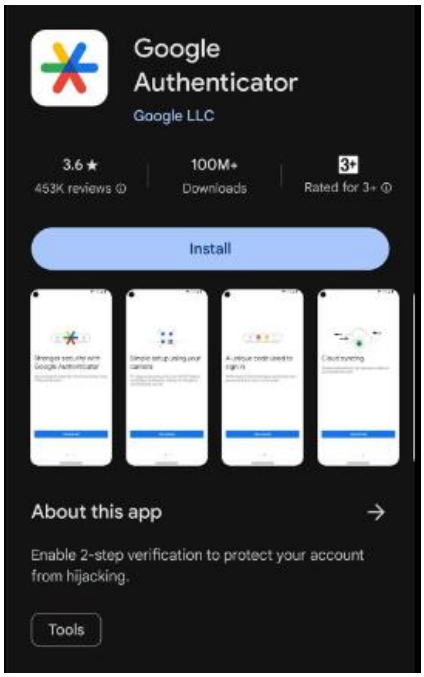


1. Download and install Google Authenticator on your mobile device.

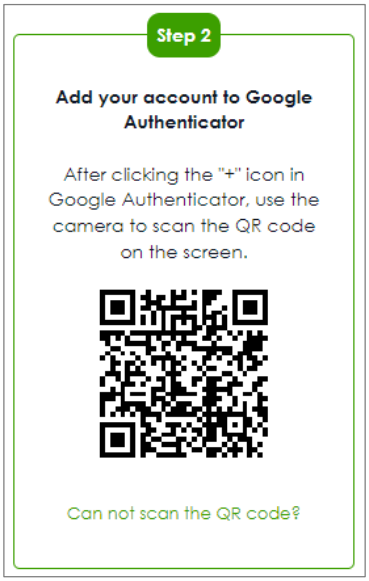
Apple Store

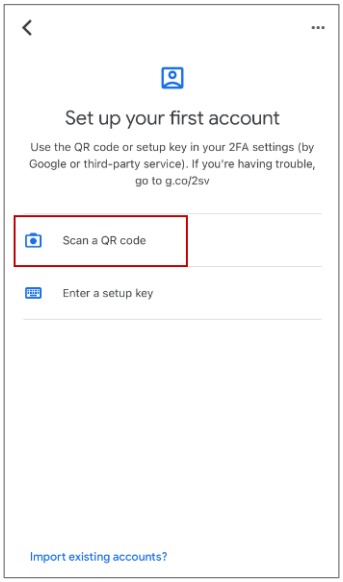


Google Play

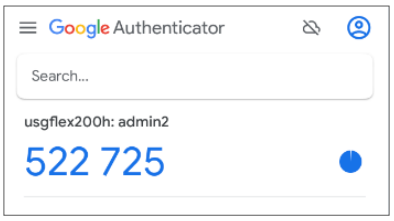


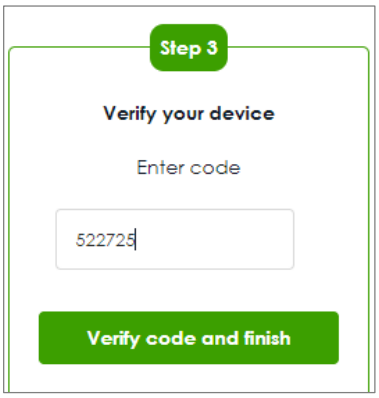
2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



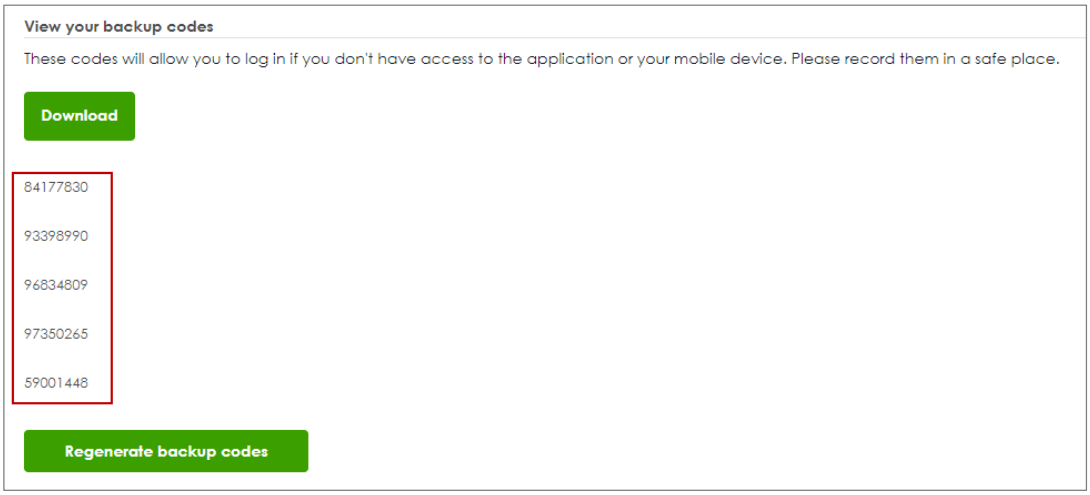


3. Enter the token code which displays on Google Authenticator to “Step 3” and click “Verify code and finish” to submit and verify the code.



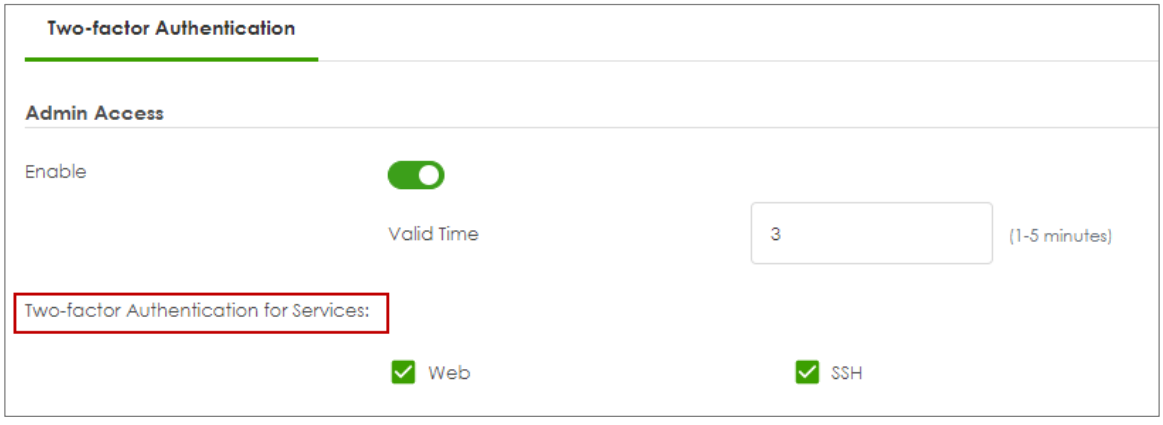


4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



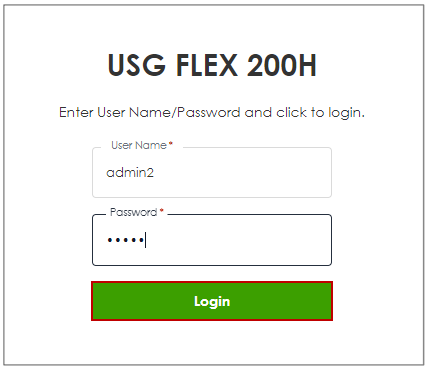
Configure valid time and login service types

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

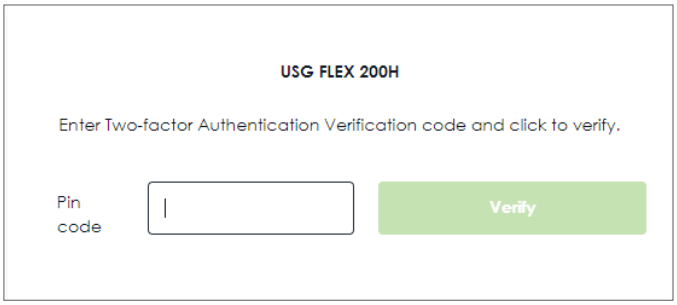


Test the Result

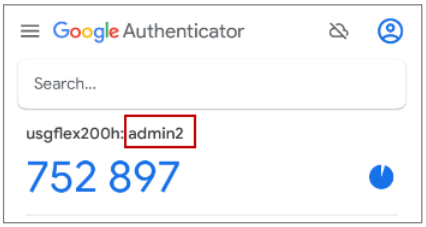
1. Login with the admin account "admin2".

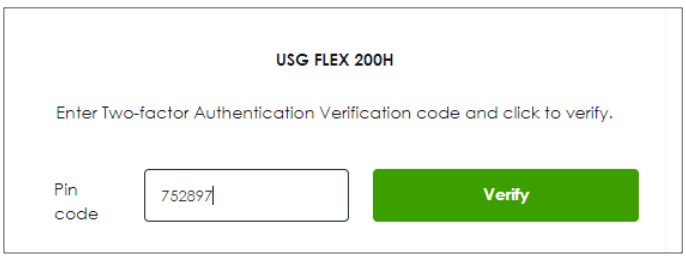


2. A pop-up window appears for administrator to enter the verification code.

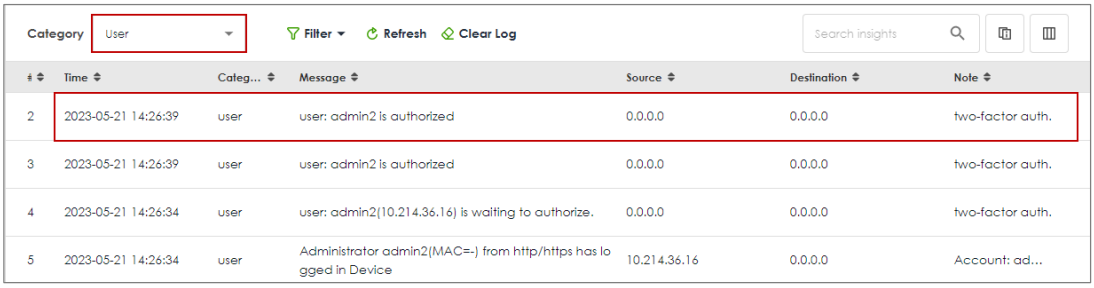


3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.





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	Categ...	Message	Source	Destination	Note
2	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
3	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
4	2023-05-21 14:26:34	user	user: admin2(10.214.36.16) is waiting to authorize.	0.0.0.0	0.0.0.0	two-factor auth.
5	2023-05-21 14:26:34	user	Administrator admin2(MAC=-) from http/https has logged in Device	10.214.36.16	0.0.0.0	Account: ad...

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

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

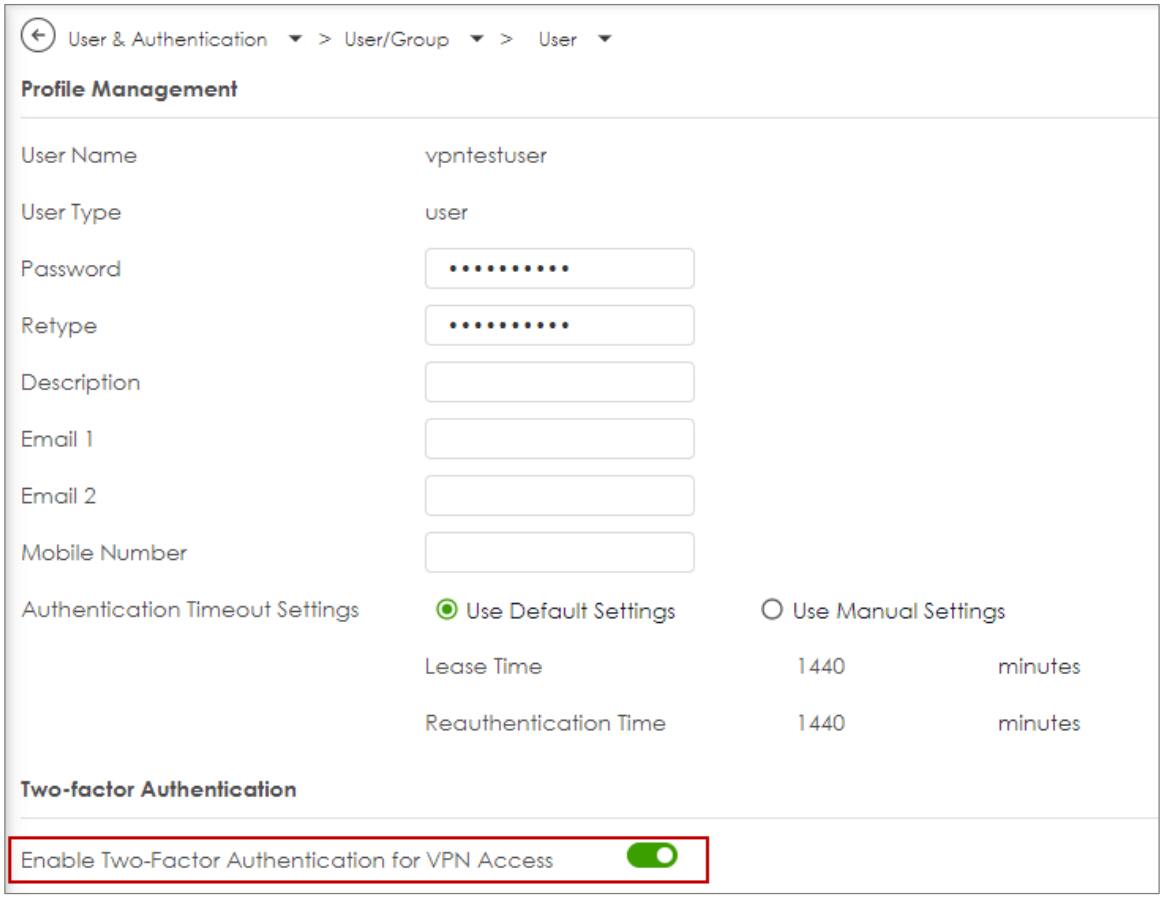
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Two Factor with Google Authenticator Flow

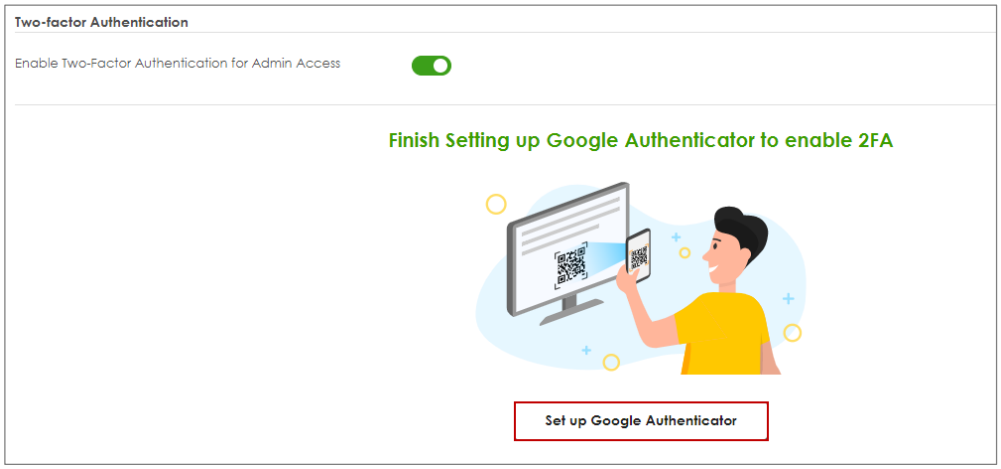
4. Enable Google Authentication on a user.
5. Set up Google Authenticator.
6. Configure valid time and VPN types.

Enable Google Authentication on a User

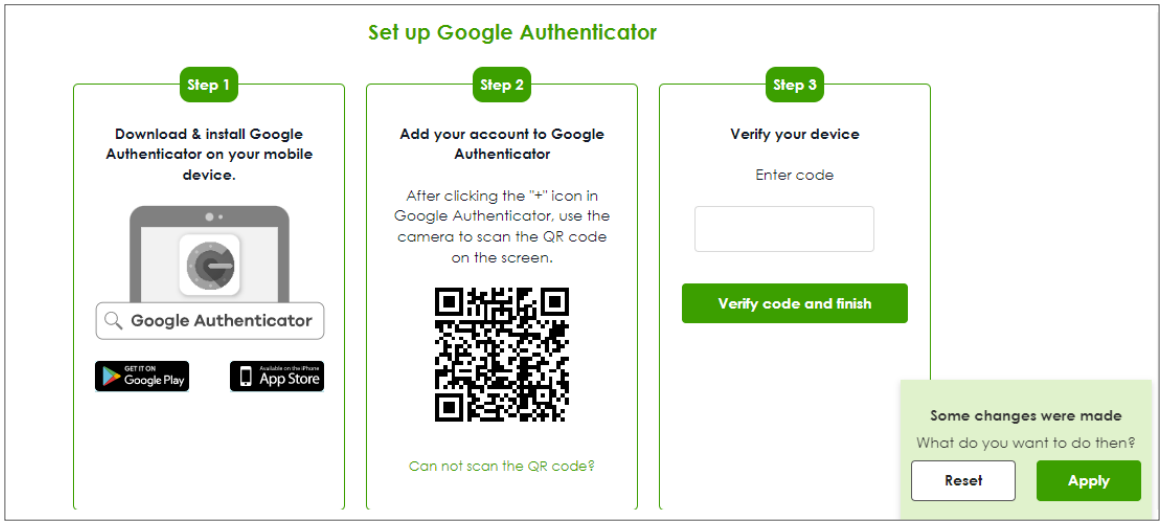
Go to User & Authentication > User/Group. Select a local user and enable Two-factor authentication.



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

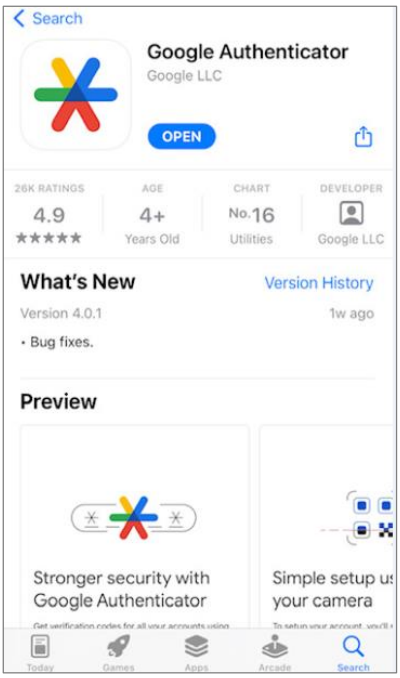


Set up Google Authenticator

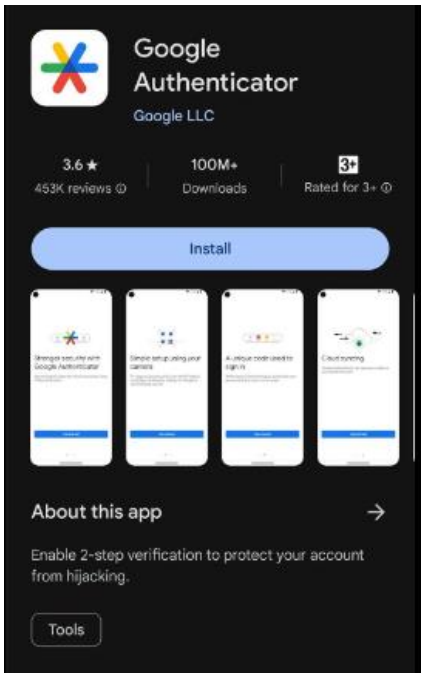


5. Download and install Google Authenticator on your mobile device.

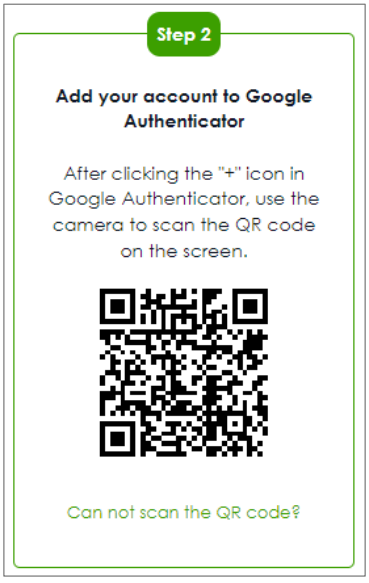
Apple Store

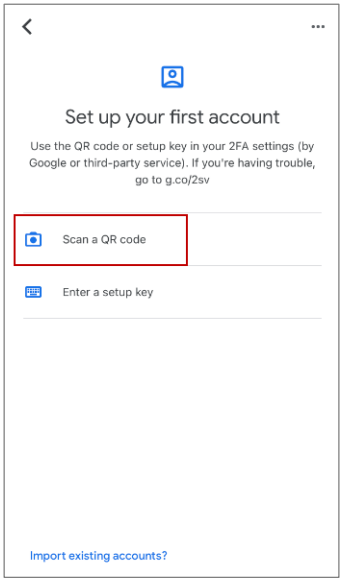


Google Play

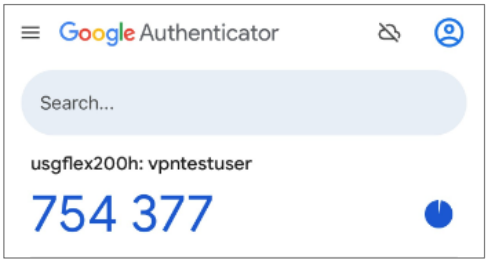


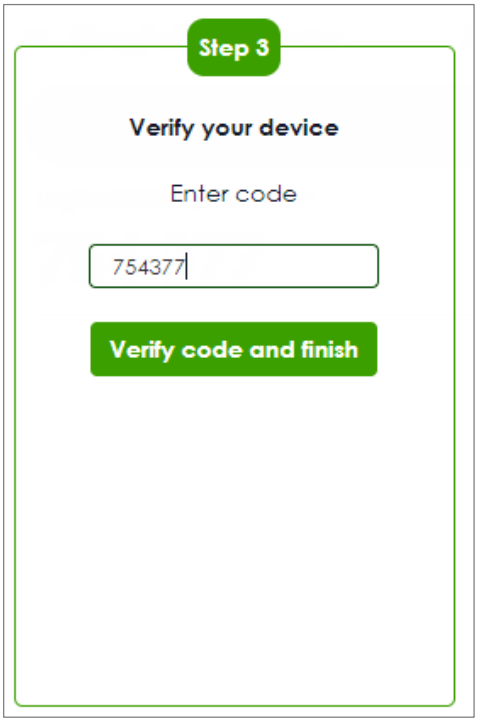
6. Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



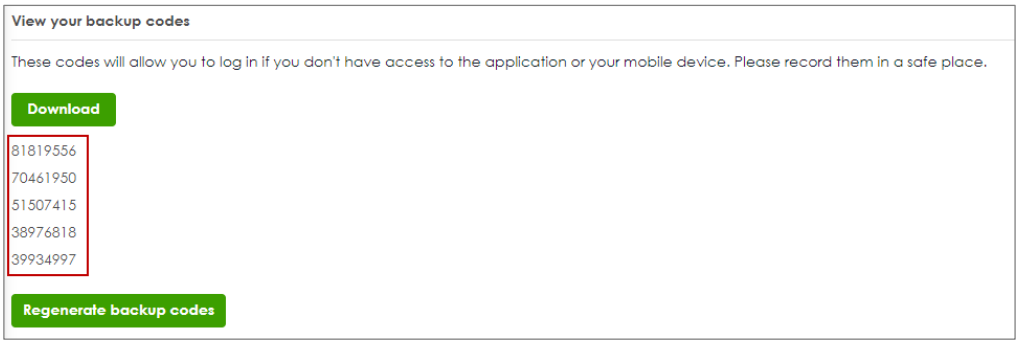


7. Enter the token code which displays on Google Authenticator to “Step 3” and click “Verify code and finish” to submit and verify the code.



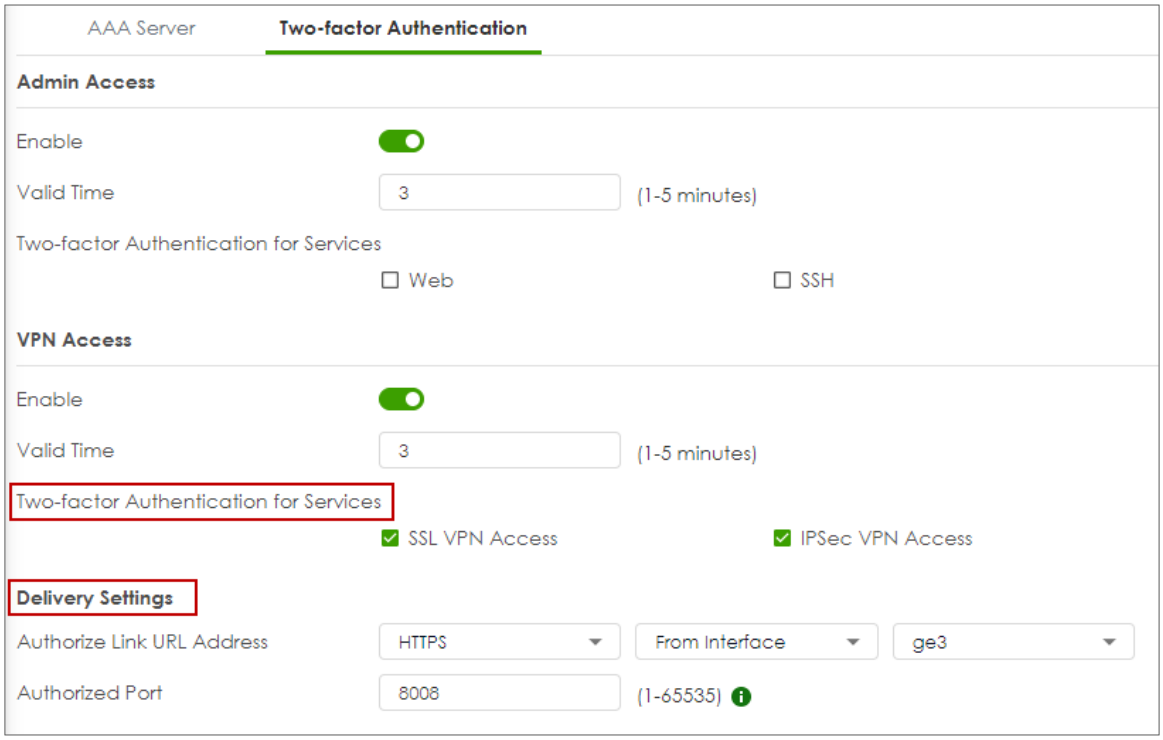


8. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



Configure valid time and login service types

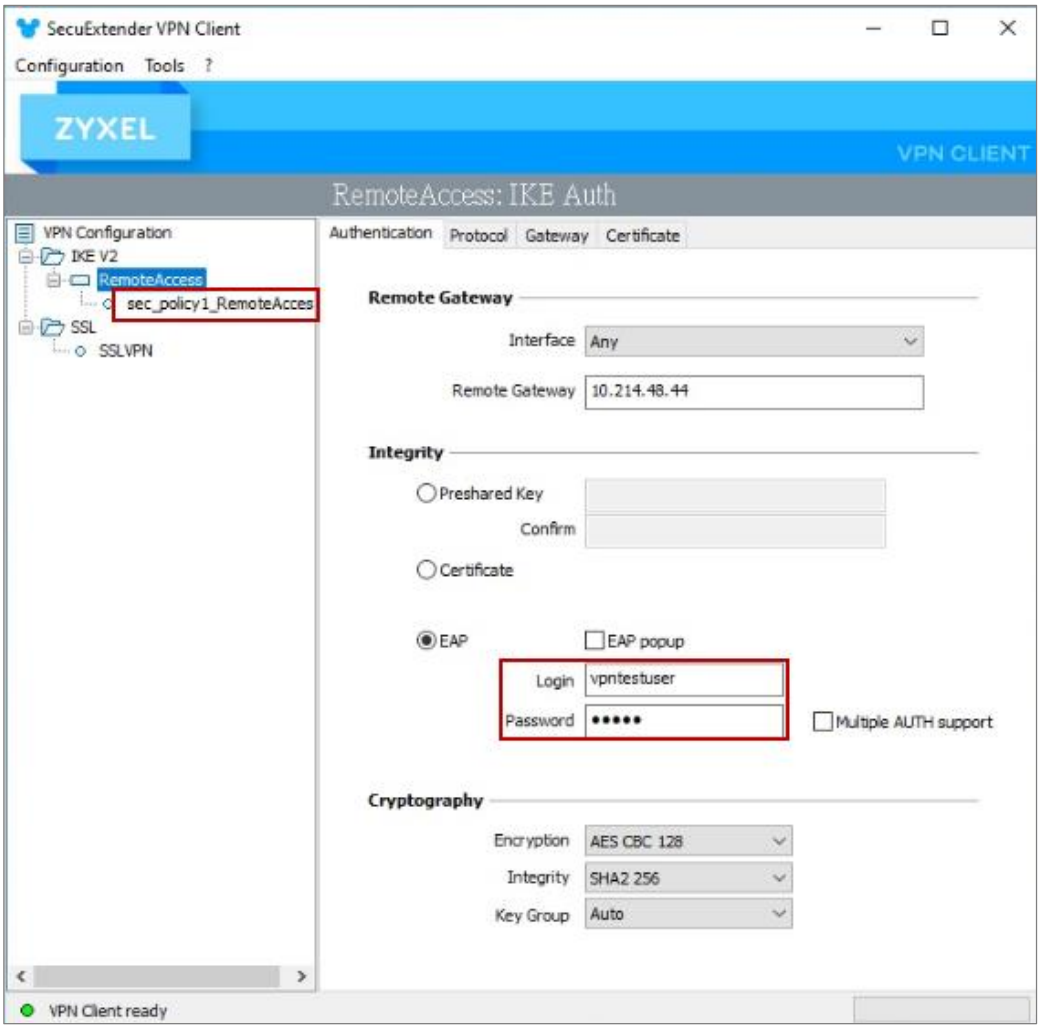
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the 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.



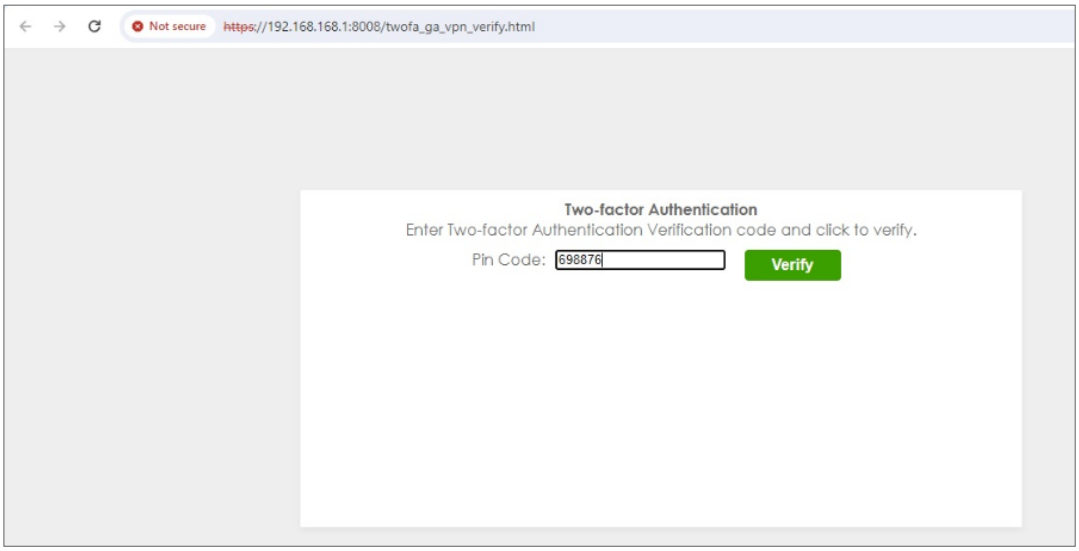
Test the Result

Remote Access VPN (IKEv2)

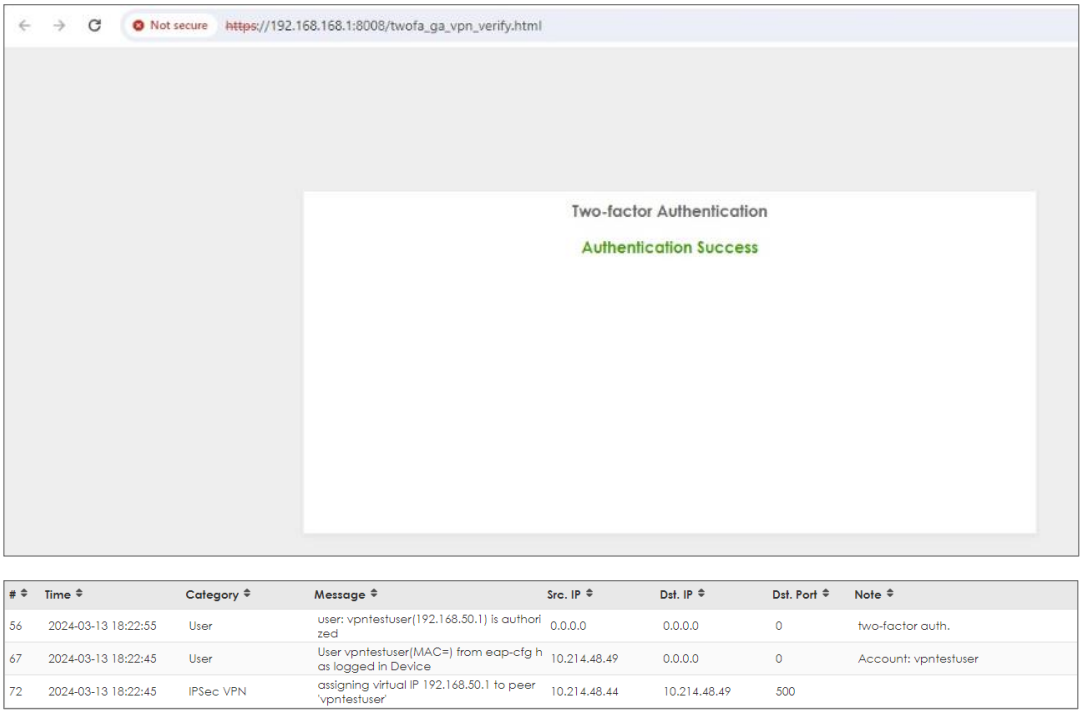
1. Open Remote Access VPN tunnel on SecuExtender VPN Client.



2. 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.



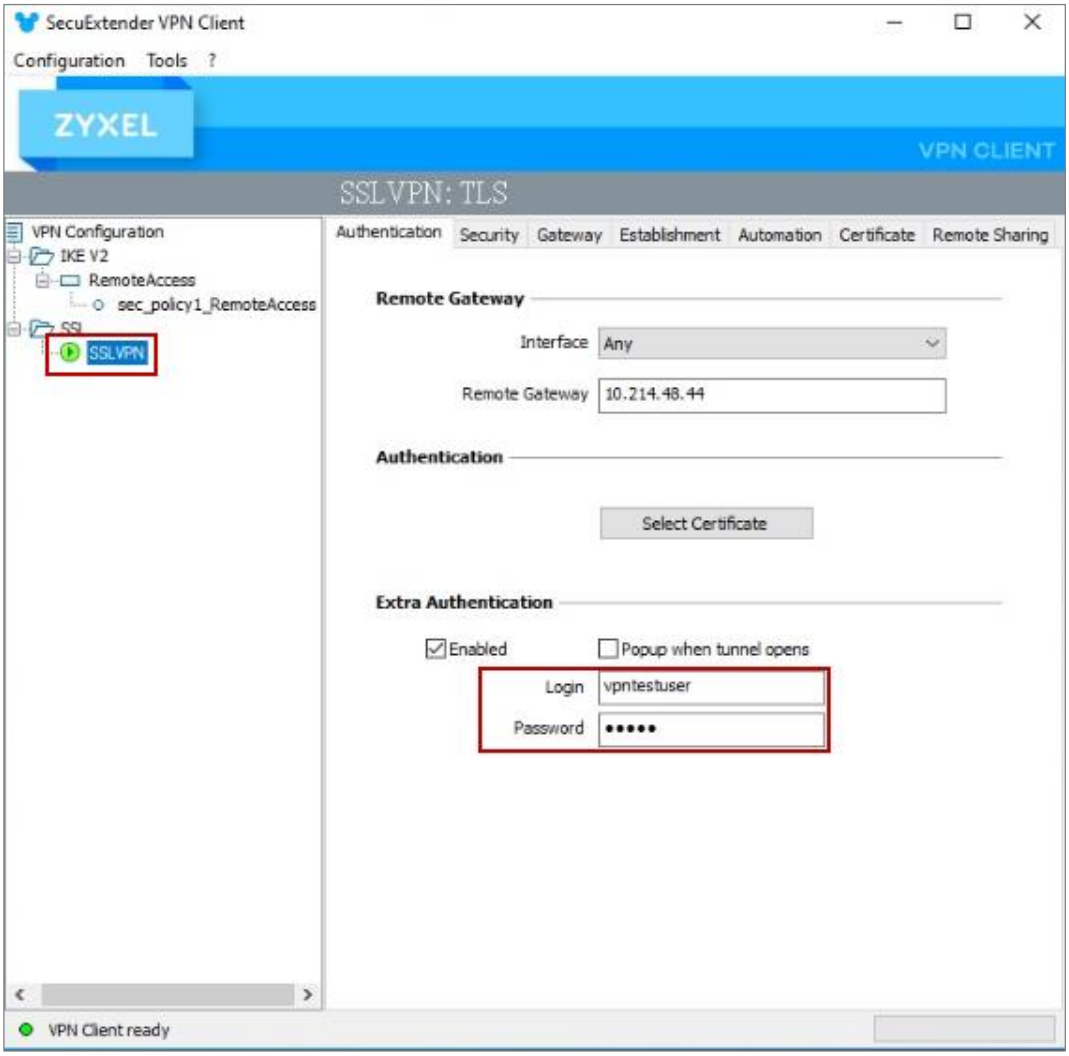
3. Authorize with username, password and the token code successfully.



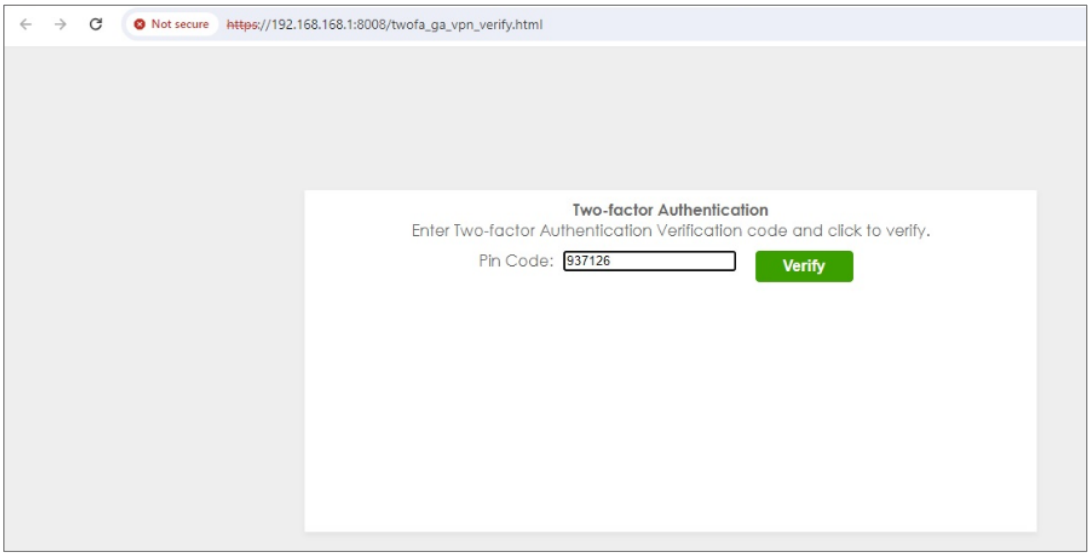
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	user: vpntestuser(192.168.50.1) is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
67	2024-03-13 18:22:45	User	User vpntestuser(MAC=) from eap-cfg has logged in Device	10.214.48.49	0.0.0.0	0	Account: vpntestuser
72	2024-03-13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

SSL VPN

1. Open SSL VPN tunnel on SecuExtender VPN Client.



2. 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.

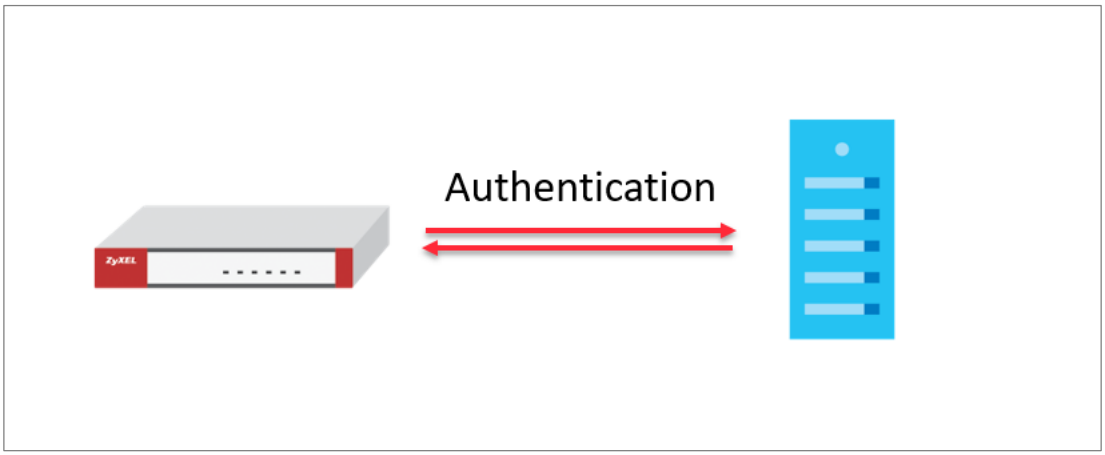


3. Authorize with username, password and the token code successfully.

#	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

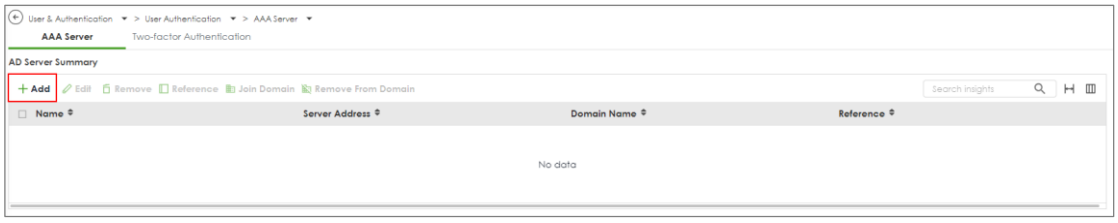
How to set up AD authentication with Microsoft AD

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.

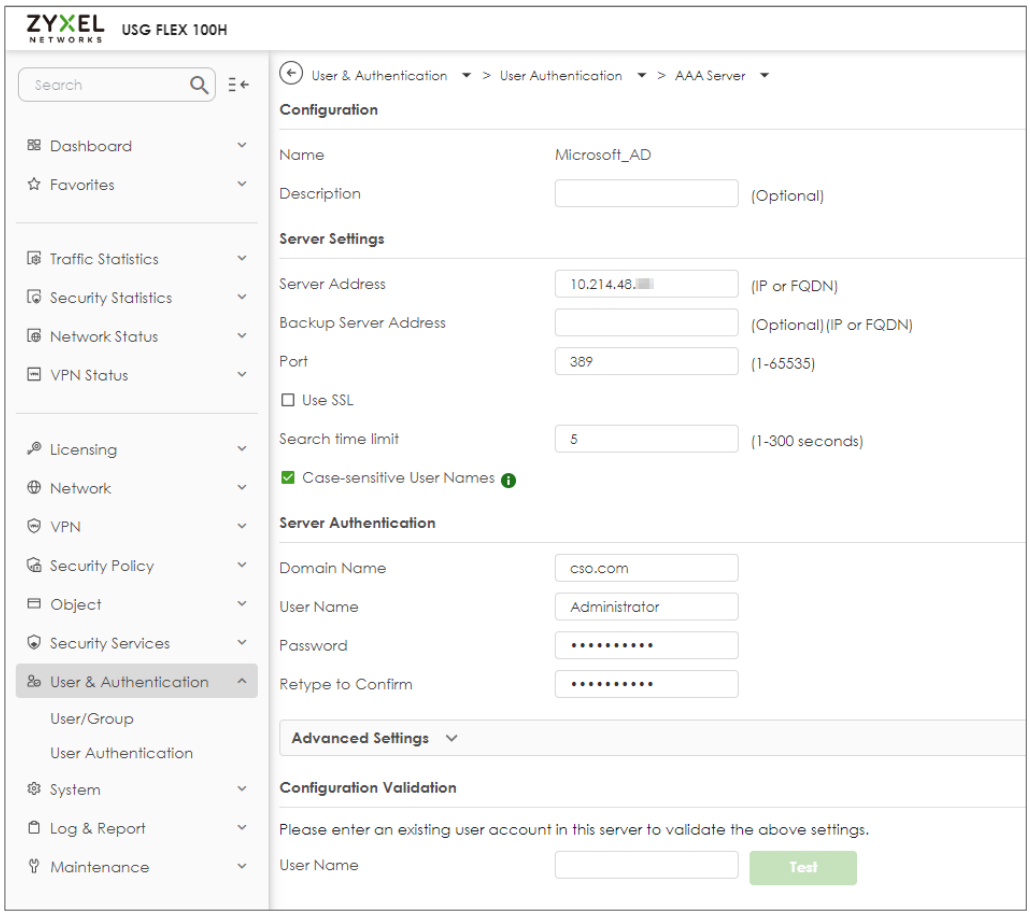


Set Up a profile for AD server

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

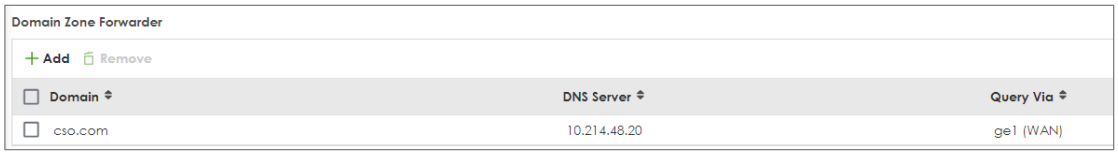


Enter the Server Address and port for Server settings. (10.214.48.XX:389 in this example). Enter the domain name and the credentials for logging into the AD server, and click Apply.



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.



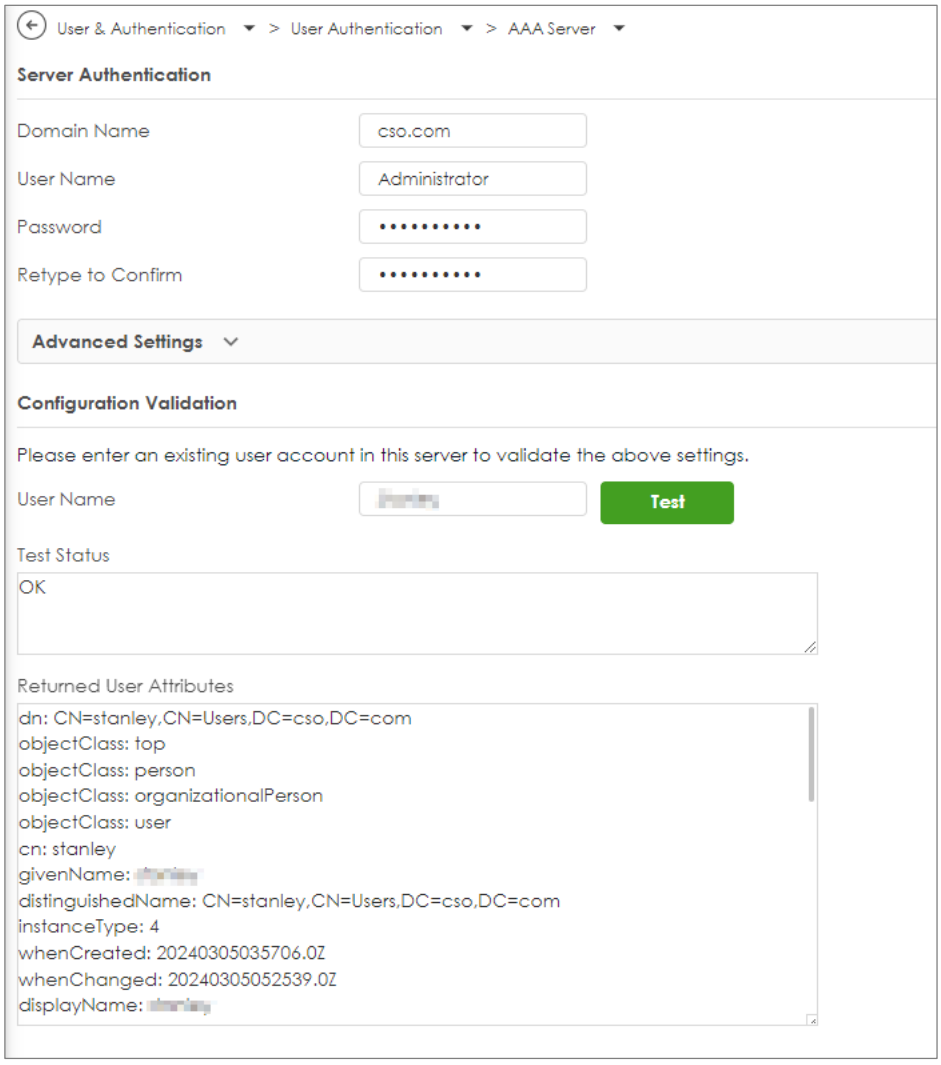
After the action above, go back to the profile page, tick it and click **Join Domain**

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

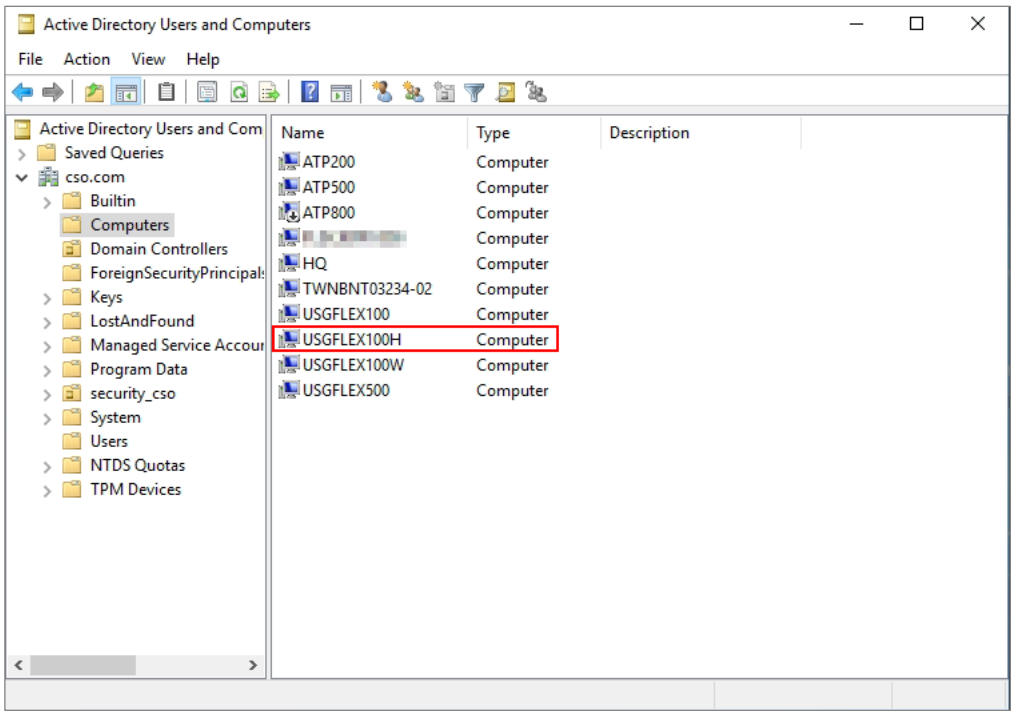
After join domain successfully, you can see this icon.

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.

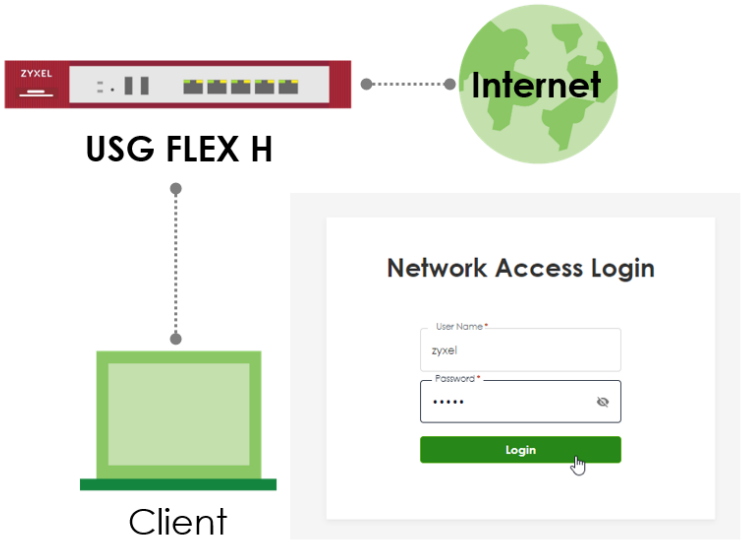


Check **computers** on Microsoft AD, you can see your firewall means join domain successfully.



How to Set Up Captive Portal?

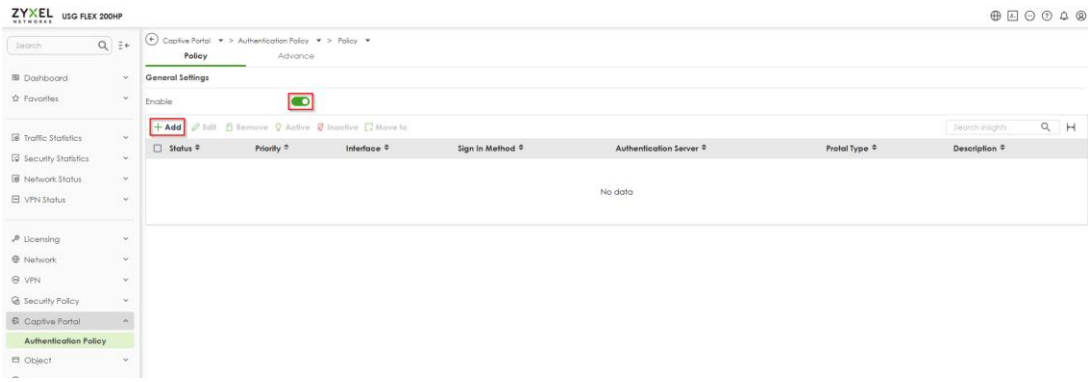
The Captive Portal feature provides functionality that requires LAN client users to complete the authentication procedure of Network Access Login page before accessing the internet. This article will guide users on how to set up and verify this feature.



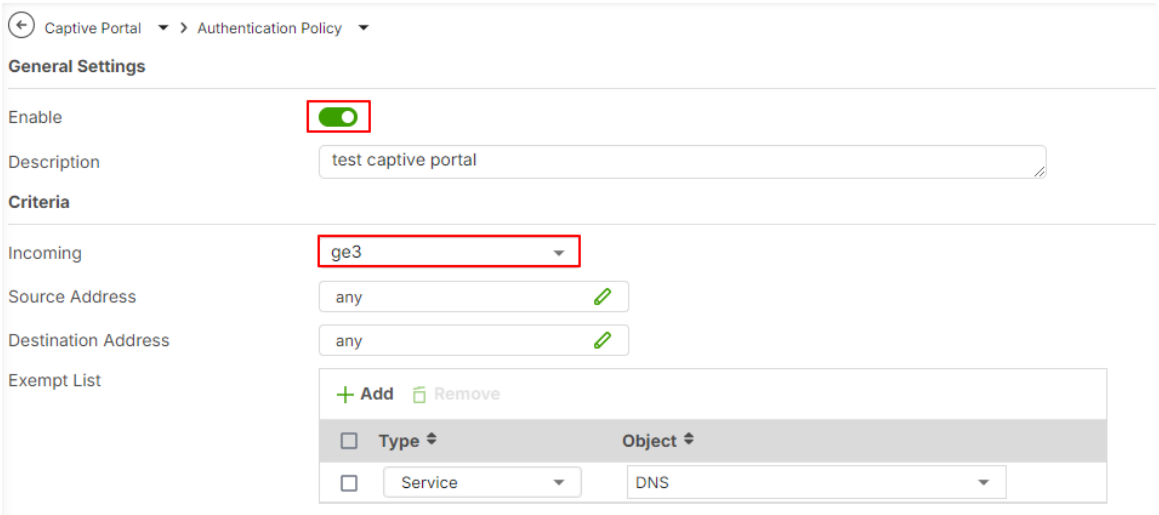
Note: Captive Portal is supported on USG Flex 100H, USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H.This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.32).

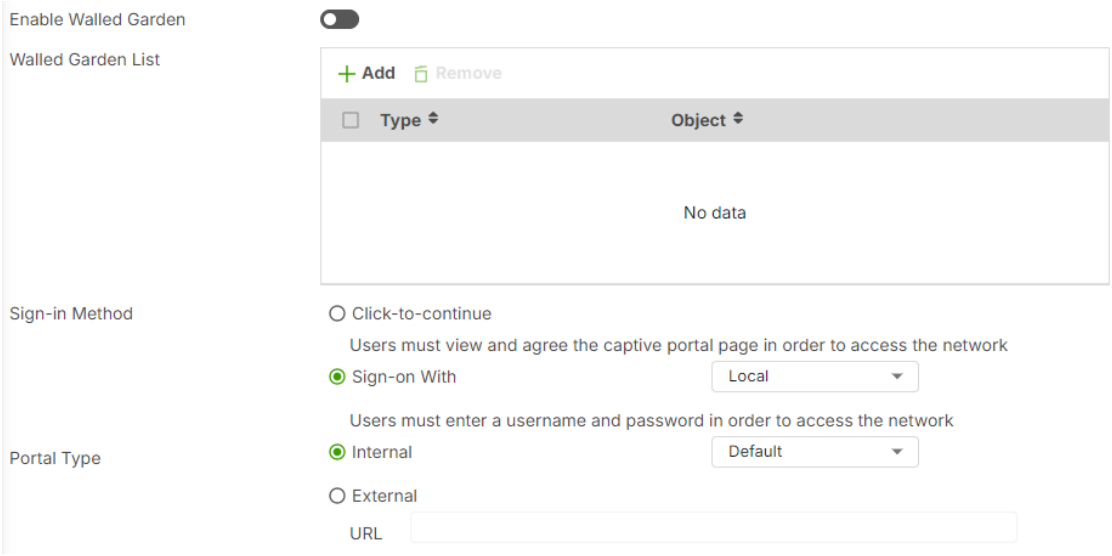
Configure the Captive Portal via the Web-GUI

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**.

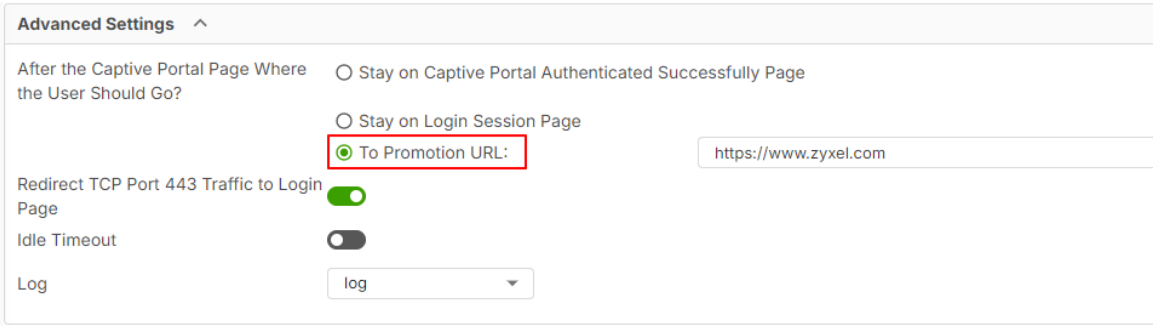


2. **Add an Authentication Policy** – Enable the Authentication Policy, provide a Description, select the Incoming interface, choose the Sign-In Method, specify the Authentication Server and Portal Type, Advanced Settings and enable Log.

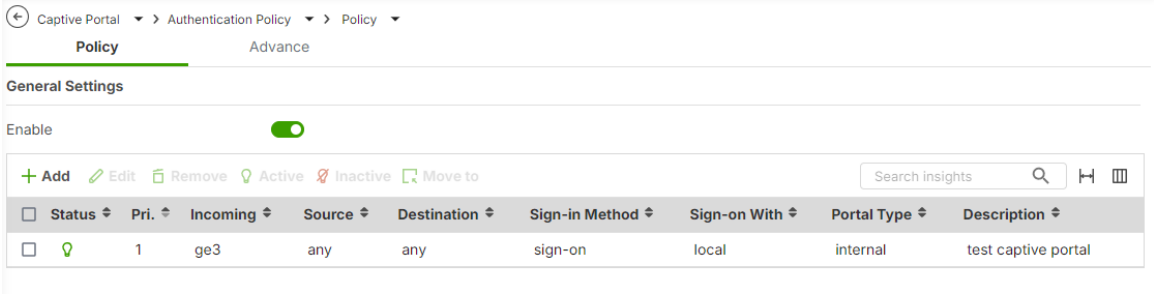




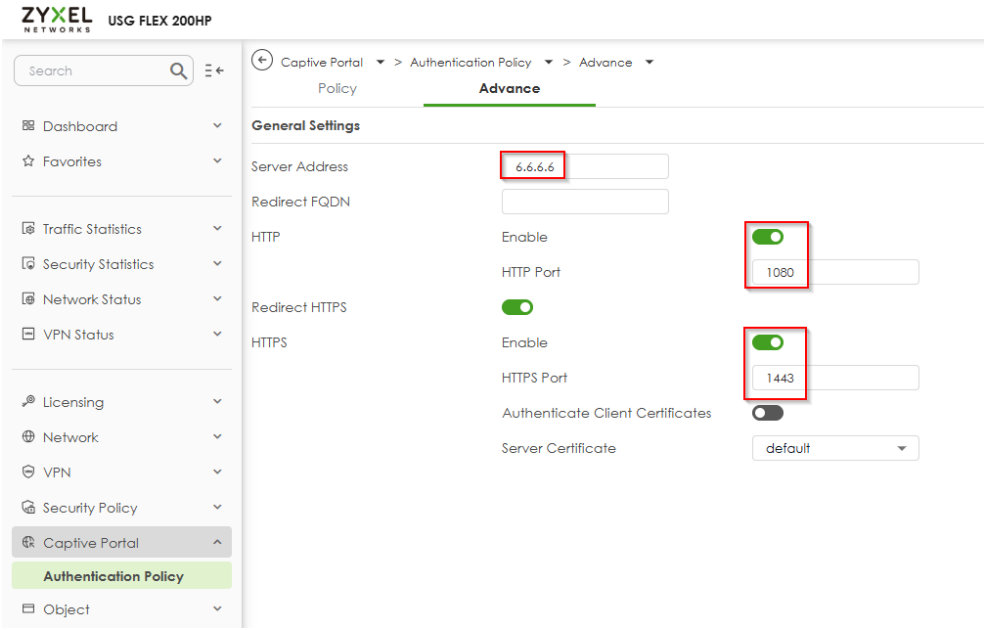
In this example, users will be redirected to the Promotion URL after logging in.



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



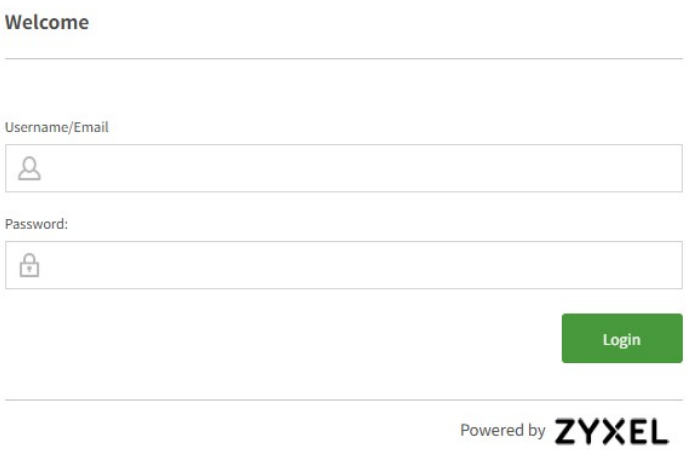
4. **Edit the Advance settings** – The default server address is 6.6.6.6, the default HTTP port is set to 1080, and the default HTTPS port is set to 1443.



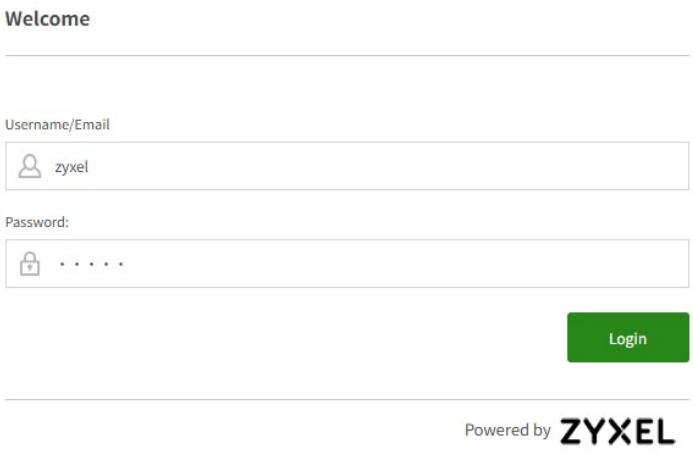
Verify the Captive Portal function

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

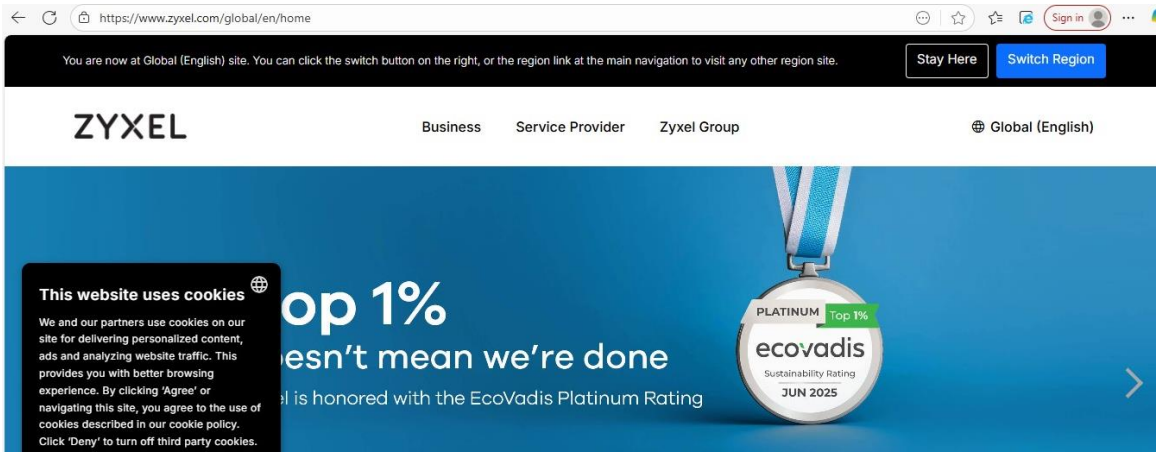
4. The PC client connects to the LAN port and opens the browser, which will be redirected to the Network Access Login page.



5. Enter the login User Name and Password.

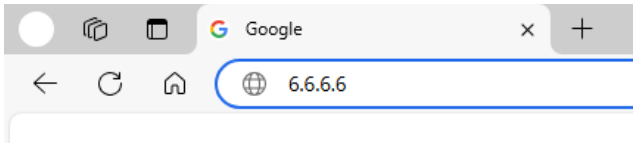


6. Once successfully logged into the Network Access Login page, the client will be redirected to the URL configured in "To Promotion URL". The client can access the Internet successfully.

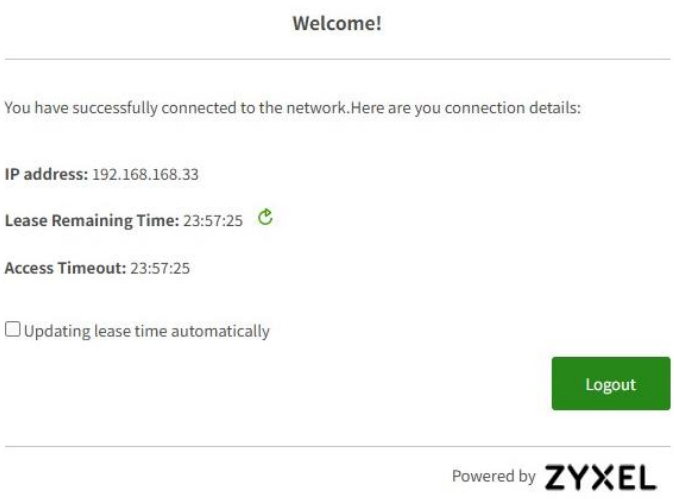


How to logout the Captive Portal?

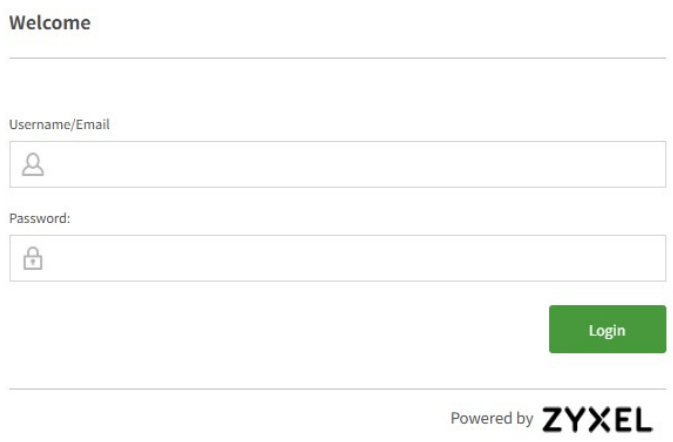
1. Enter the defined server link. The default link is https://6.6.6.6.



2. Enter the Welcome page and click “Logout”.

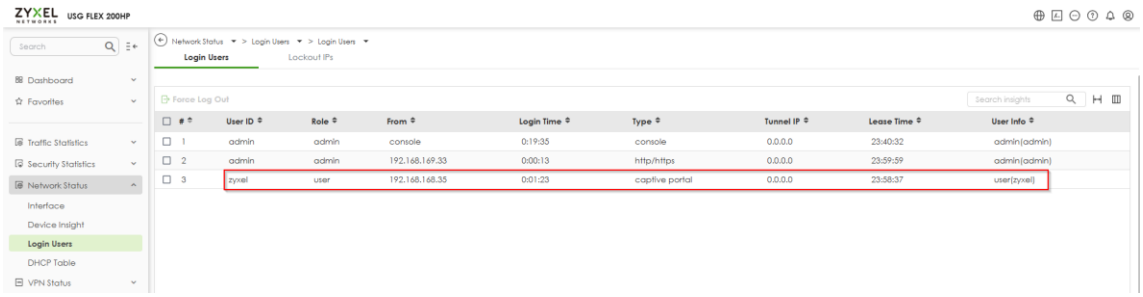


3. Redirect to the Network Access Login page. If the user needs to access the internet, they must re-enter the username and password to complete the Captive Portal authentication process.

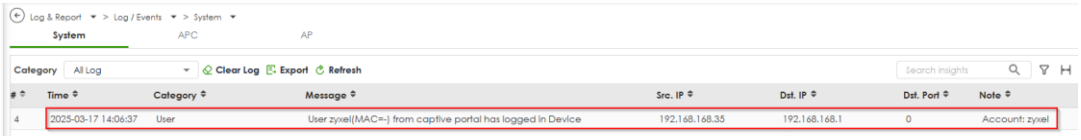


How to check the status?

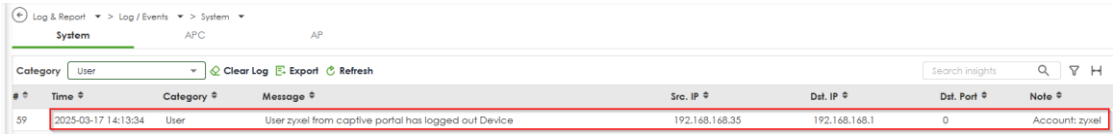
When the user successfully logs into the Captive Portal page, they can navigate to the GUI path: Network Status > Login Users > Login Users, to check if the user account has already logged into the Captive Portal.



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.



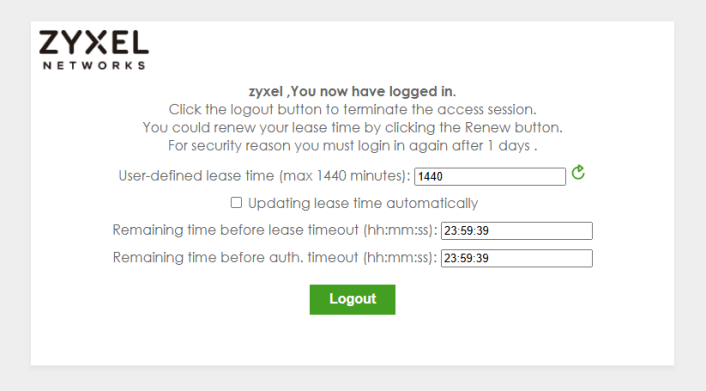
When the user successfully logs out the Captive Portal page, they can navigate to the GUI path: Log & Report > Log / Events > System, to verify the log message indicating that they have successfully logged out the captive portal.



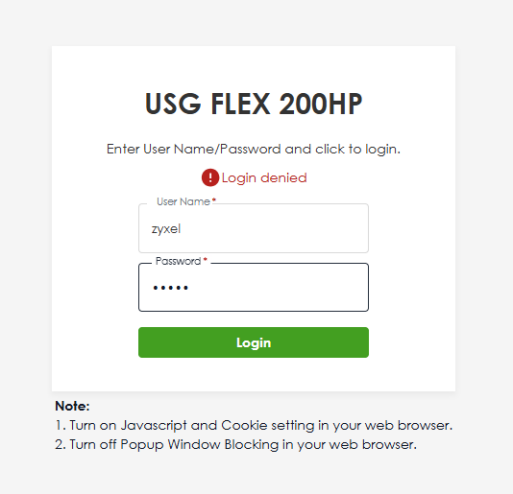
Feature Change:

> 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:

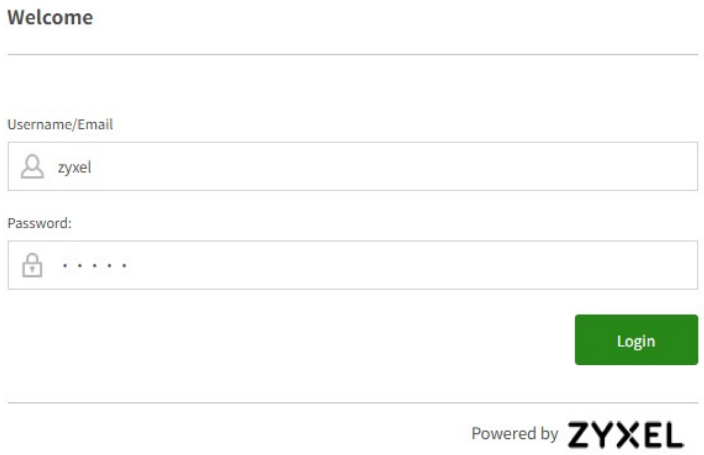


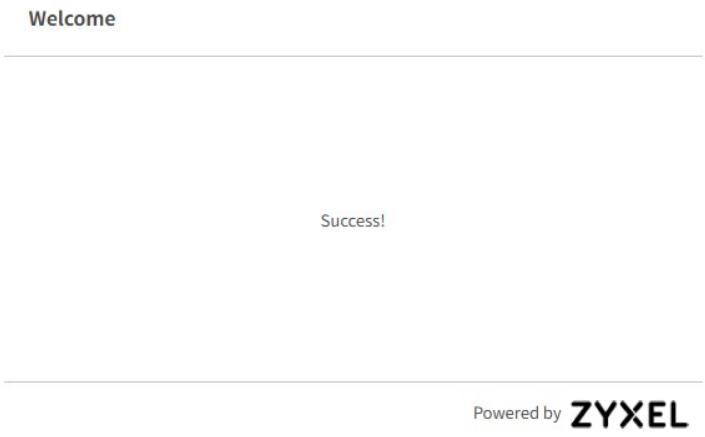
Starting from firmware version uOS 1.32, if an account that does not belong to the Local Administrator attempts to log in to the Web-GUI page, access will be denied, as shown below:



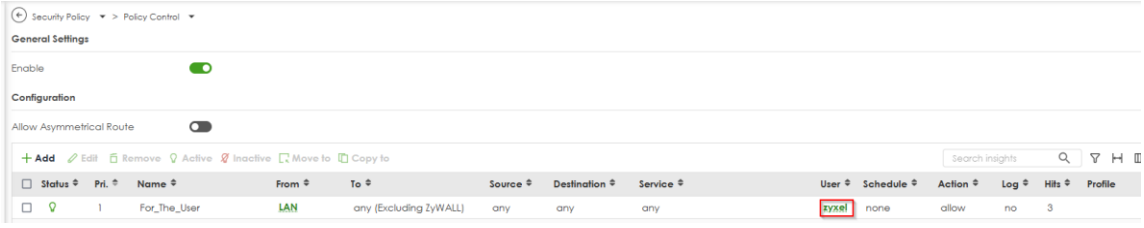
Therefore, starting from firmware version uOS 1.32, if users wish to utilize security policies or BWM policies for login users, they need to enable the Captive Portal function. Users must successfully log in to the Network Access Login page to activate the security or BWM policies, as show in below:

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



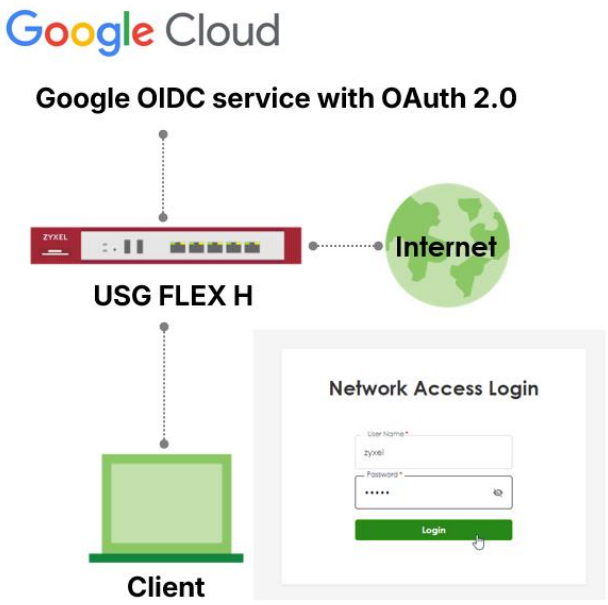


They can then activate the security or BWM policies for the specific user account.



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:

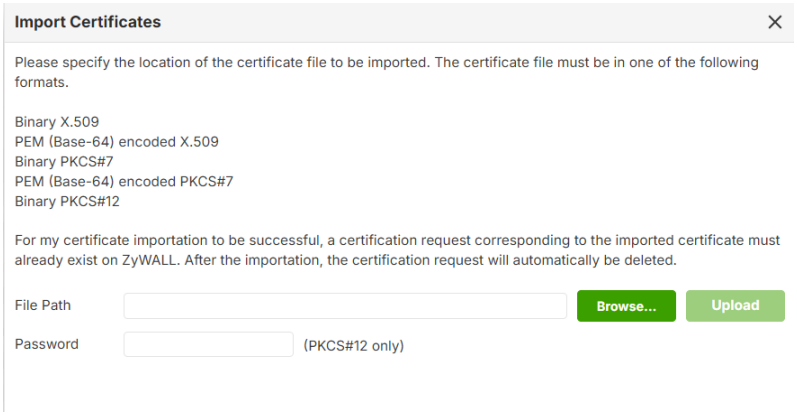
- The **Common Name (CN)** or **Subject Alternative Name (SAN)** must be a **Fully Qualified Domain Name (FQDN)**
- The FQDN must resolve to the **Captive Portal server address**
    - Default Captive Portal address: 6.6.6.6

Example:

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

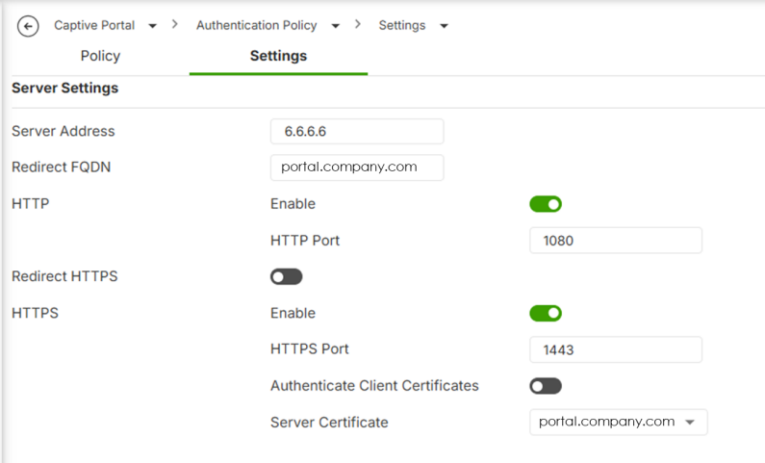
Uploading the Certificate to the USG FLEX H Series

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.



Assigning the Certificate to Captive Portal

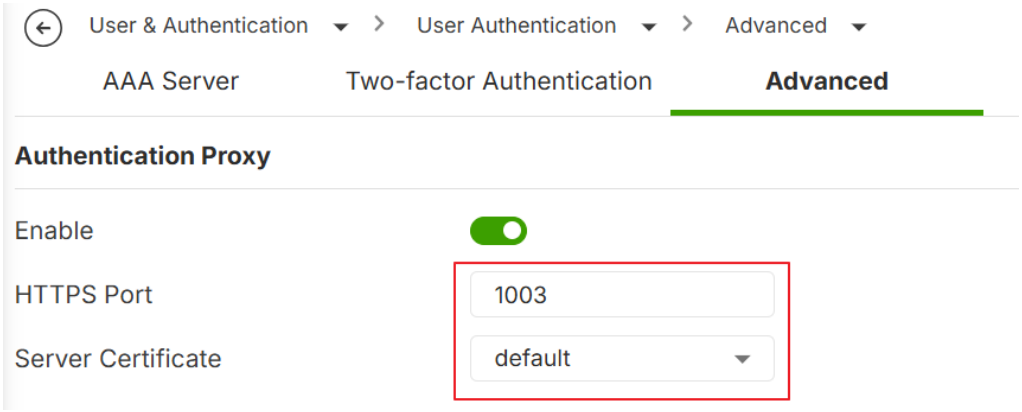
1. Go to **Captive Portal > Authentication Policy > Settings.**
2. Locate the **HTTPS / Server Certificate** settings.
3. Select the imported certificate.
4. Apply the configuration.



Authentication Proxy

Navigate to User & Authentication > User Authentication > Advanced.

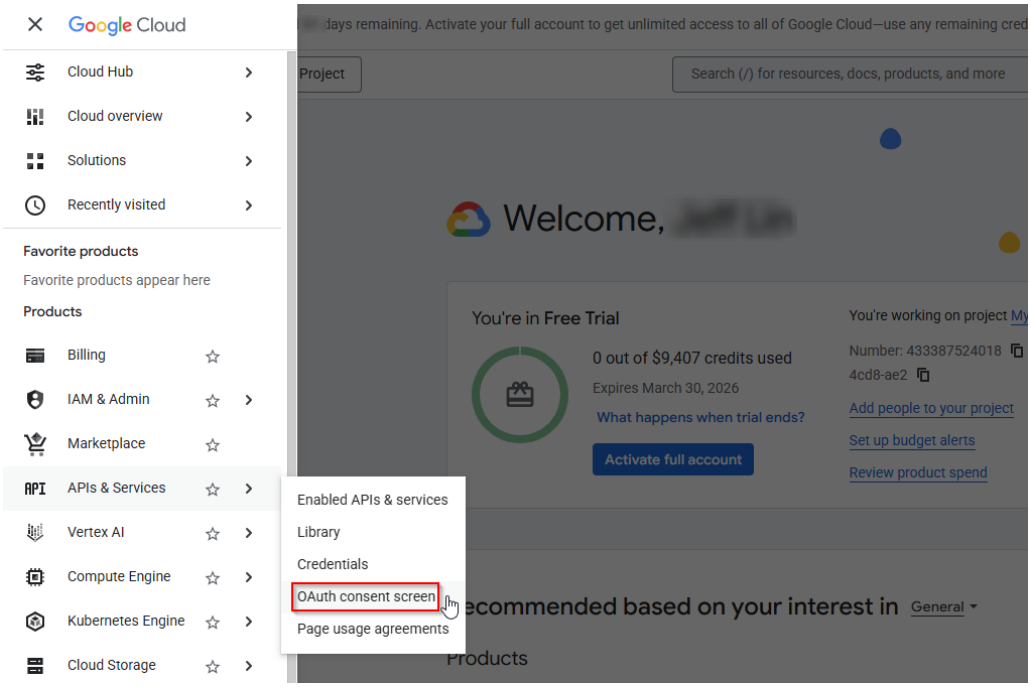
To prevent certificate warnings during the authentication phase, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve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



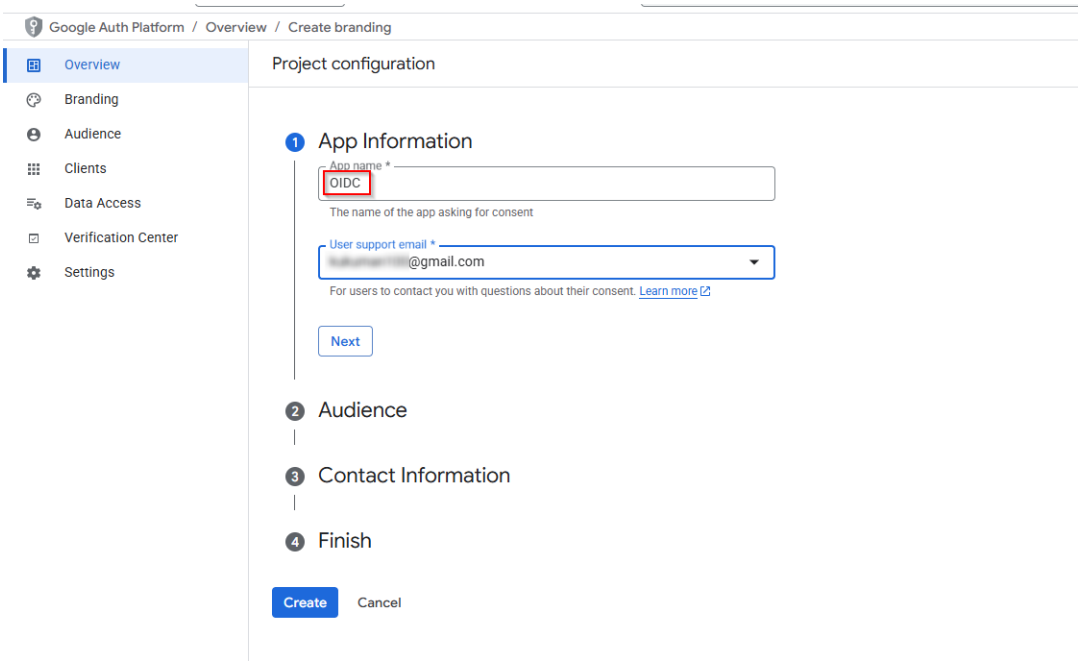
Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

Google Workspace/Cloud

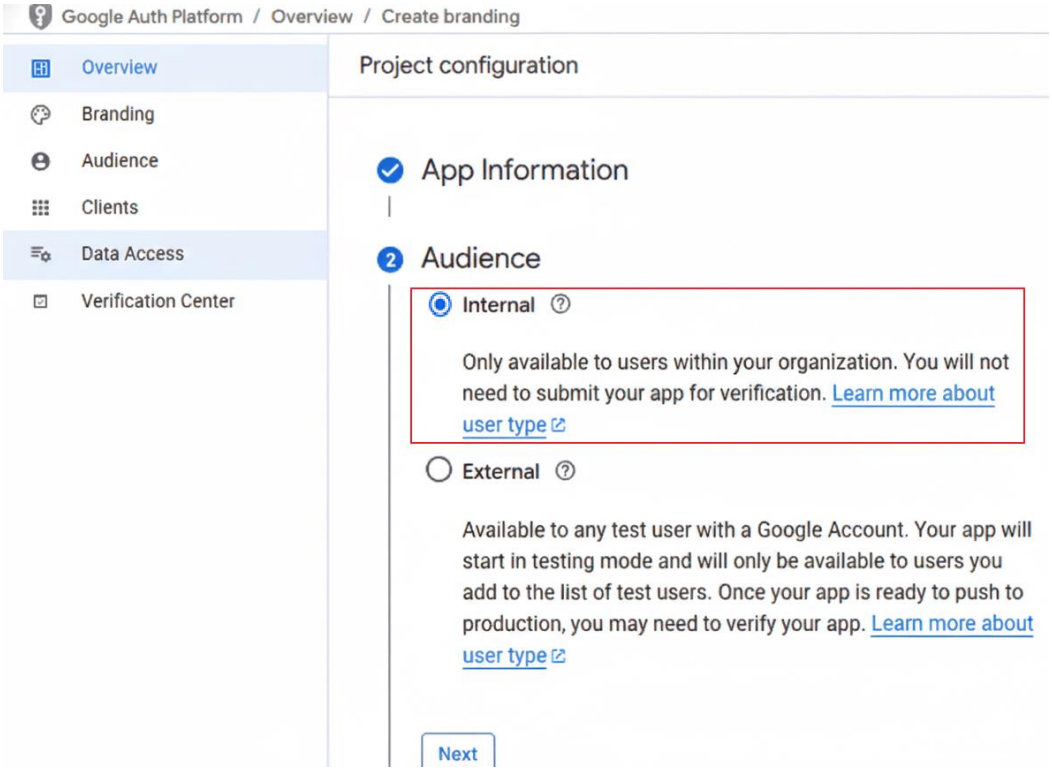
Go to Google Cloud Console > APIs & Services > OAuth consent screen.



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

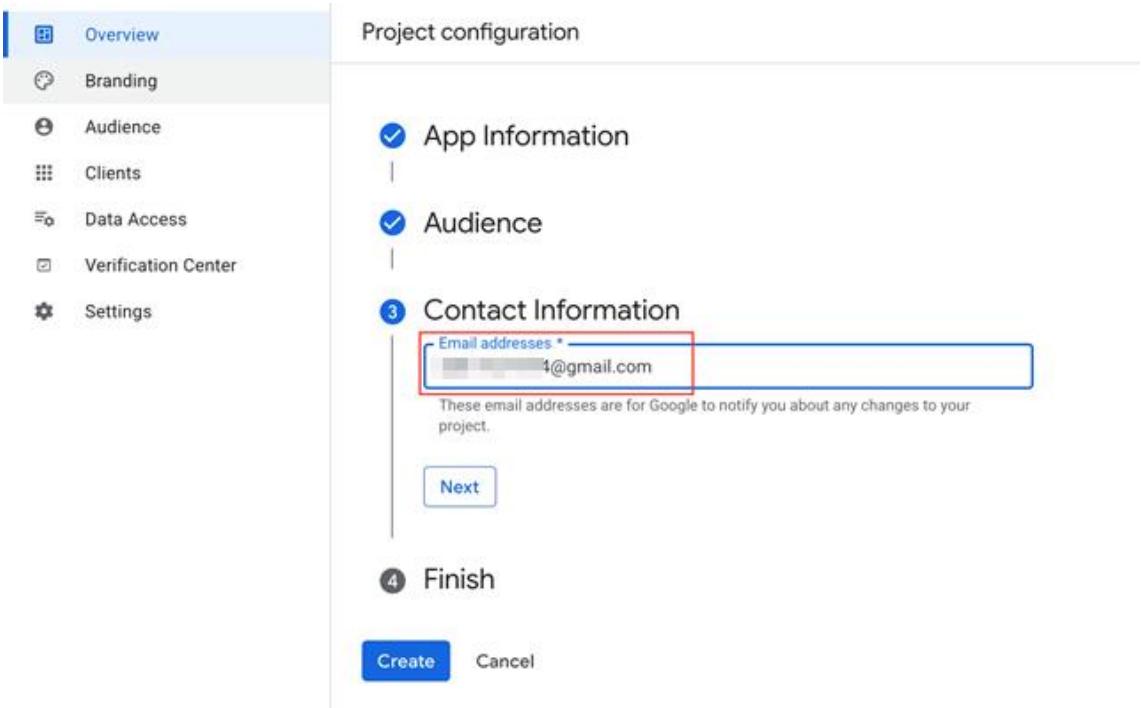


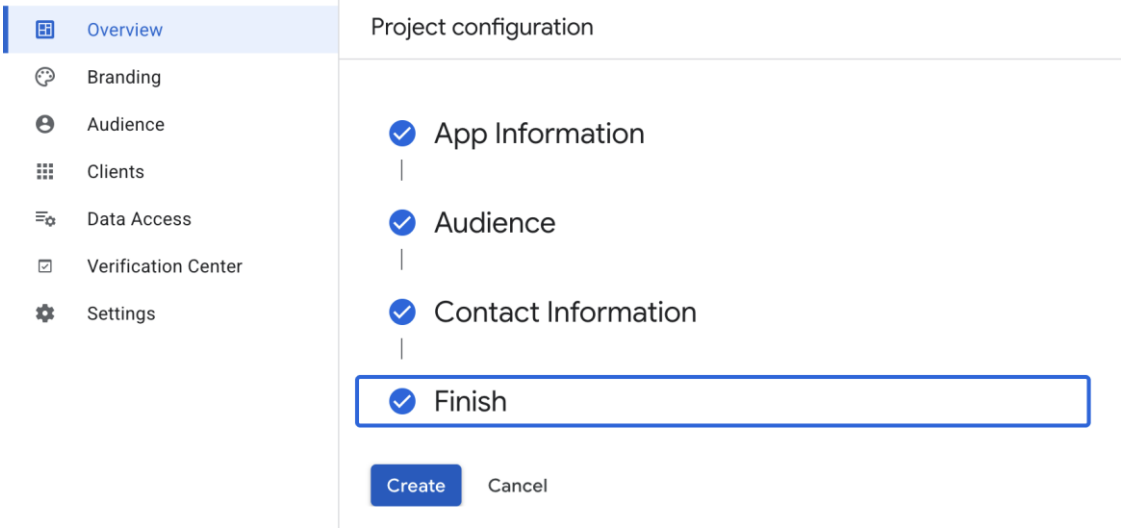
The Audience is set to Internal to restrict API access exclusively to authorized workshop participants and ensure environment isolation.



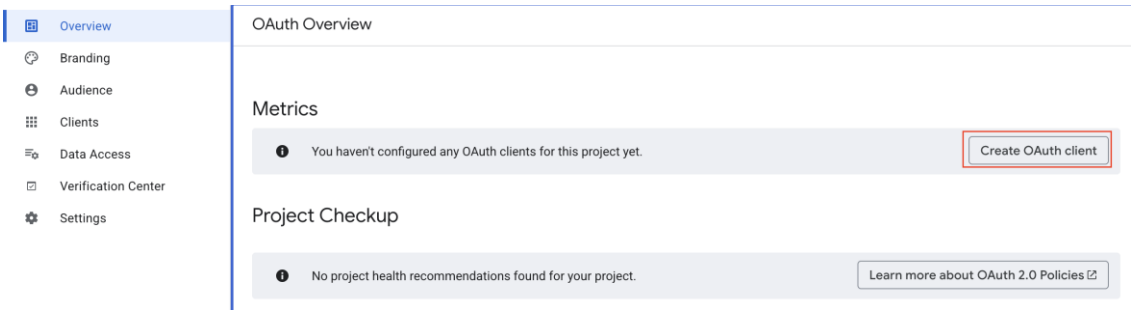
Note: For External Type, to maintain strict access control, you must restrict login permissions under the Audience > Test Users section. Only Google accounts manually added to this whitelist will be authorized to access the application.

Enter Contact Information and Create.

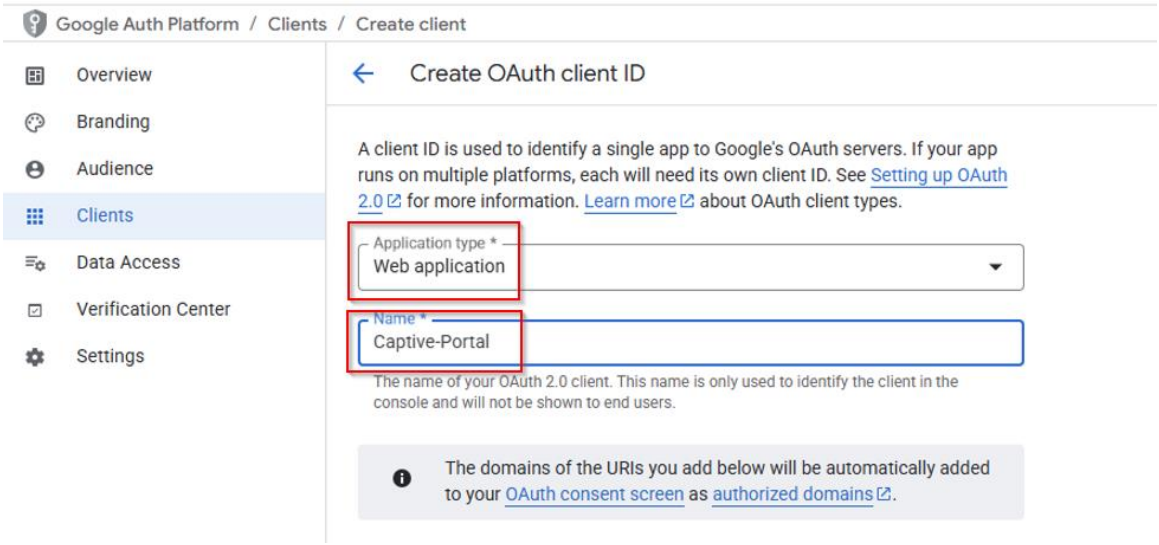




Continue with the setup wizard to create your OAuth client.

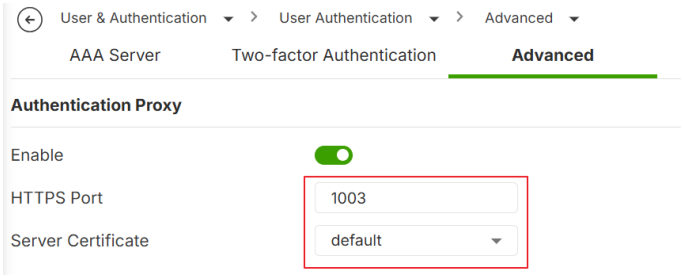


Select Application type as "Web application". Assign a recognizable name to your client.

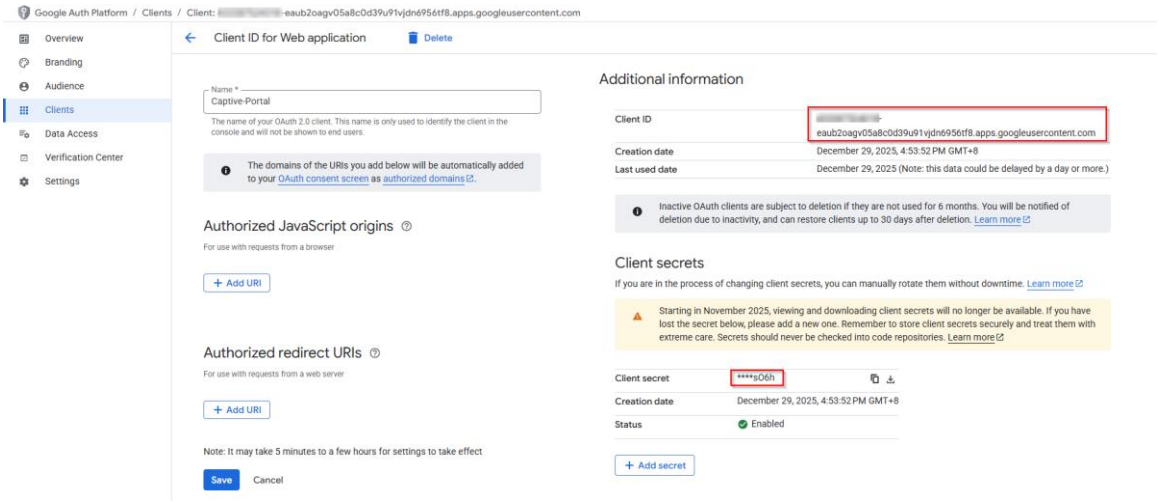


Configure OIDC on USG FLEX H Series

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**



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



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

Fill in Server details

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

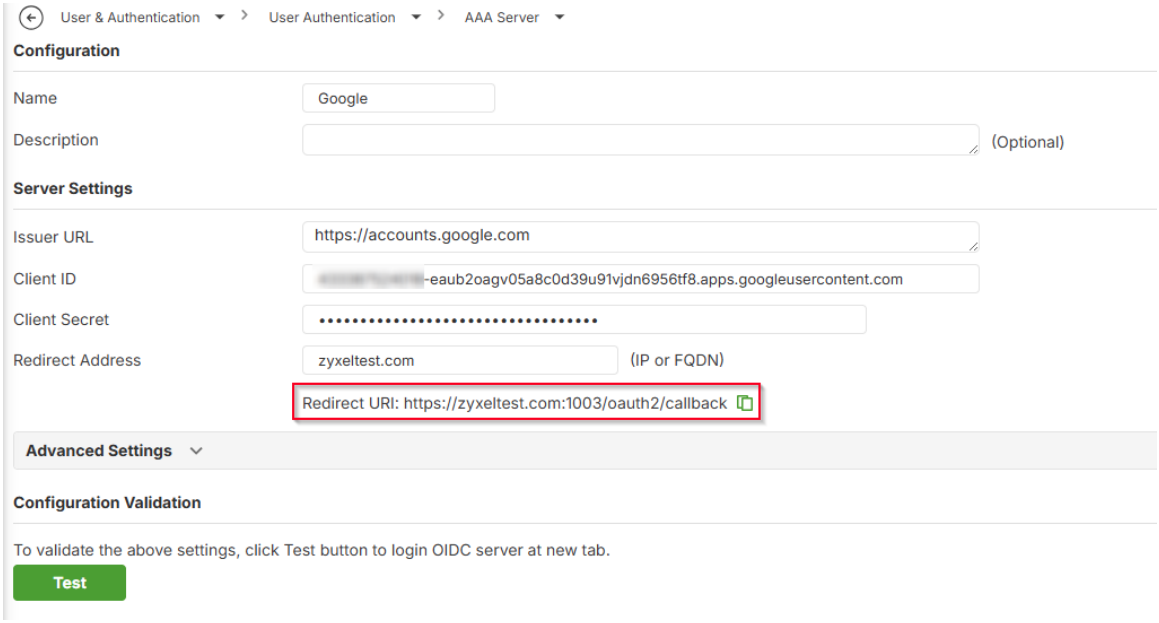
Client ID: {Client ID}

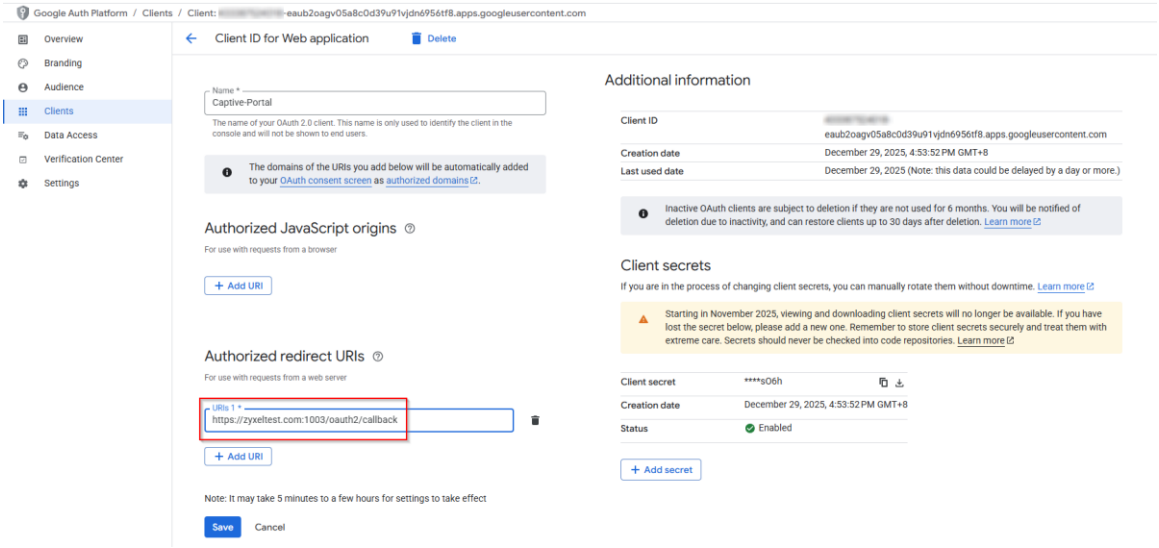
Client Secret: {Client Secret)

Redirect Address: {FQDN}

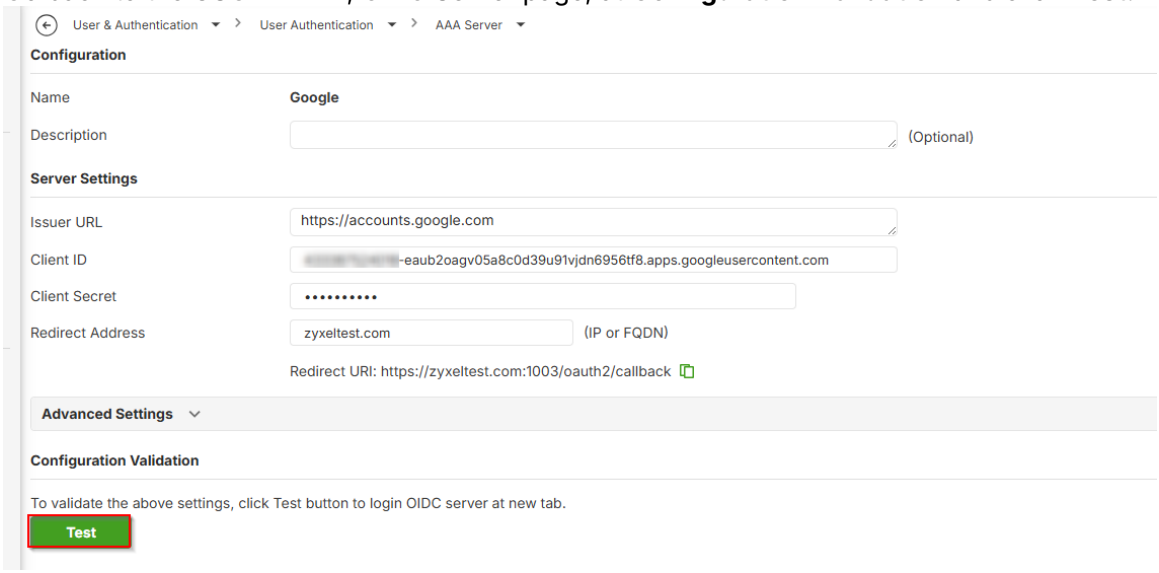
Note: The hostname of the redirect URI should be a FQDN. And the FQDN should match the certificate settings of Authentication proxy on your firewall.

Copy the following “Redirect URL” back to Google Oauth 2.0 Client IDs and paste in Authorized redirect URLs

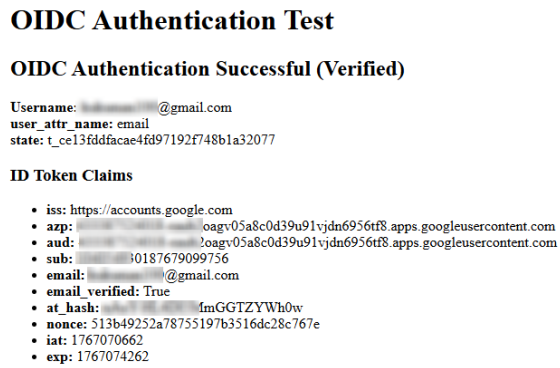




Go back to the USG FLEX H, OIDC Server page, at **Configuration Validation** and click **Test.**



You should see "OIDC Authentication Successful."



OIDC Authentication Test

OIDC Authentication Successful (Verified)

Username: @gmail.com
user_attr_name: email
state: t_ce13fddfacae4fd97192f748b1a32077

ID Token Claims

- **iss:** https://accounts.google.com
- **azp:** oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- **aud:** oagv05a8c0d39u91vjdn6956tf8.apps.googleusercontent.com
- **sub:** 0187679099756
- **email:** @gmail.com
- **email_verified:** True
- **at_hash:** fmGGTZYWh0w
- **nonce:** 513b49252a78755197b3516dc28c767e
- **iat:** 1767070662
- **exp:** 1767074262

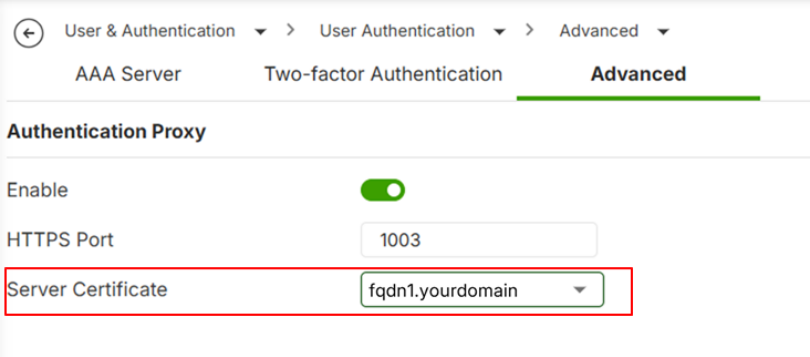
Note: The **Advanced Settings** at USG FLEX H GUI are **optional**.

- **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

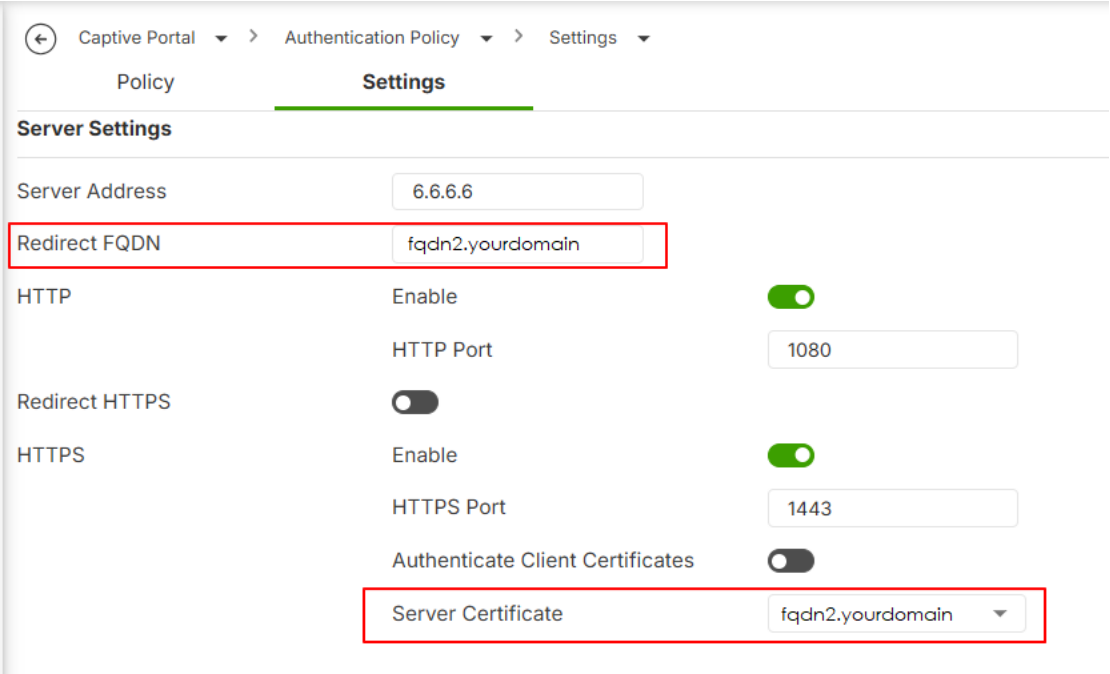
To ensure a smooth and secure Captive Portal authentication experience, proper certificate and DNS preparation is required before configuring OIDC authentication.

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).



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)



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**

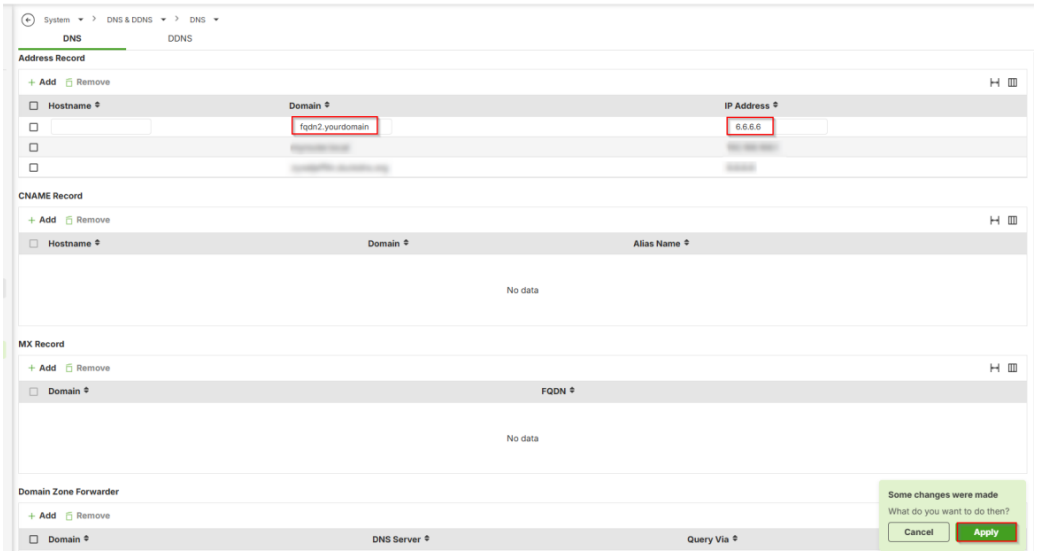
(2). Add an **Address Record**

(3). Leave the Hostname empty

(4). Select or +Add a **Domain** fqdn2.yourdomain

(5). Fill-in **IP address** in 6.6.6.6

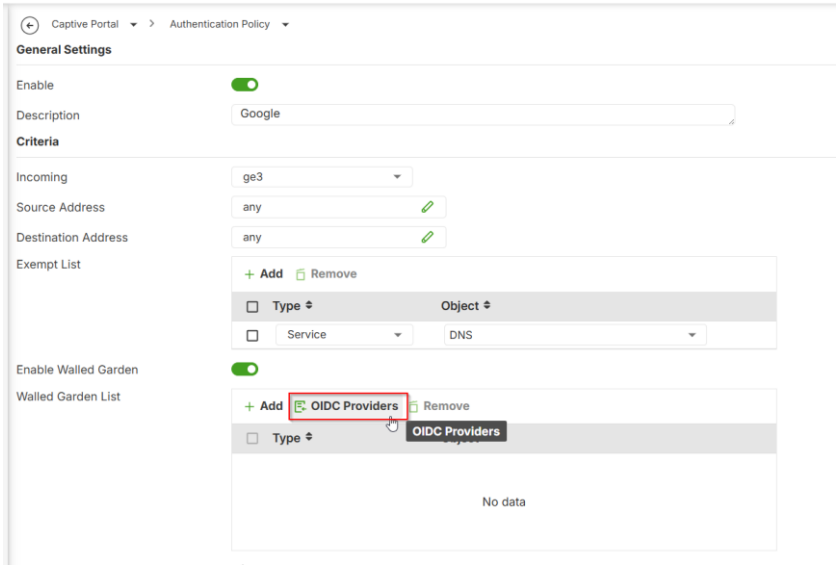
(6). Click **Apply**

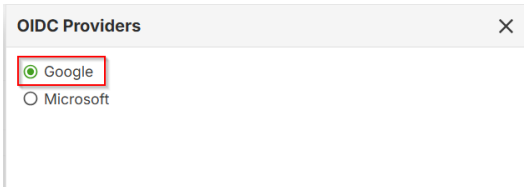


Configure Captive Portal on USG FLEX H Series

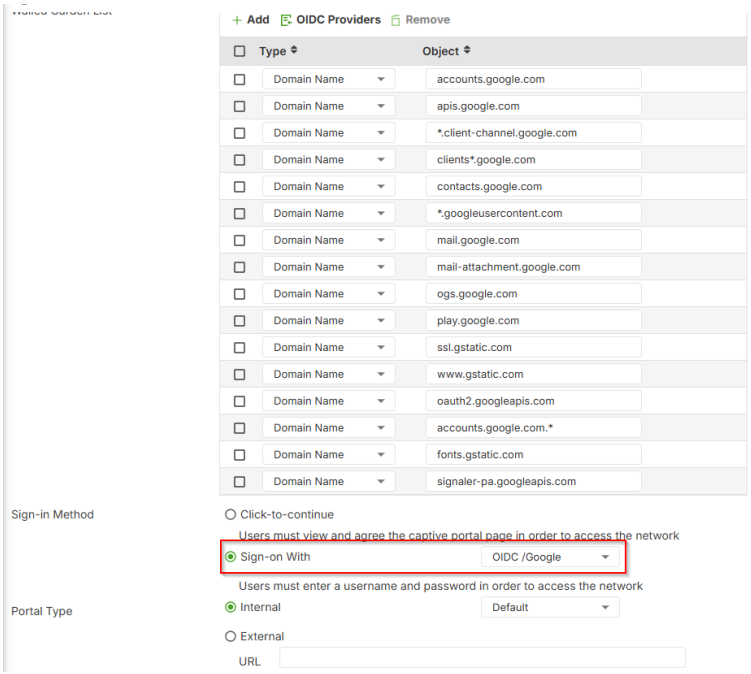
1. Go to **Captive Portal > Authentication Policy > Policy**
2. **Add** a Policy and enable and configure the policy criteria details.
3. In the **Walled Garden List**, click **OIDC Providers** and select **Google**.
4. Select **Sign-on With** > **OIDC** server at **Sign-in Method**.
5. Click **Apply**

Click OIDC Providers and select Google.





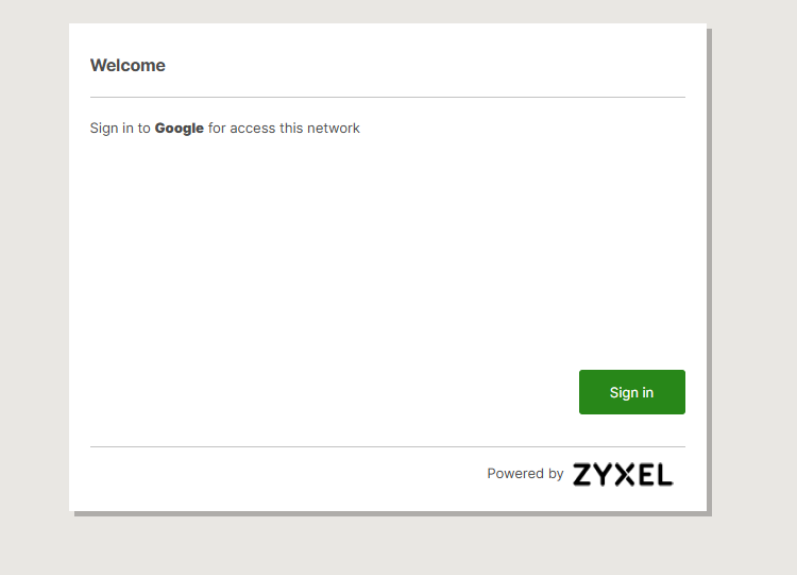
Select Sign-on With > OIDC server at Sign-in Method.



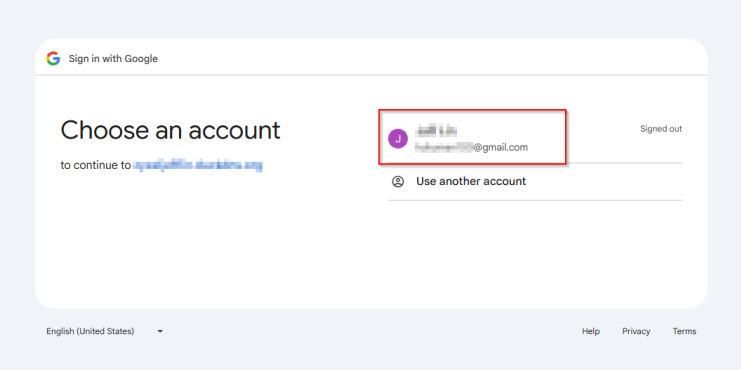
Verification- Test User Login

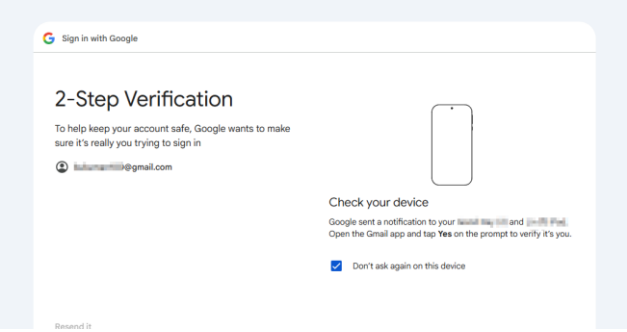
Verify that the Captive Portal correctly redirects unauthenticated users to Google Workspace/Cloud and grants access after successful authentication.

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

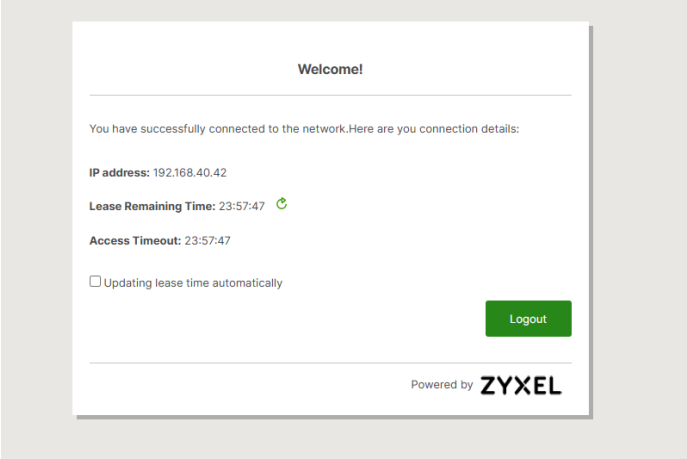


3. Confirm redirect to Google login





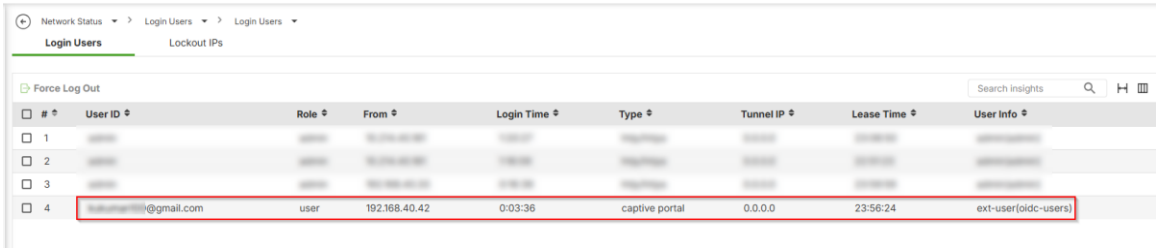
4. Successful Authentication and Access Granted.



Internet access is successful.

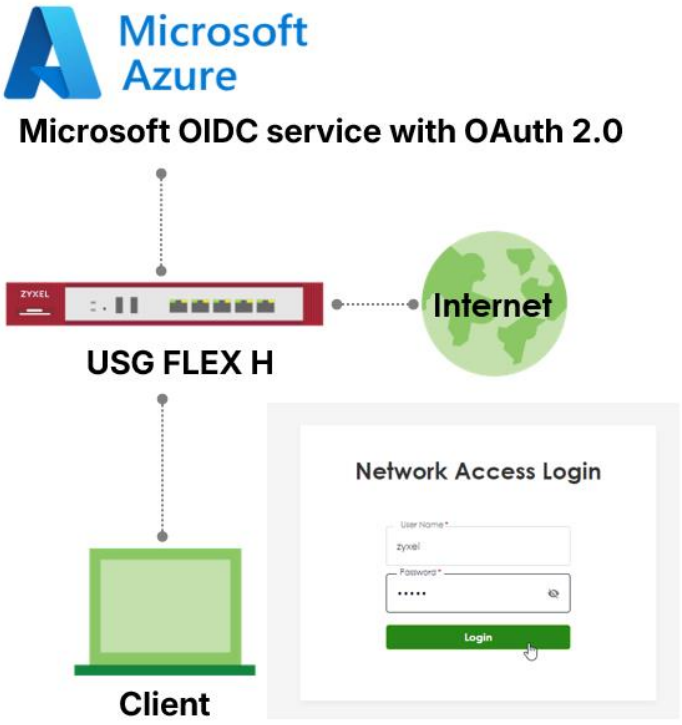
5. Check login user status at **Network Status > Login Users > Login Users**

   User shown as authenticated via OIDC



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:

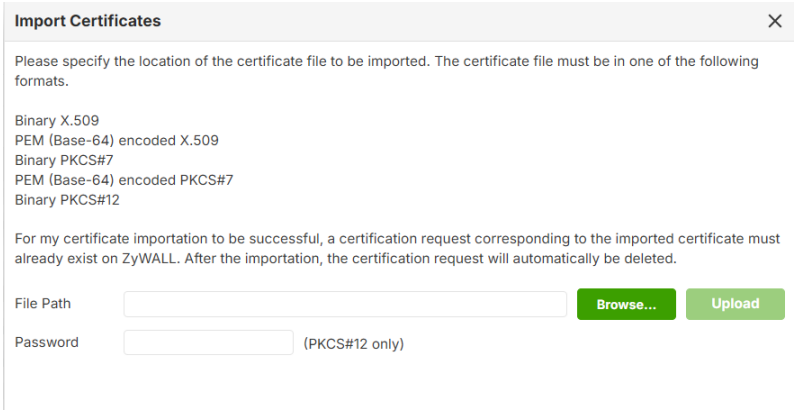
- The **Common Name (CN)** or **Subject Alternative Name (SAN)** must be a **Fully Qualified Domain Name (FQDN)**
- The FQDN must resolve to the **Captive Portal server address**
    - Default Captive Portal address: 6.6.6.6

Example:

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

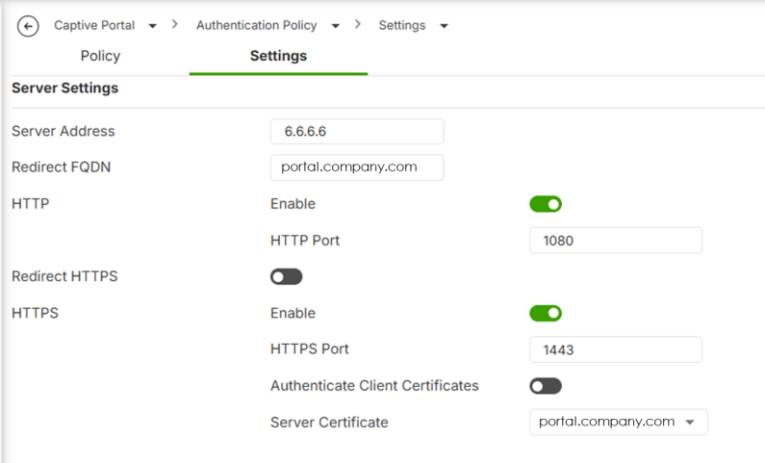
Uploading the Certificate to the USG FLEX H Series

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.



Assigning the Certificate to Captive Portal

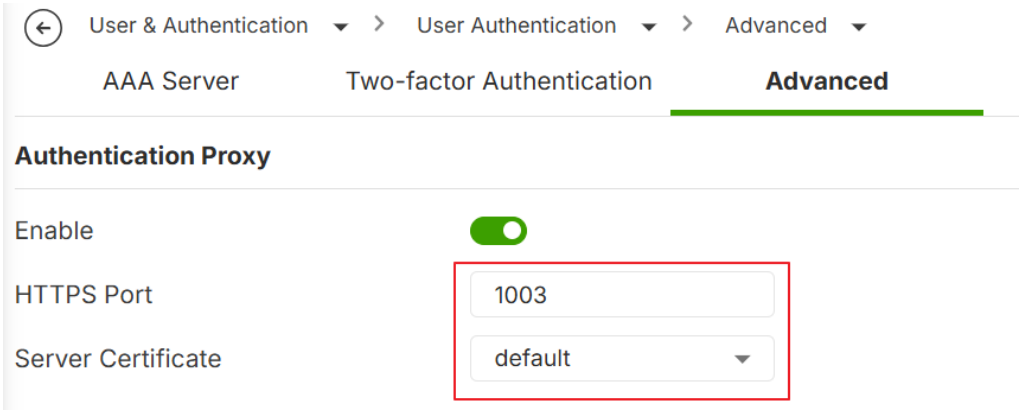
5. Go to **Captive Portal > Authentication Policy > Settings.**
6. Locate the **HTTPS / Server Certificate** settings.
7. Select the imported certificate.
8. Apply the configuration.



Authentication Proxy

Navigate to User & Authentication > User Authentication > Advanced.

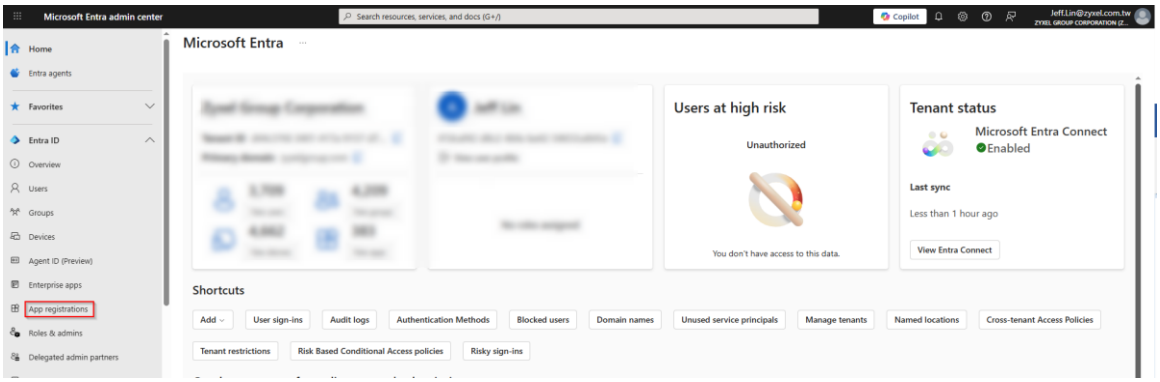
To prevent certificate warnings during the authentication, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve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



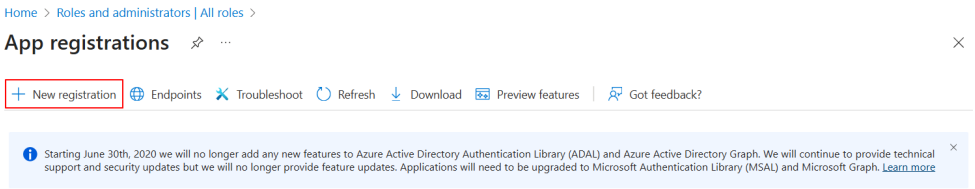
Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

Microsoft Entra ID

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



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

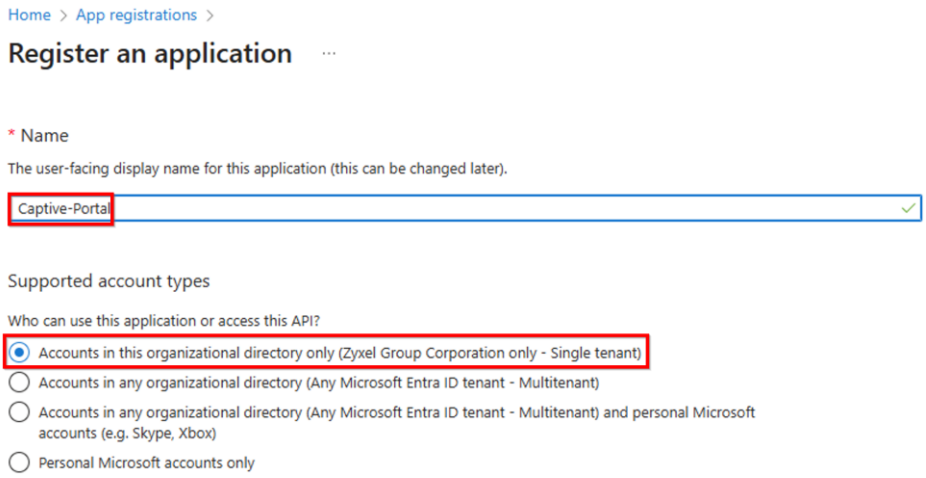


On the Register an application page, provide the following information:

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

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

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



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

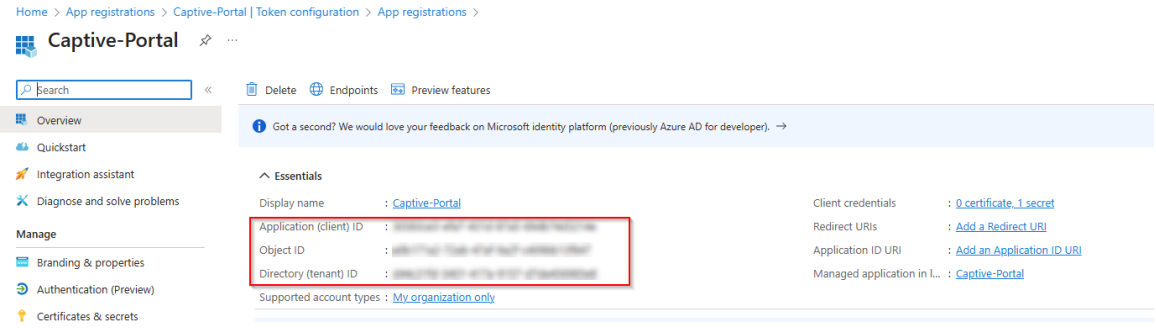
   You don't need to specify a URL in the next field.

2. Click **Register.**

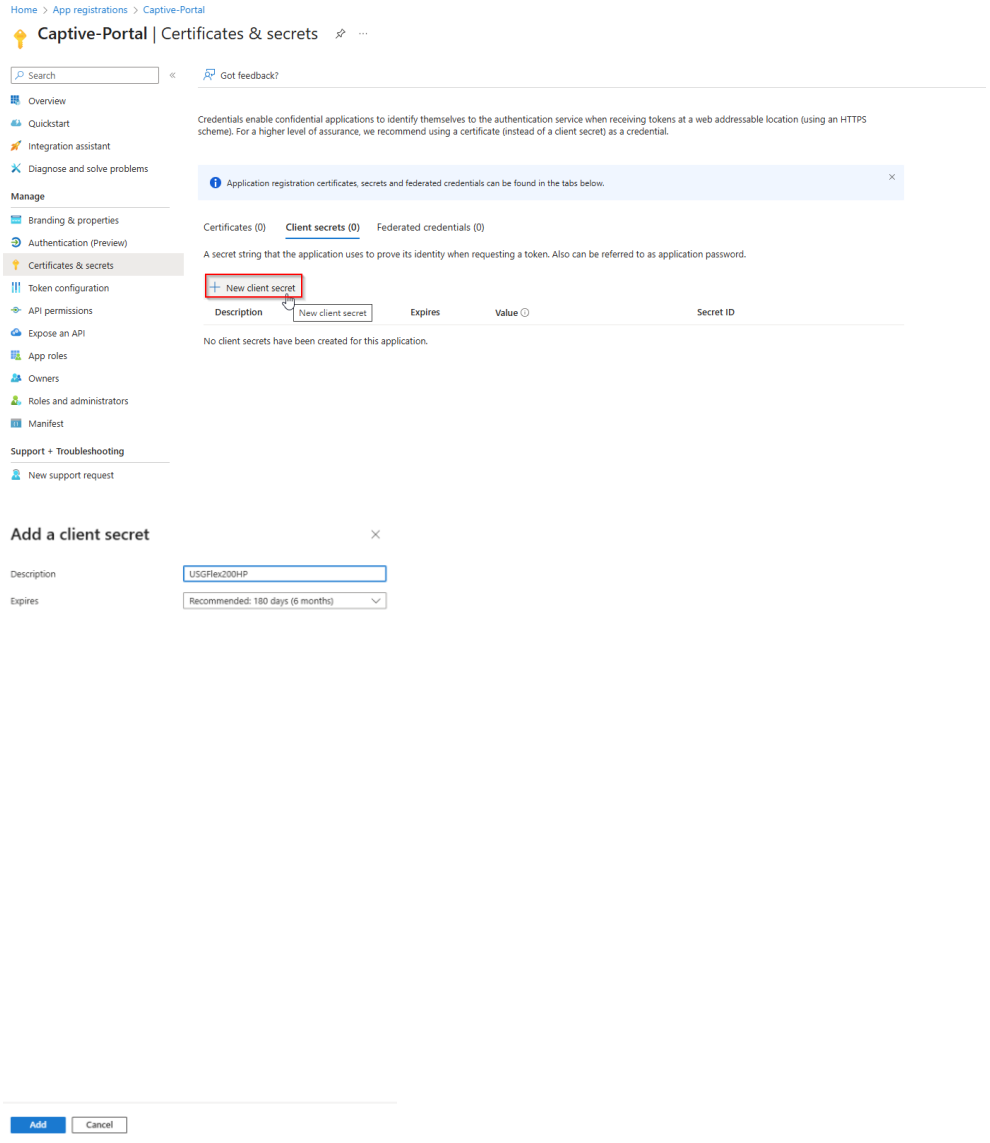
   Microsoft Entra Portal shows the details of the application you created.

3. **Note** the following details:
   - **Application (client) ID**
   - **Directory (tenant) ID**

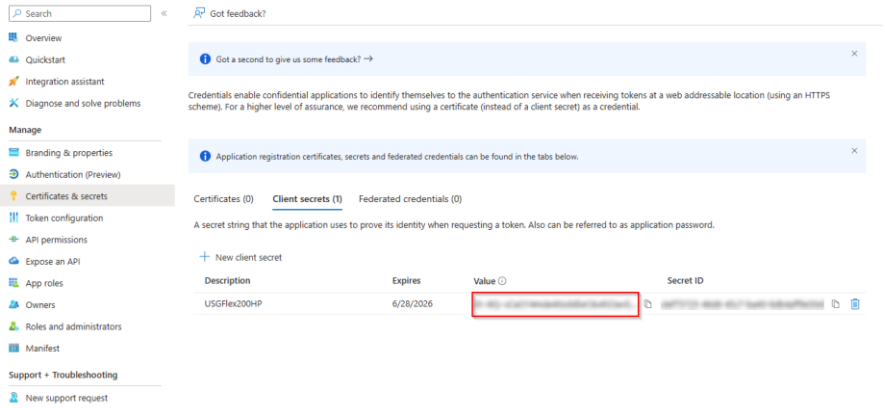
You must enter these details when adding a Microsoft Entra ID server to the firewall (USG FLEX H).



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

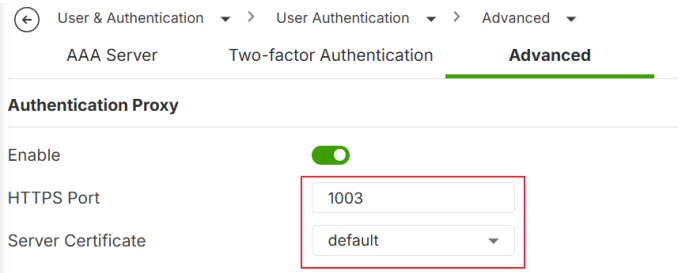


Create a secret and copy the Secret Value immediately. You will need this for the Firewall setup.

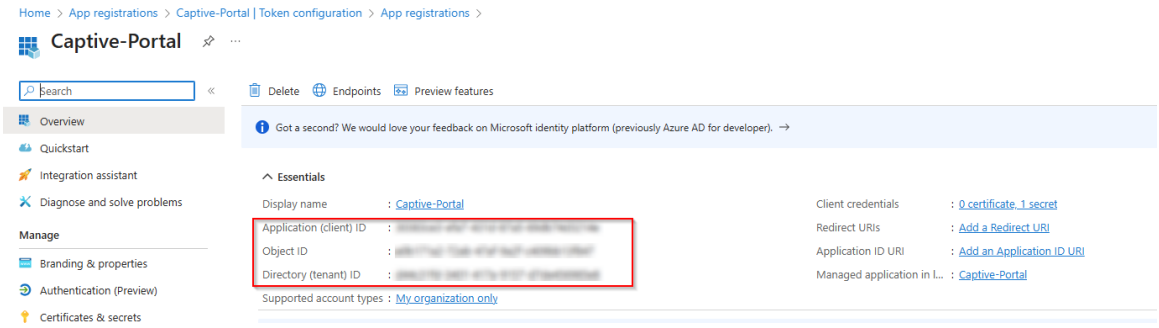


Configure OIDC on USG FLEX H Series

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**



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



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

Fill in Server details

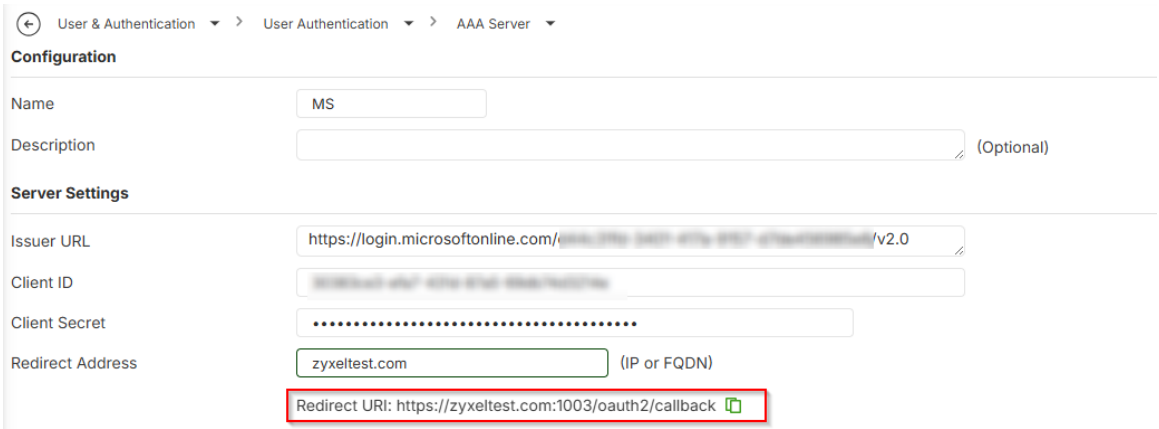
Issuer URL: https://login.microsoftonline.com/{Tenant ID}/v2.0

Client ID: {Client ID}

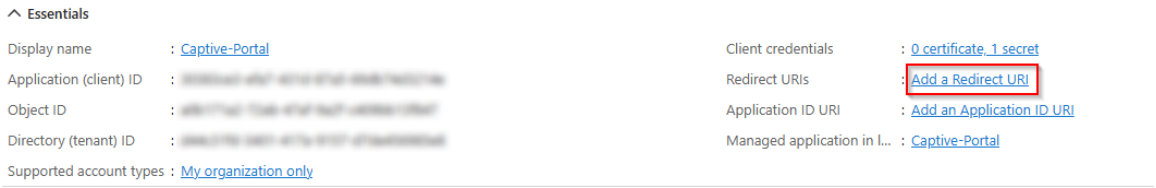
Client Secret: {You already have Secret at “Manage > Certificate & secrets”)

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.

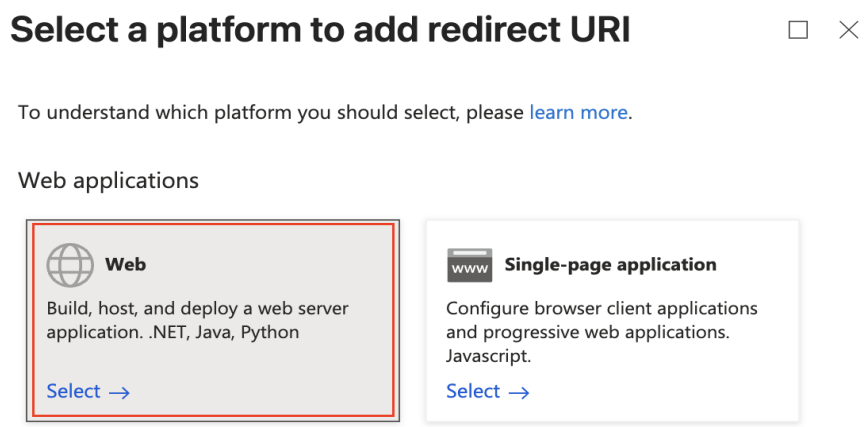


Copy the above “Redirect URL” and back to Entra Portal Overview > Add a Redirect URI > Add a platform > Web. Go to the application you created for the firewall, and under **Essentials > Redirect URIs**, click **Add a Redirect URI**.

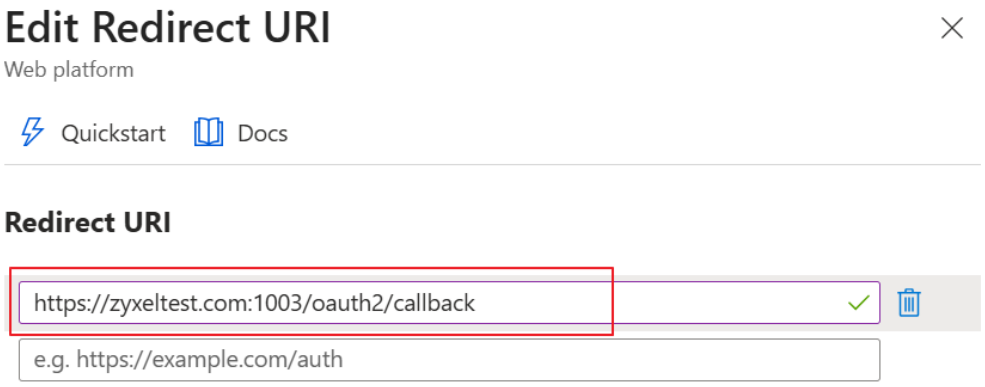


Copy the above “Redirect URL” and back to Entra Portal Overview > Add a Redirect URI > Add a platform.

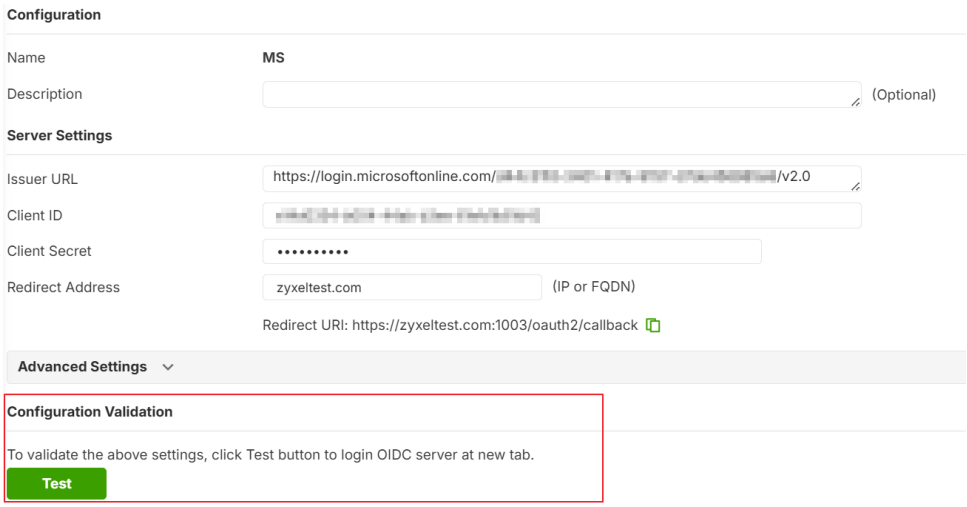
Go to **Add a platform > Web**, in **Redirect URIs**, paste the URL (you copied from USG FLEX H GUI) and click **Configure.**



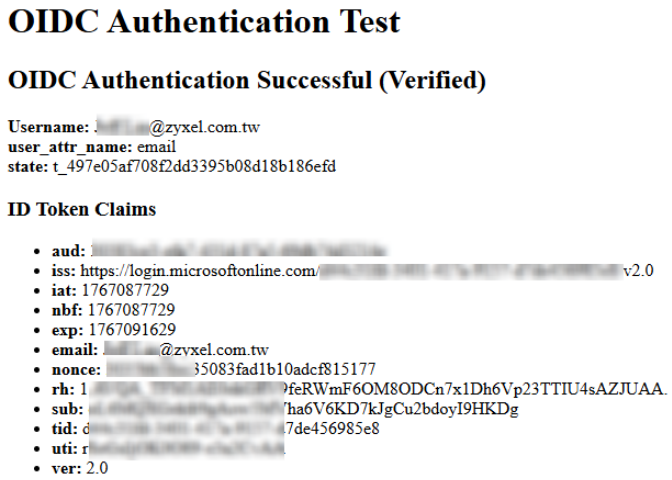
Paste the URL.



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



You should see "OIDC Authentication Successful."



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**.

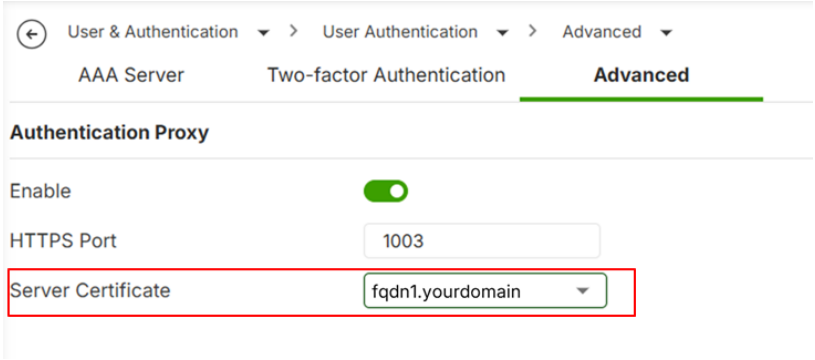
Configure Portal Service Settings on USG FLEX H Series

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).



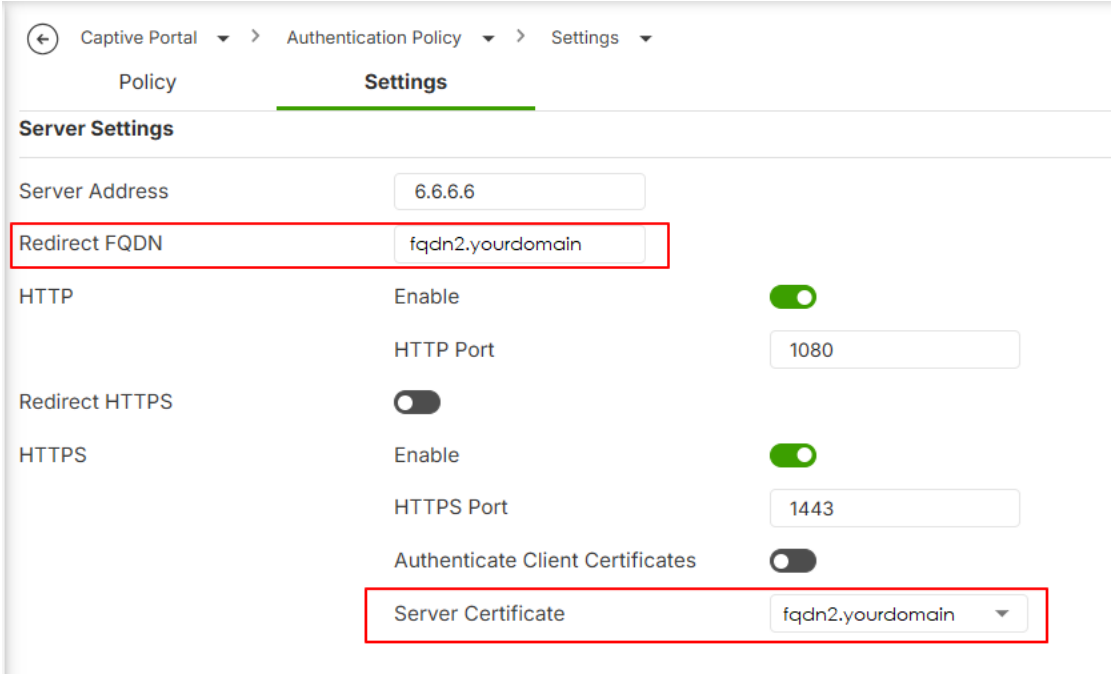
Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

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)



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**

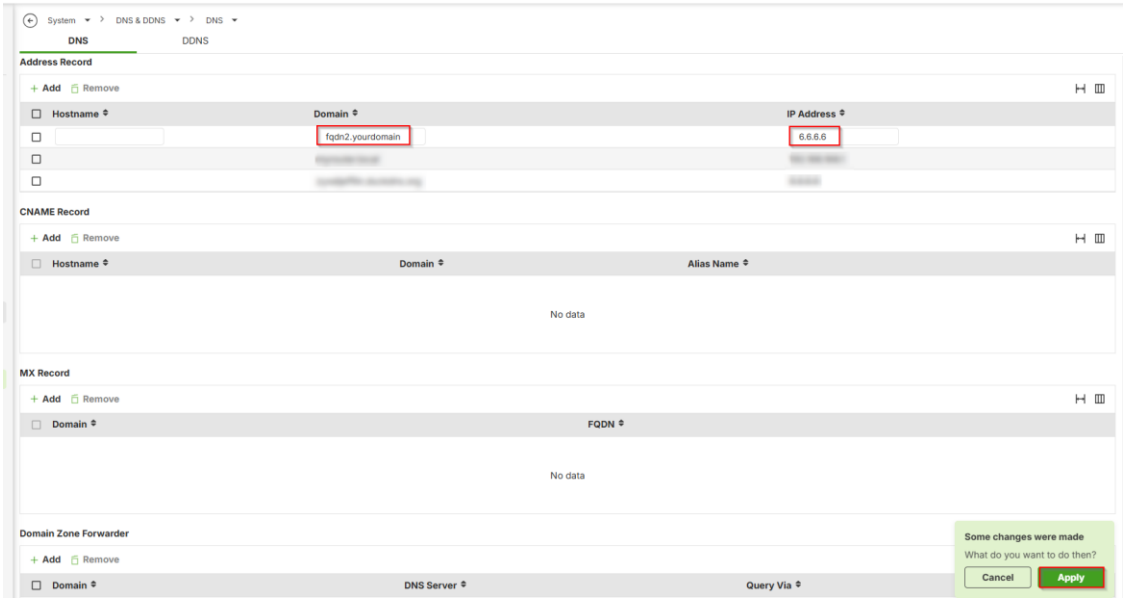
(8). Add an **Address Record**

(9). Leave the Hostname empty

(10). Select or +Add a **Domain** fqdn2.yourdomain

(11). Fill-in **IP address** in 6.6.6.6

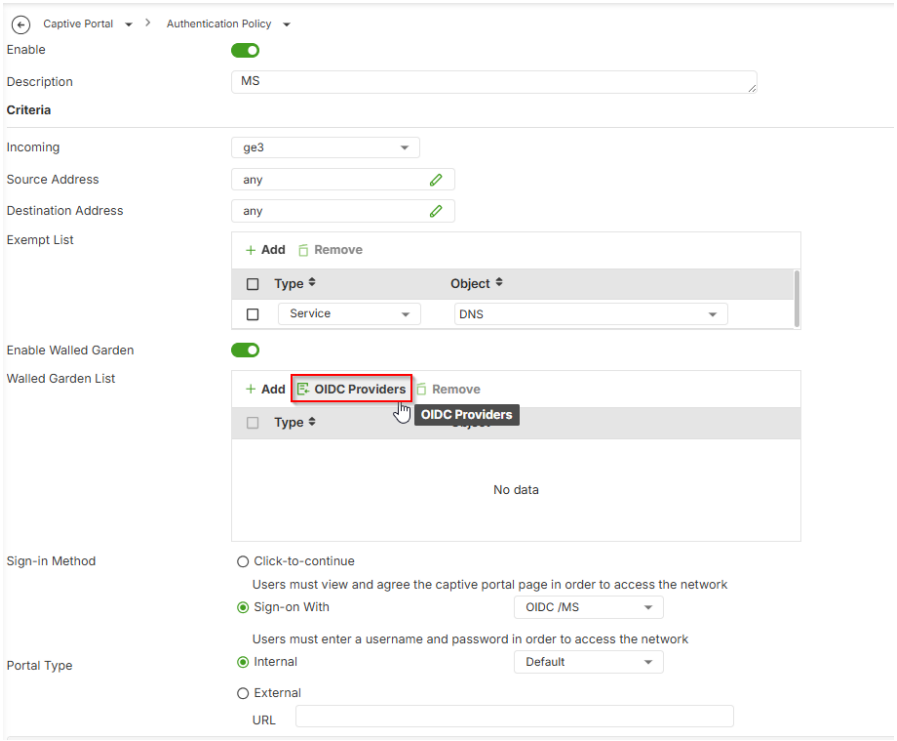
(12). Click **Apply**

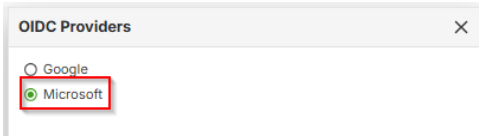


Configure Captive Portal on USG FLEX H Series

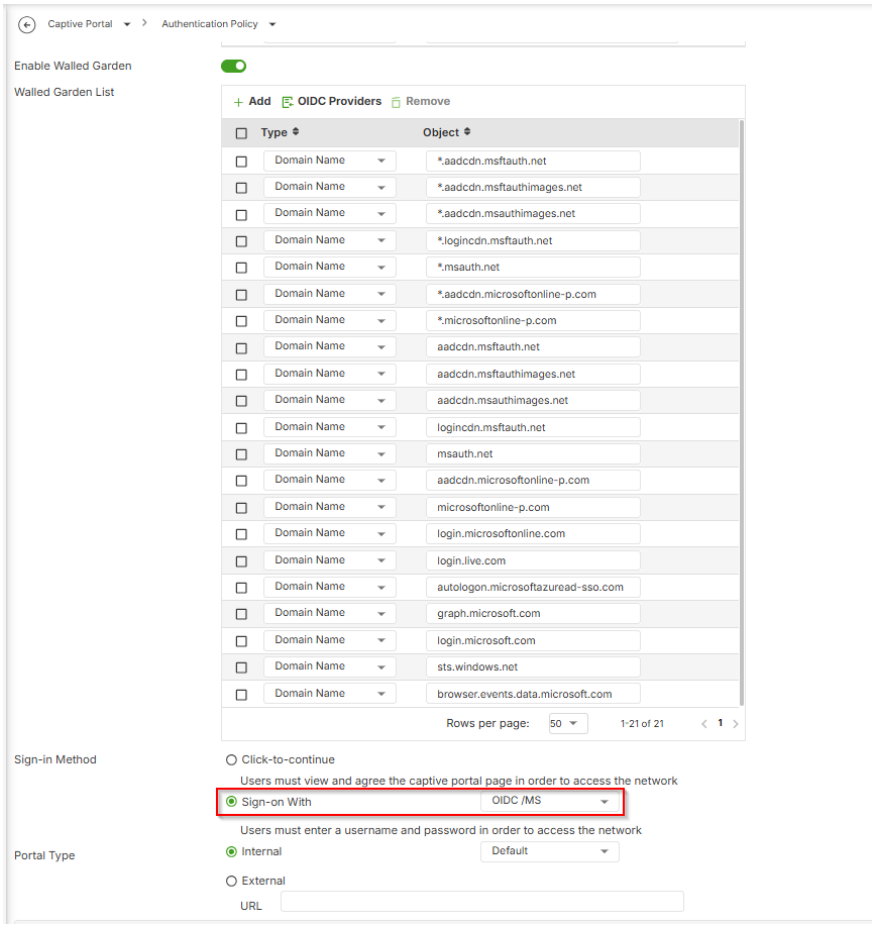
6. Go to **Captive Portal > Authentication Policy > Policy**
7. **Add** a Policy and enable and configure the policy criteria details.
8. In the **Walled Garden List**, click **OIDC Providers** and select **Microsoft**.
9. Select **Sign-on With** > **OIDC** server at **Sign-in Method**.
10. Click **Apply**

Click OIDC Providers and select Microsoft.





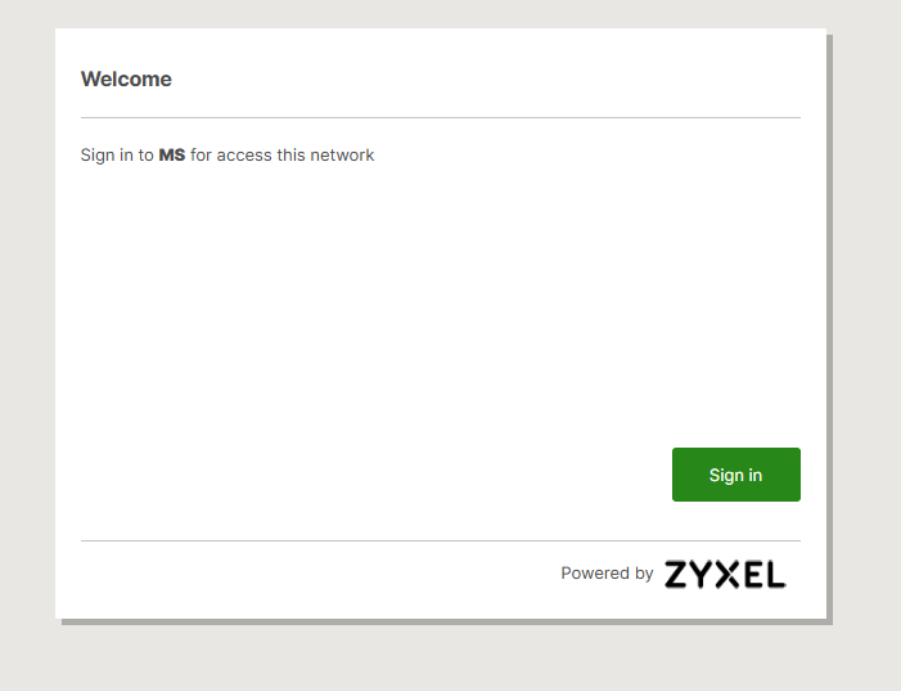
Select Sign-on With > OIDC server at Sign-in Method.



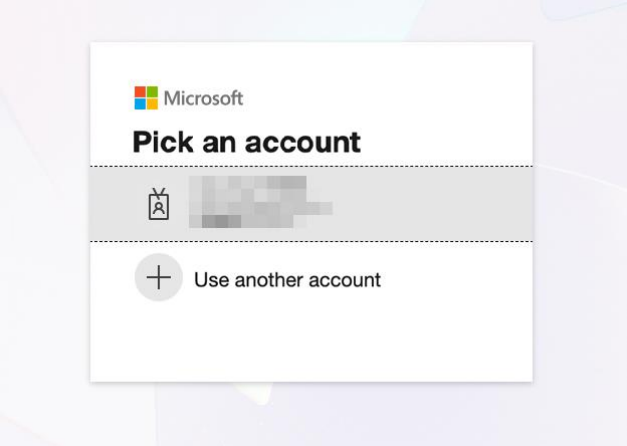
Verification- Test User Login

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

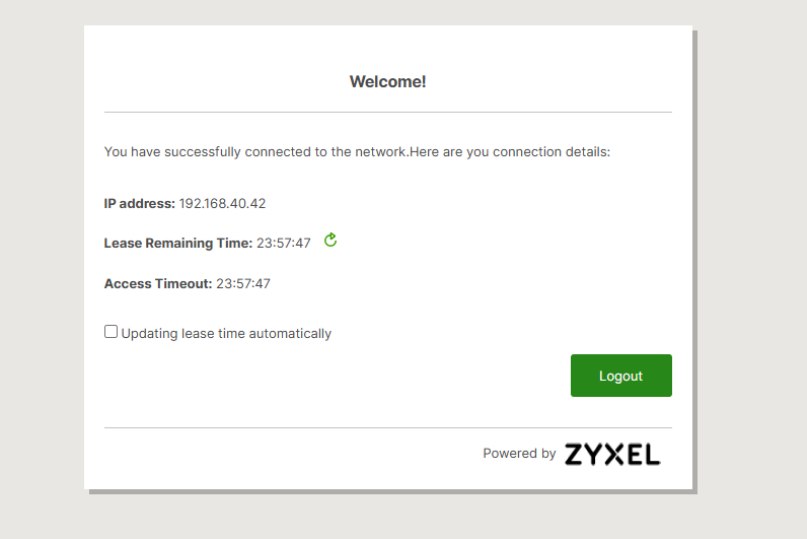
6. Connect a client device
7. Open a browser, display the Captive Portal page, and then click Sign in



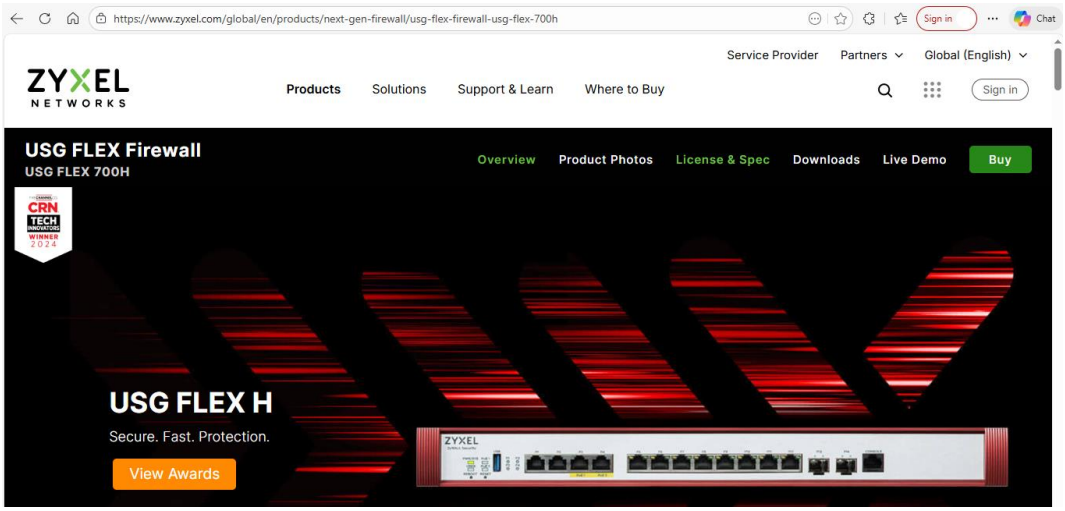
8. Confirm redirect to Microsoft login



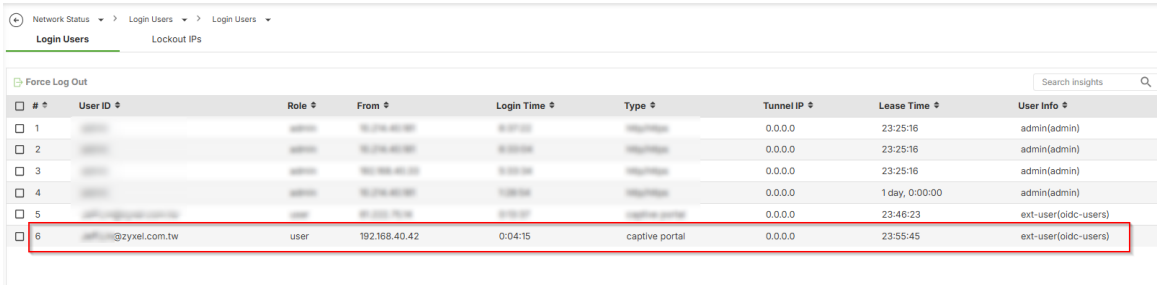
9. Successful Authentication and Access Granted.



Internet access is successful.

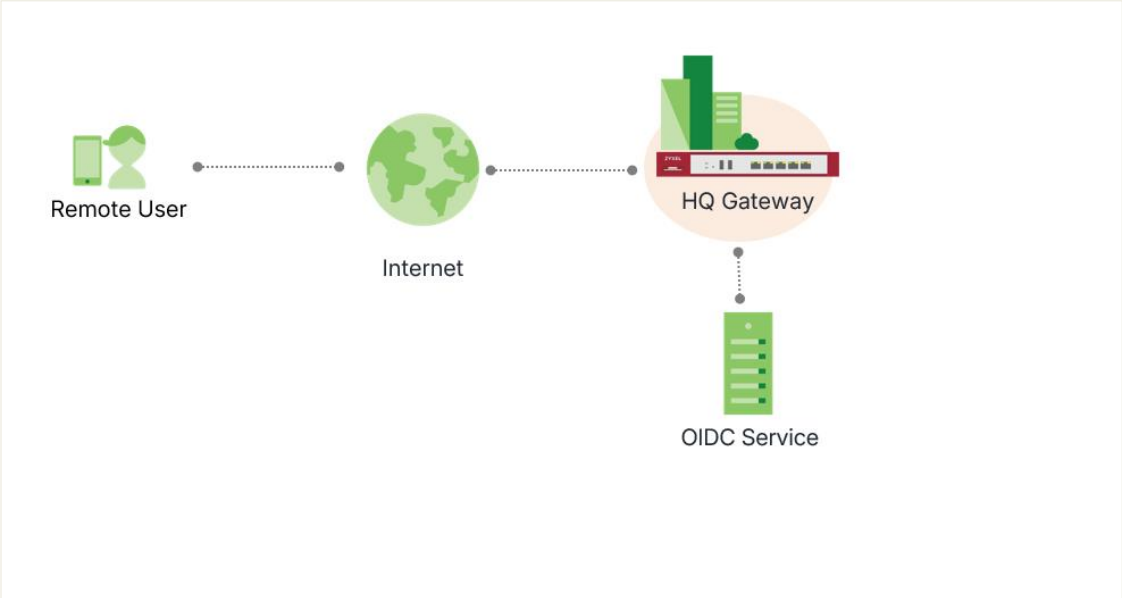


10. Check login user status at **Network Status > Login Users > Login Users.**
    User shown as authenticated via OIDC



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.



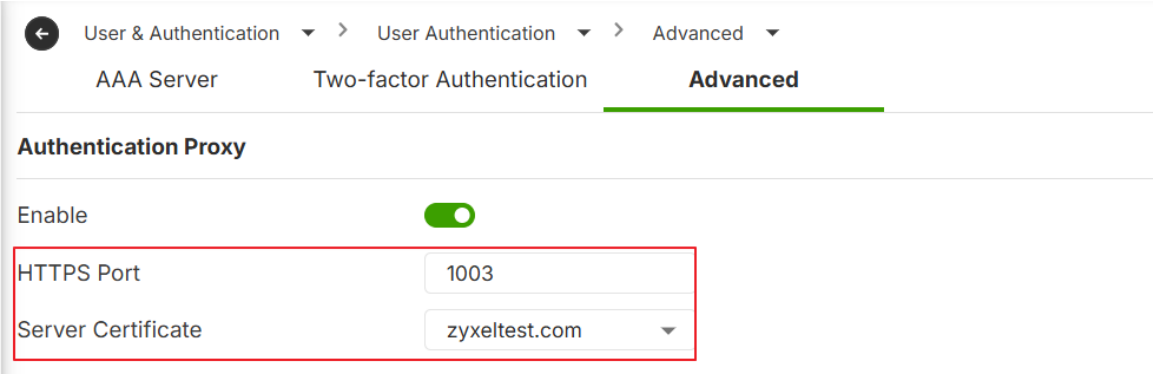
Before You Begin

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

Authentication Proxy

Navigate to User & Authentication > User Authentication > Advanced.

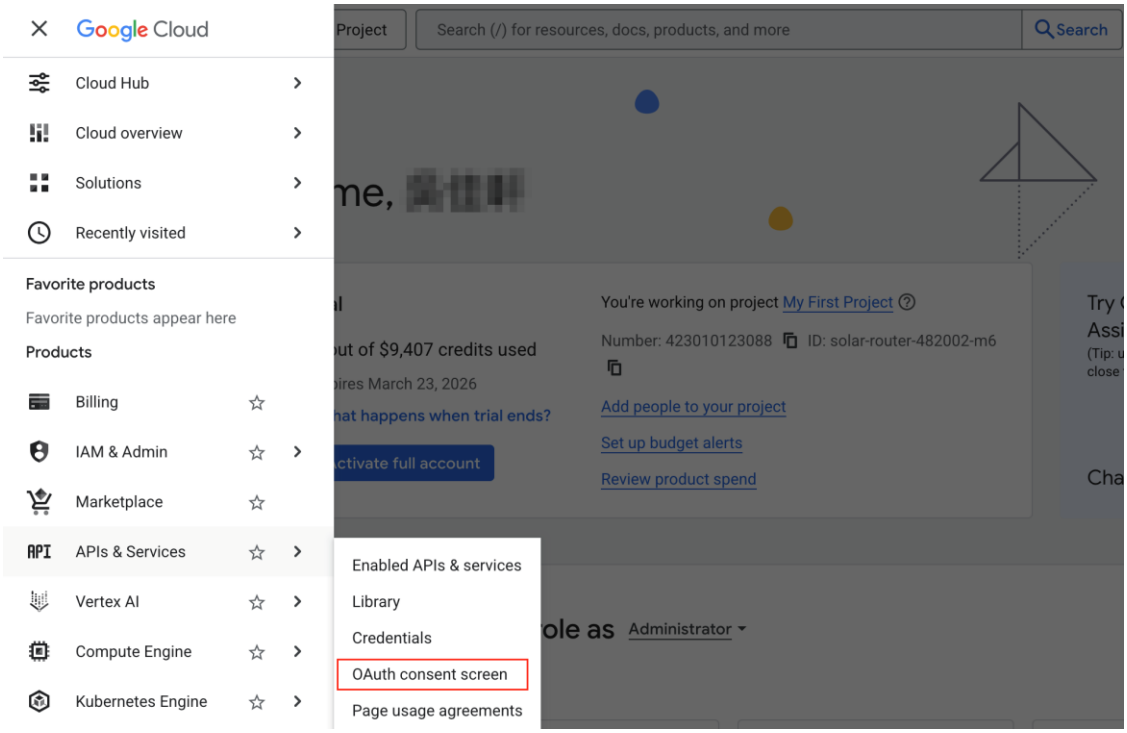
To prevent certificate warnings during the VPN client dial-up, this should be a commercial CA-signed certificate or your internal CA's certificate must be distributed to all client devices. And the Common Name (CN) or SAN (Subject Alternative Name) of the certificate should be a FQDN that can be resolve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



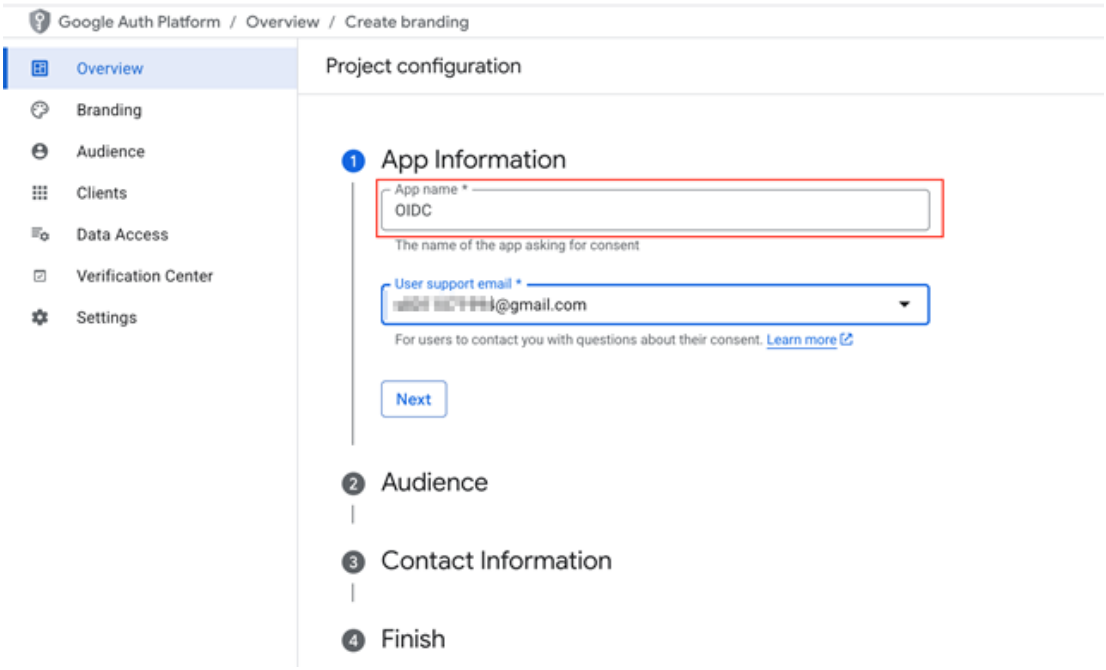
Note: Allow Authentication proxy port (default TCP 1003) at your WAN to ZyWALL secure-policy

Register an APIs & Services in Google

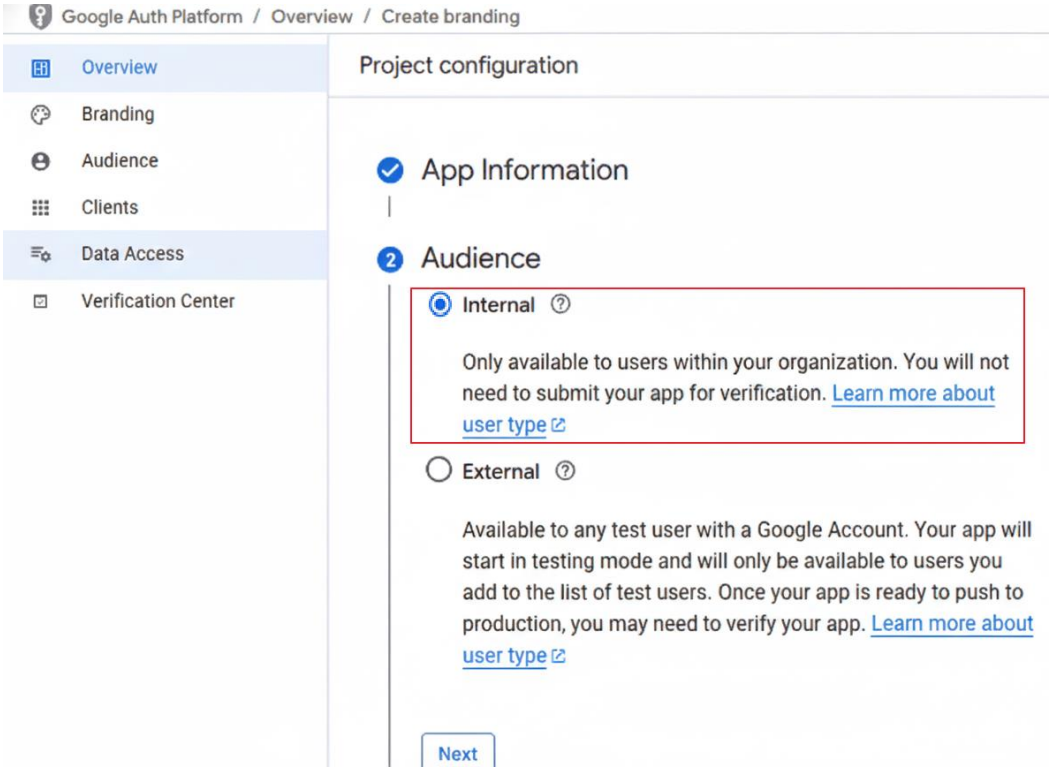
1. Go to Google Cloud Console > APIs & Services > OAuth consent screen



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

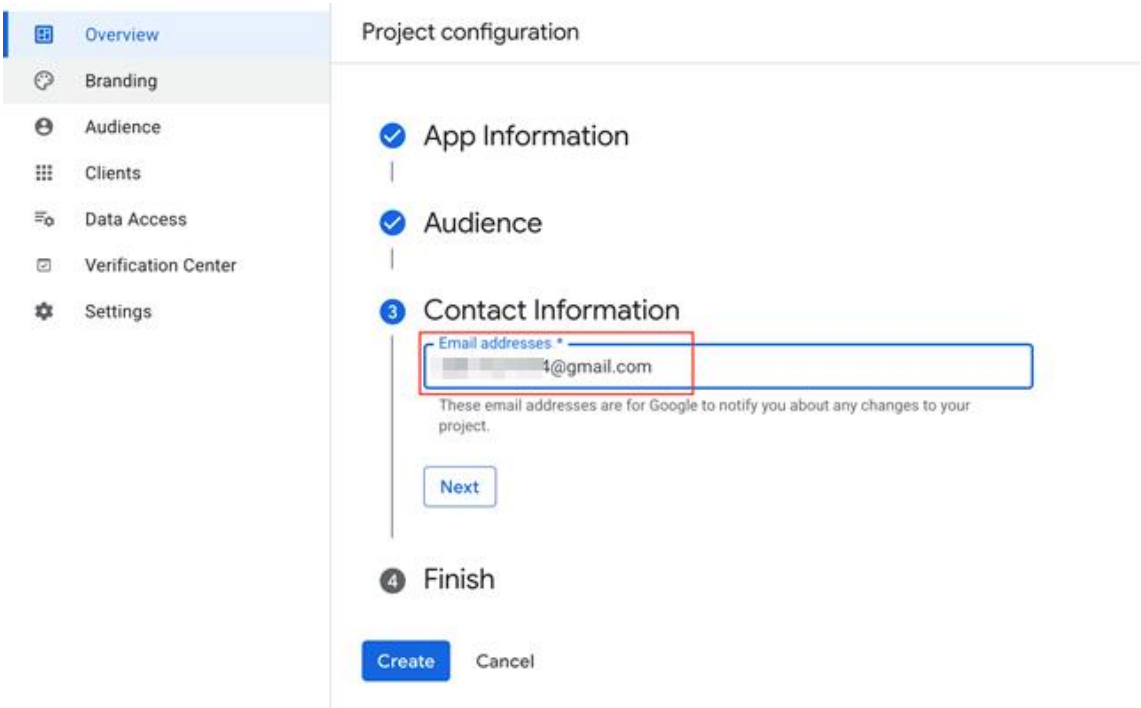


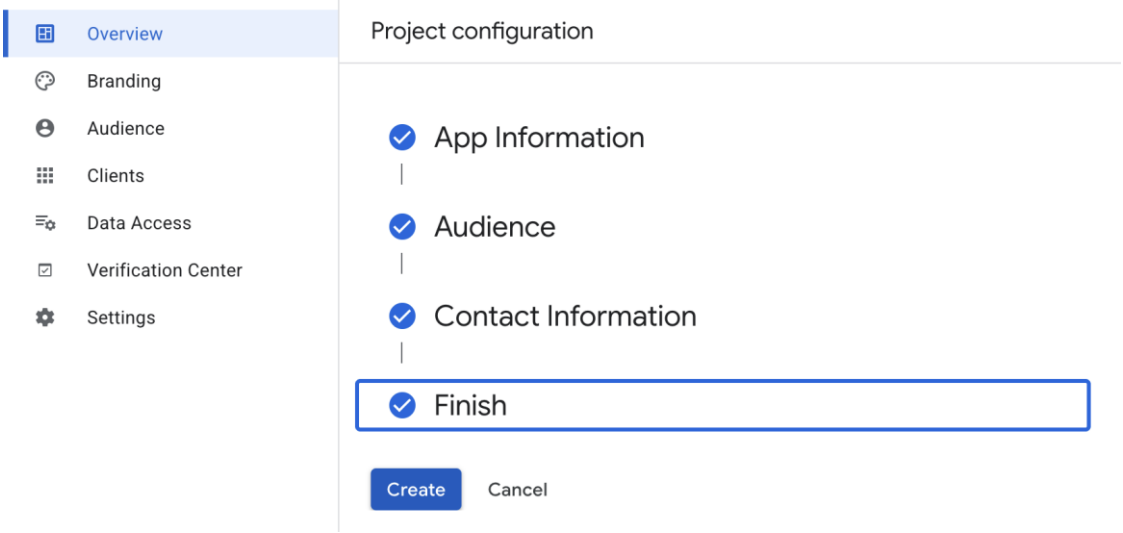
3. The Audience is set to Internal to restrict API access exclusively to authorized workshop participants and ensure environment isolation



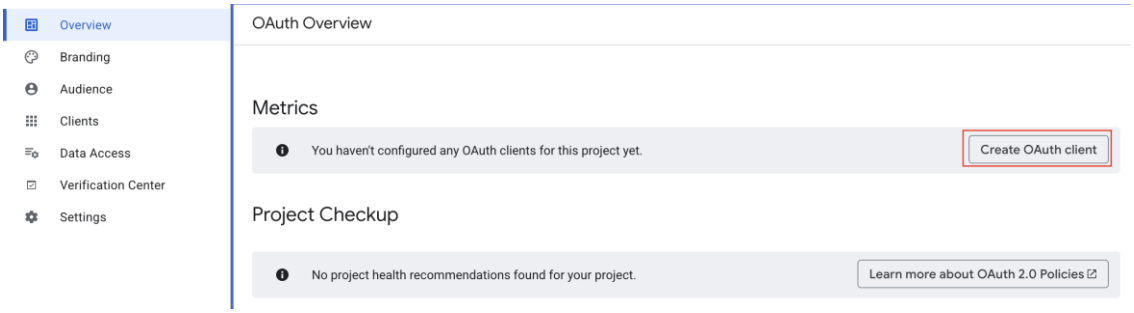
Note: For External Type, to maintain strict access control, you must restrict login permissions under the Audience > Test Users section. Only Google accounts manually added to this whitelist will be authorized to access the application.

4. Enter Contact Information and Create

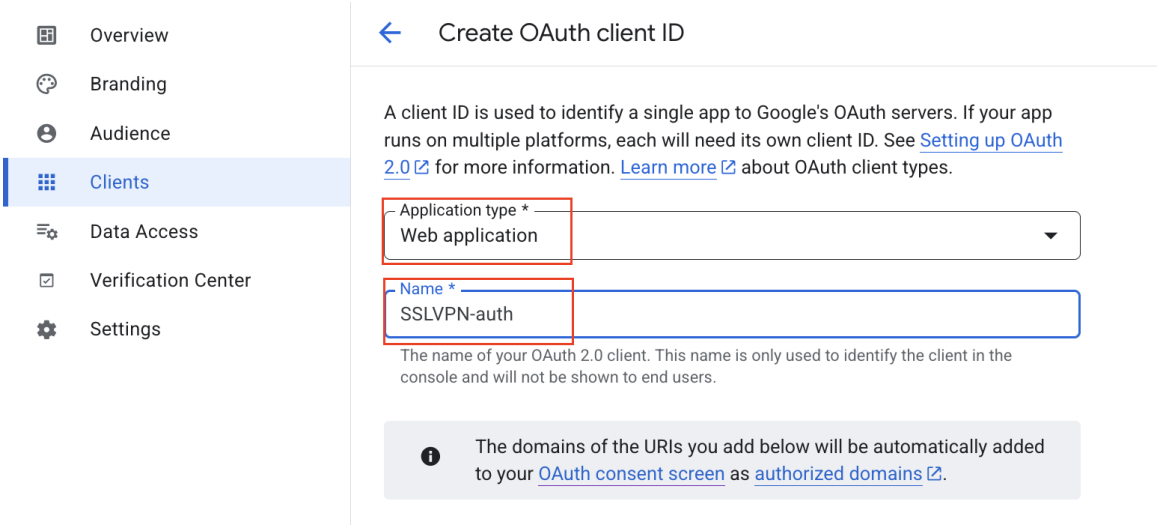




5. Continue with the setup wizard to create your OAuth client



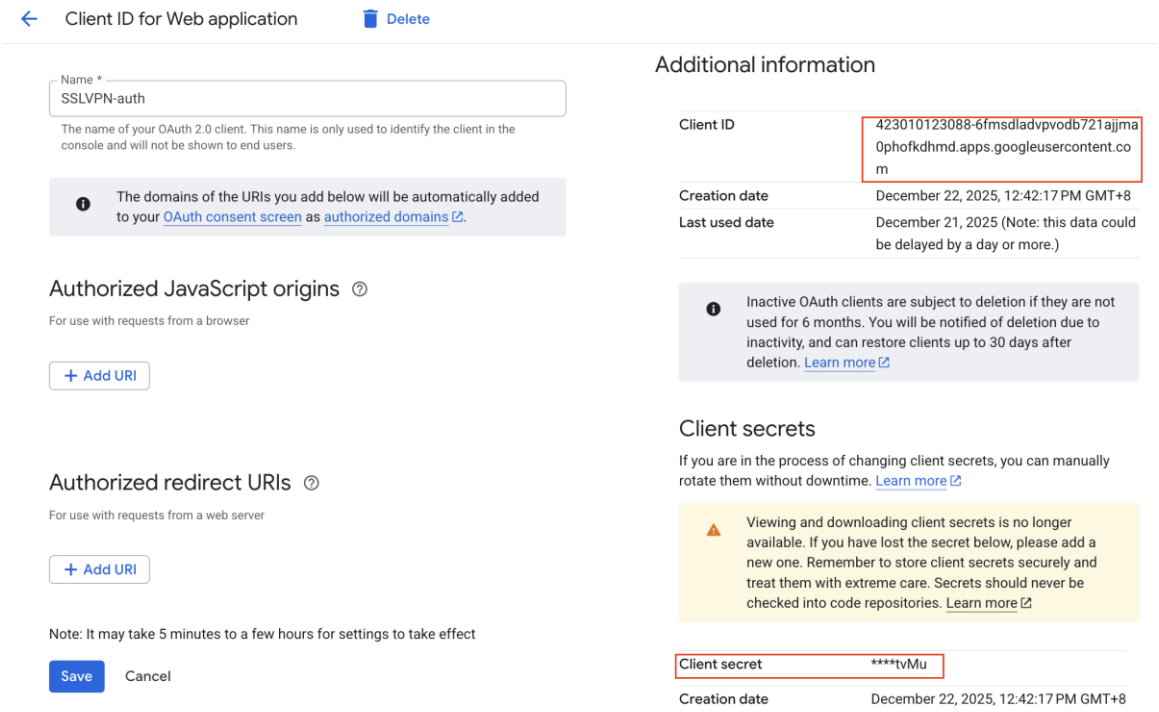
6. Select Application type as "Web application". Assign a recognizable name to your client.



Create OIDC AAA Server

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

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



2. Fill in Server details

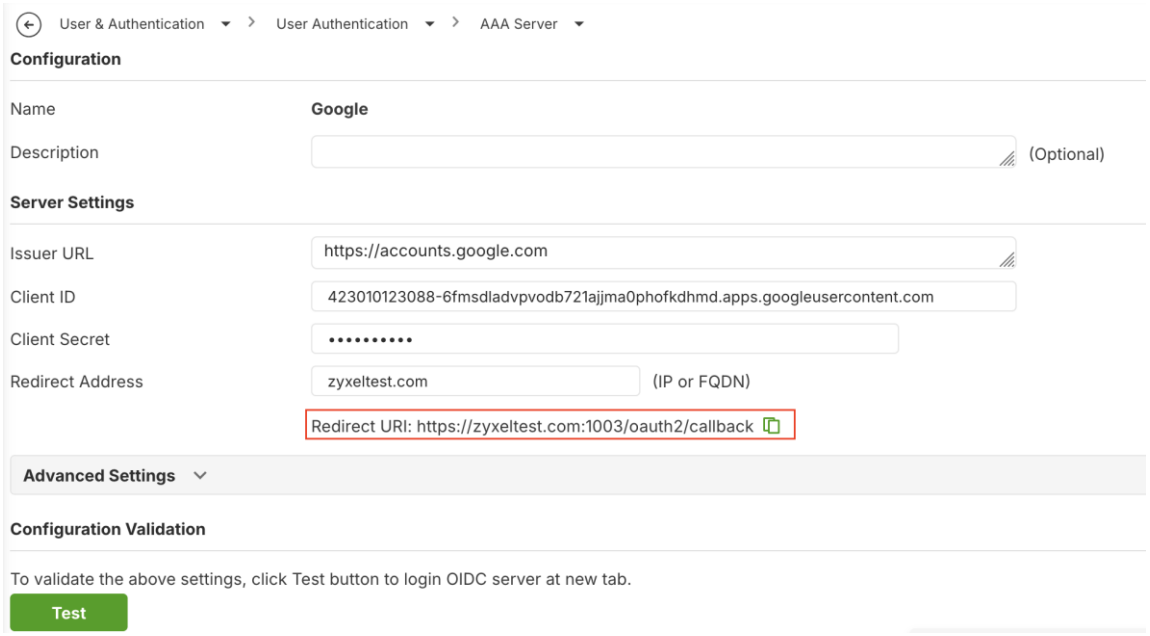
Issuer URL: https://accounts.google.com

Client ID: *{Client ID}*

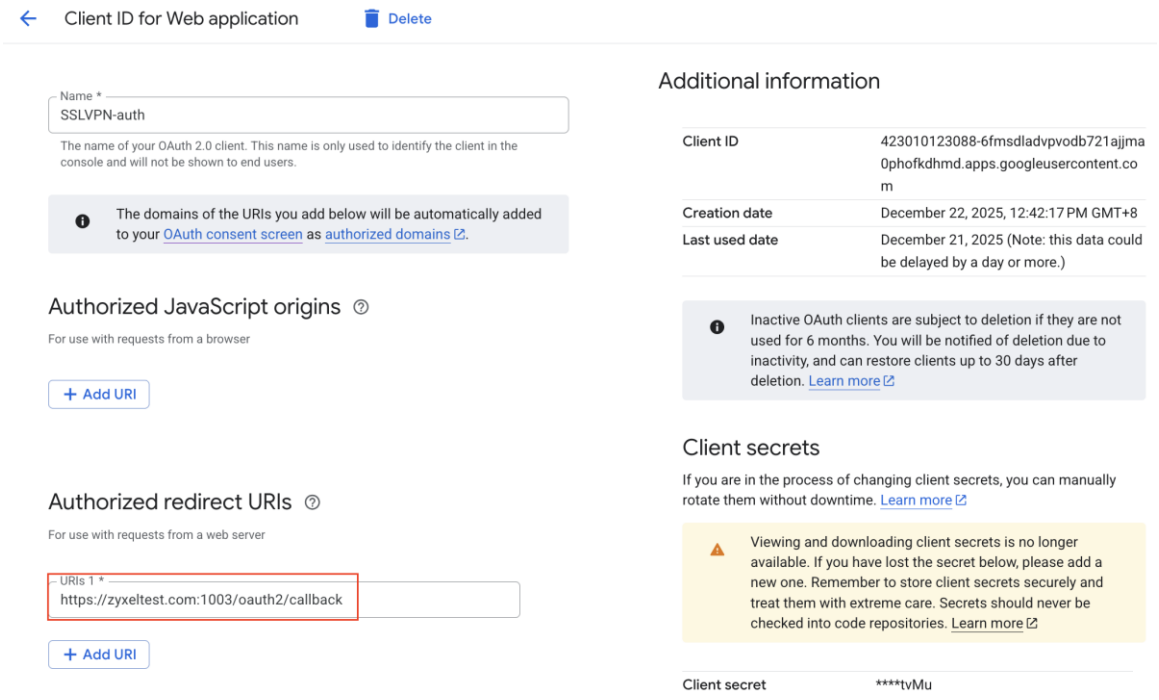
Client Secret: *{Client Secret}*

Redirect Address: *{FQDN}*

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

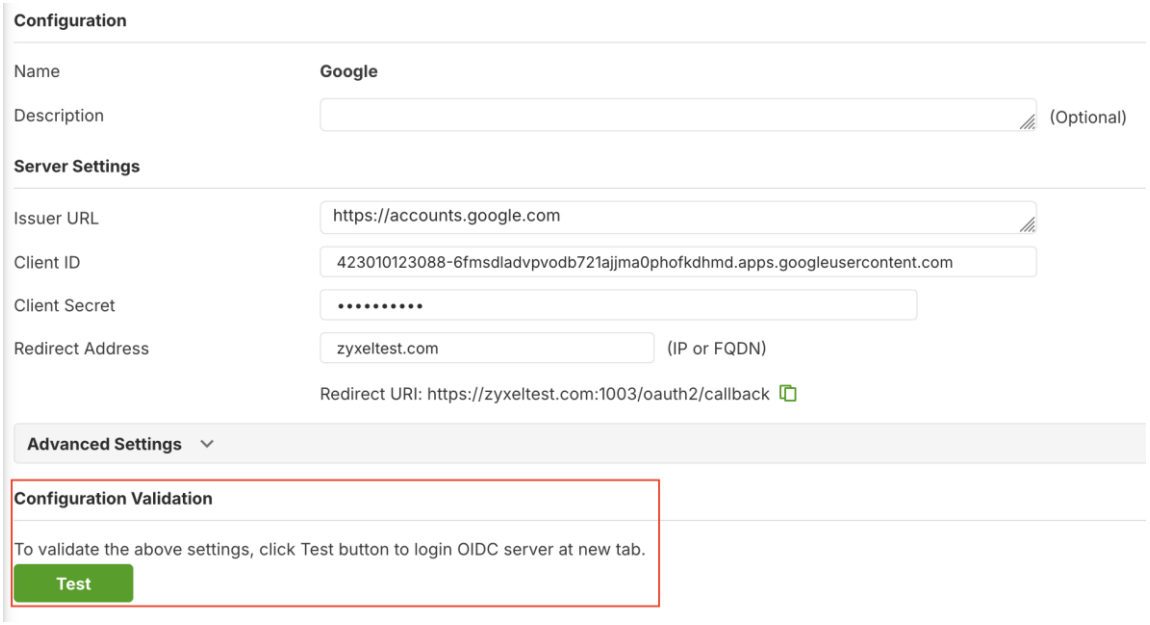


3. Copy the above “Redirect URI” back to Oauth 2.0 Client IDs and paste in Authorized redirect URIs



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

5. Click Test on the Firewall.

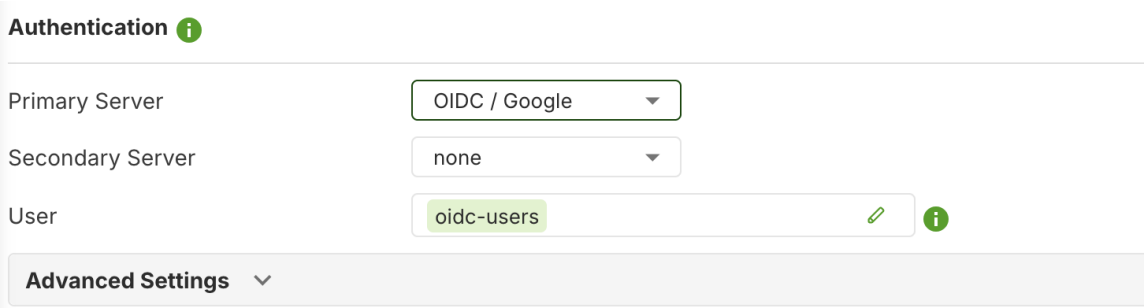


6. You should see "OIDC Authentication Successful."

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.



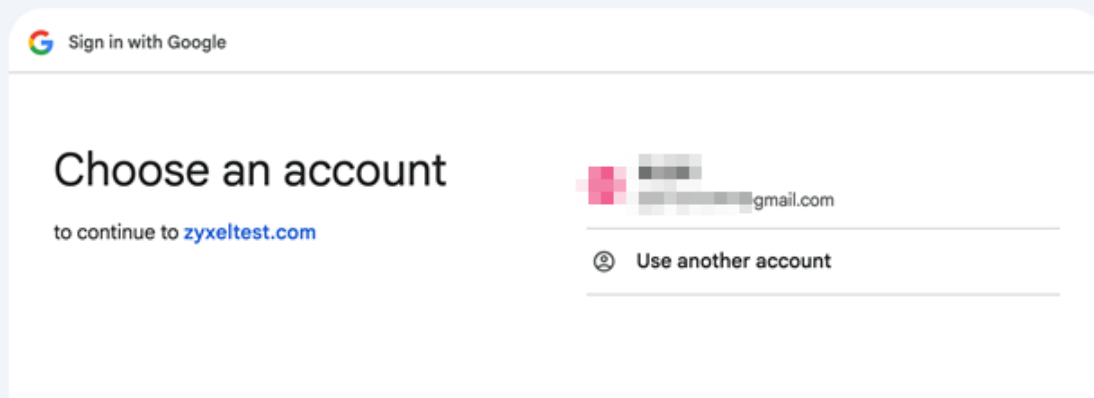
Verification

1. Connected VPN via OpenVPN Connect Client

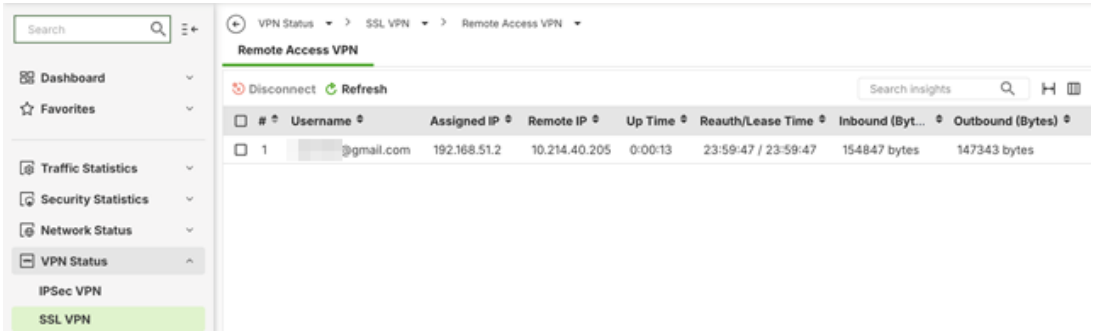
2. A browser will automatically open the Google login page.

3. Authenticate with your Google account.

> Note: The OIDC only support OpenVPN Connect Client

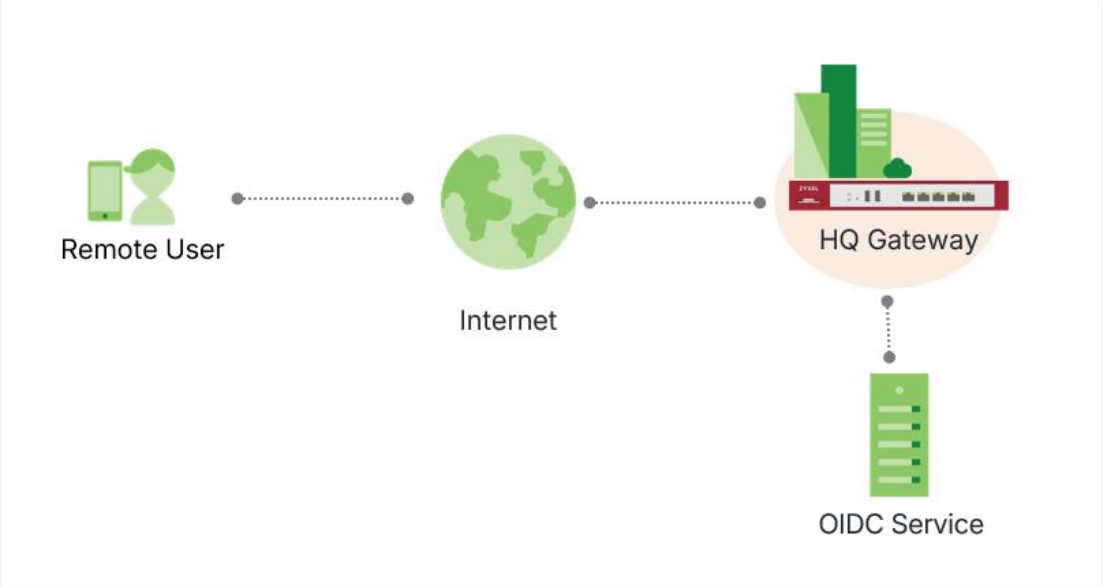


4. Check status at VPN Status > SSL VPN > Remote Access VPN.



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

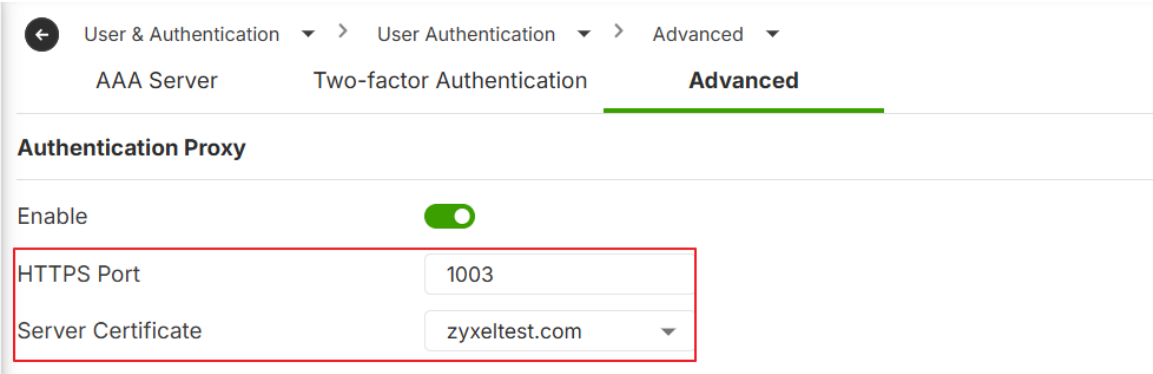
Before configuring the firewall, you must complete the required setup.

- 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**

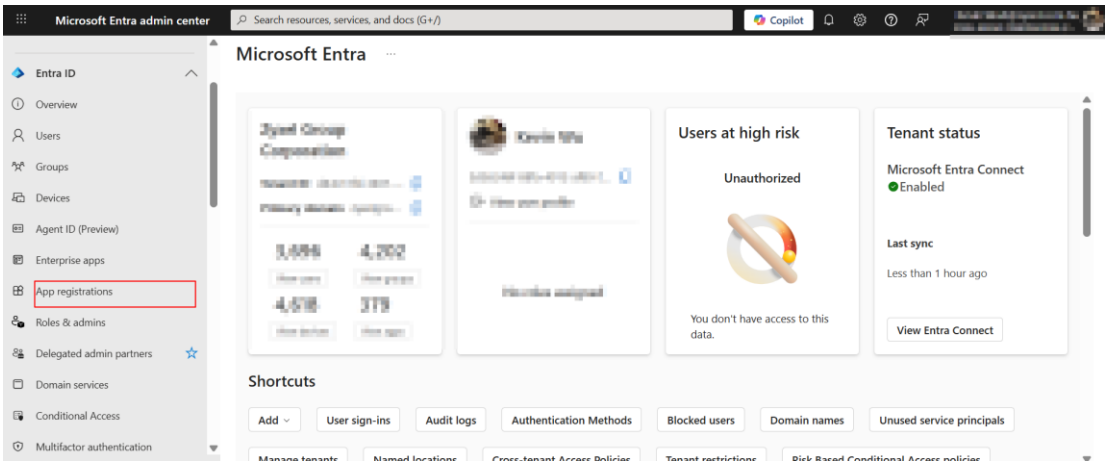
To prevent certificate warnings during the VPN client dial-up, this should be a commercial **CA-signed certificate** or your internal CA's certificate must be distributed to all client devices. And the **Common Name (CN) or SAN (Subject Alternative Name)** of the certificate should be a FQDN that can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

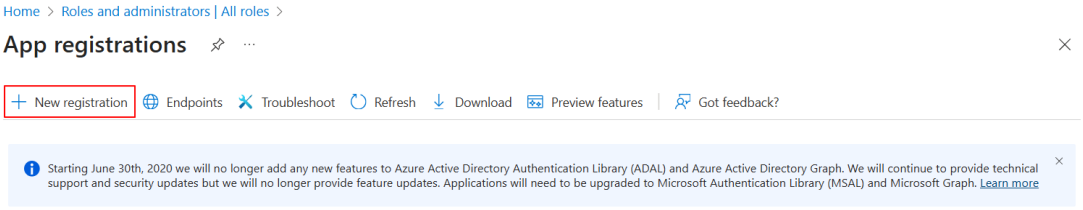


Note: Allow Authentication proxy port (default TCP 1003) on your WAN to ZyWALL secure-policy

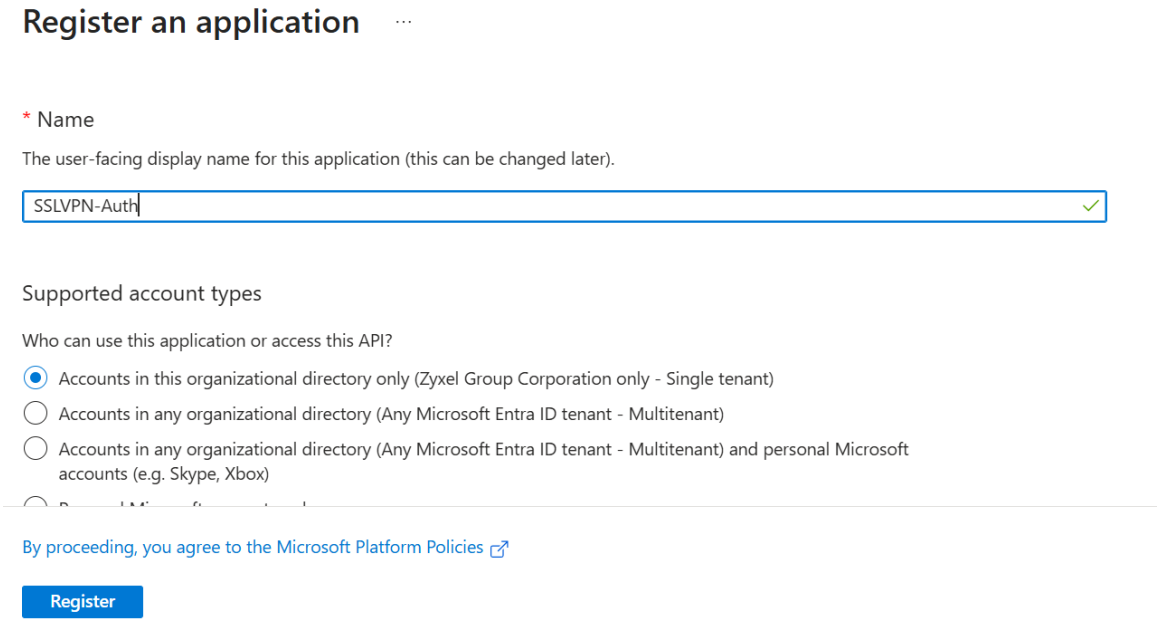
Register an Application in Microsoft Entra ID

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

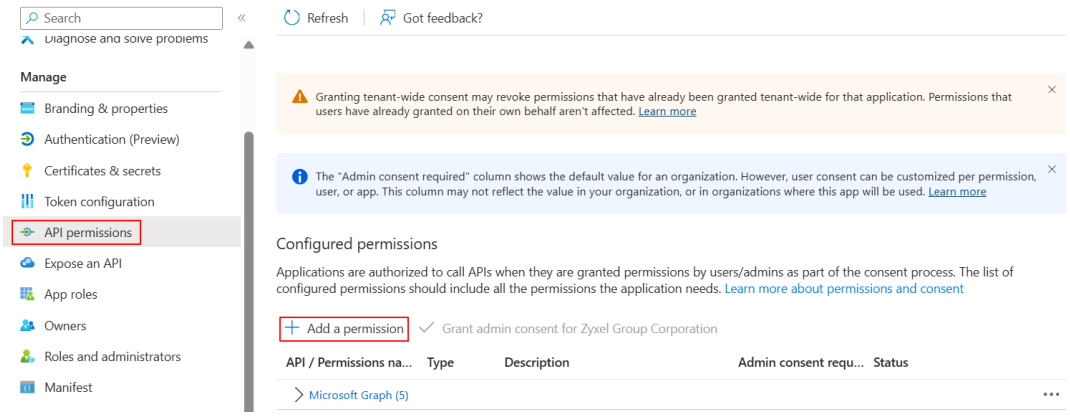




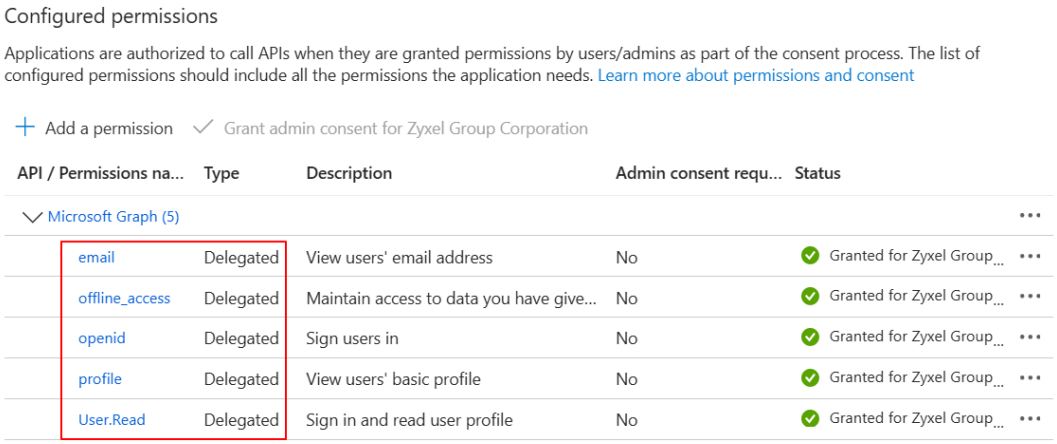
2. Enter a display name



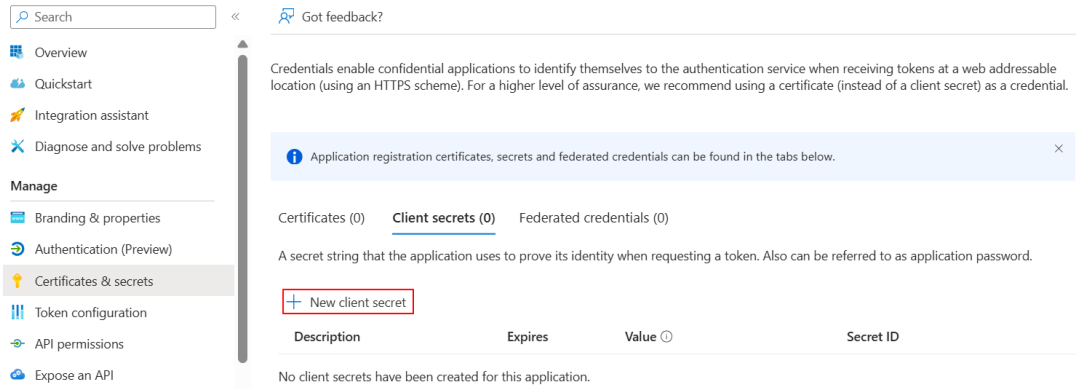
3. Navigate to Manage > API permissions > Add a permissions



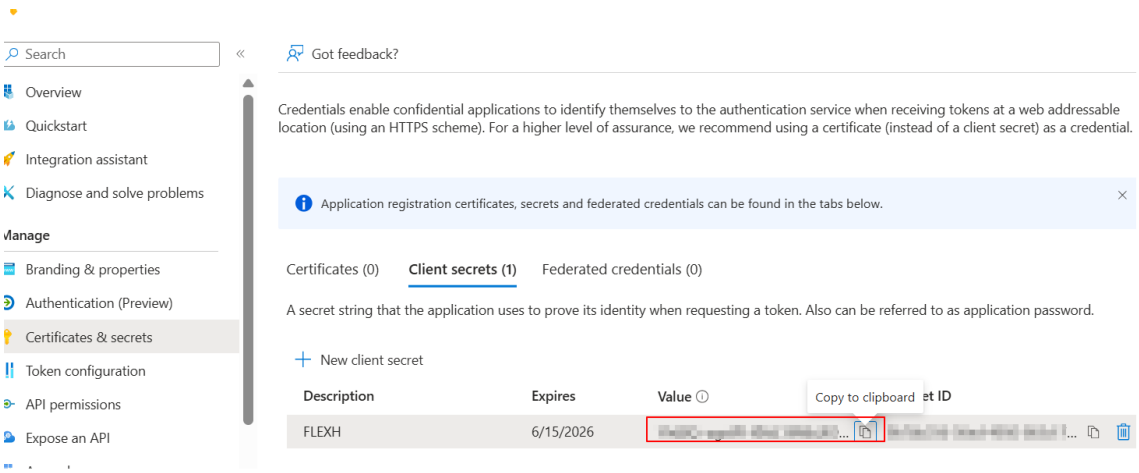
4. Please allow “email”, “offline_access”, “openid”, “profile” and “User.Read”



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



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

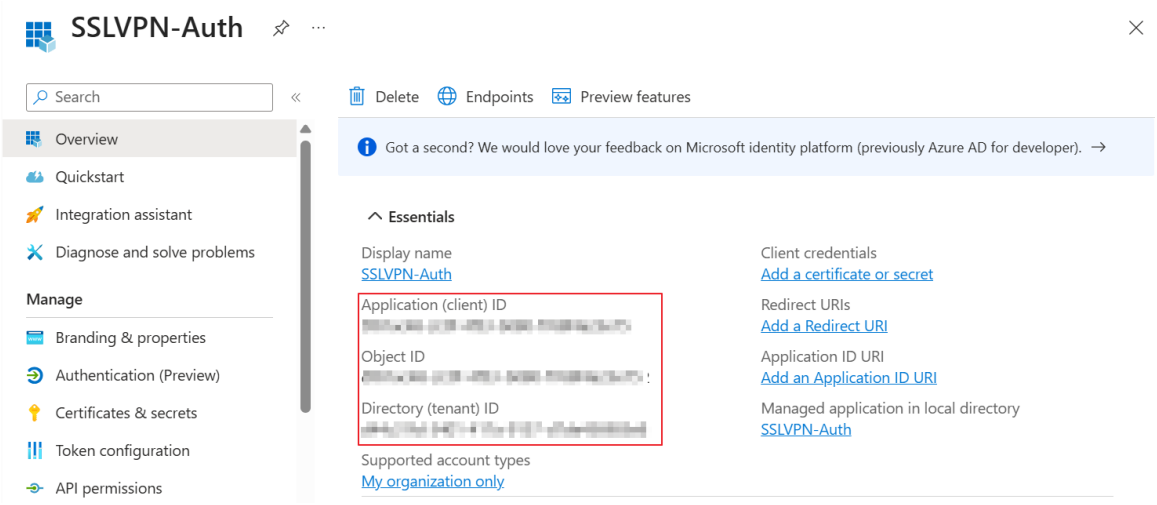


Note: **You must copy the secret immediately** because Microsoft Entra Portal hides the secret once the page reloads.

Create OIDC AAA Server

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

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



2. Fill in Server details

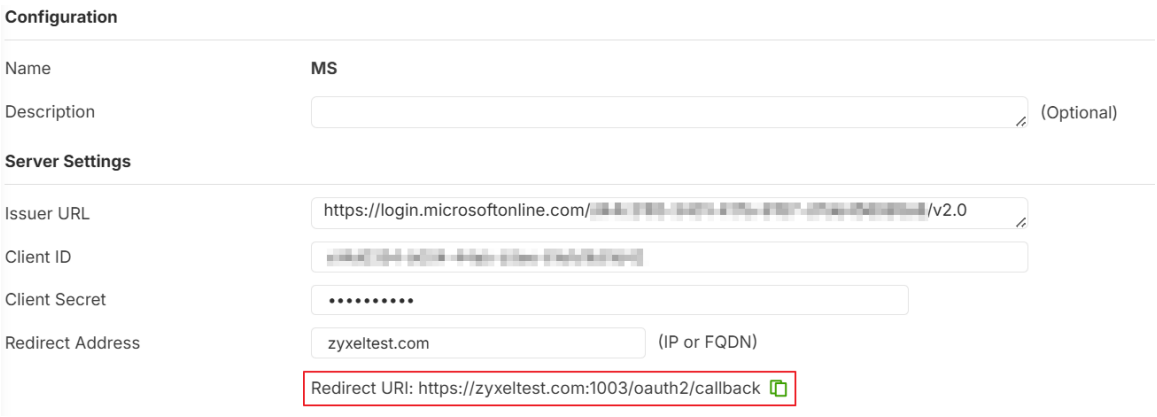
Issuer URL: https://login.microsoftonline.com/*{Tenant ID}*/v2.0

Client ID: *{Client ID}*

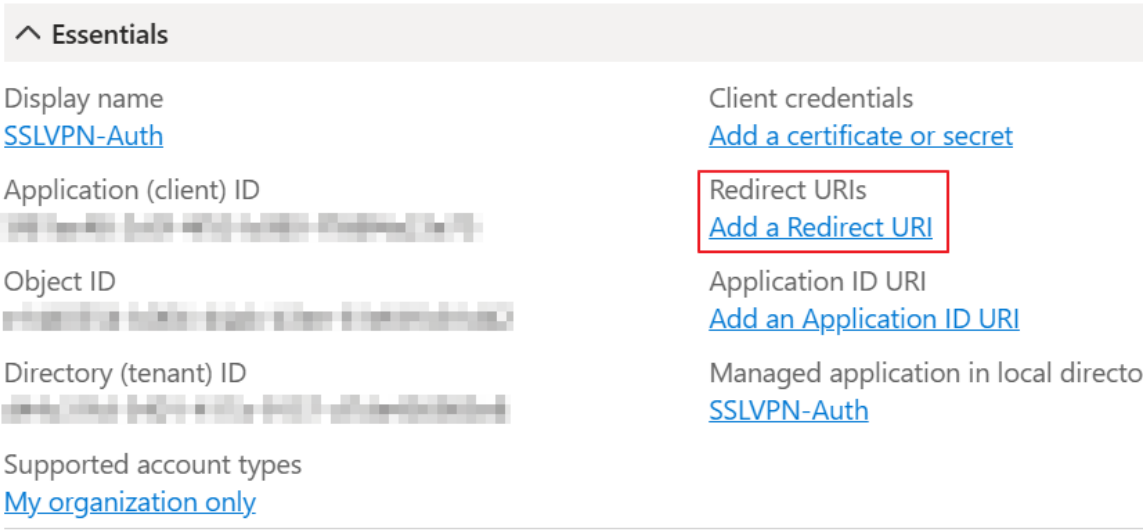
Client Secret: *{You already have Secret at "Manage > Certificate & secrets")*

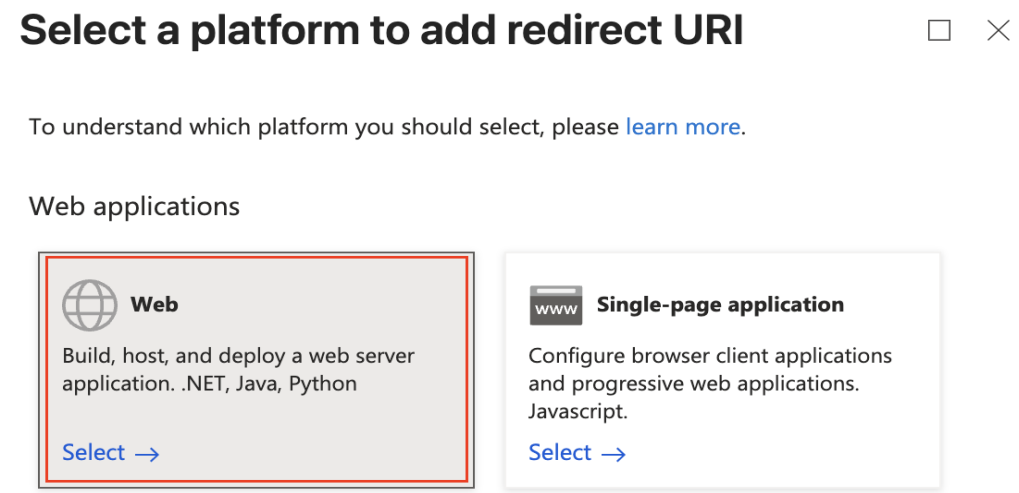
Redirect Address: *{FQDN}*

> 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.

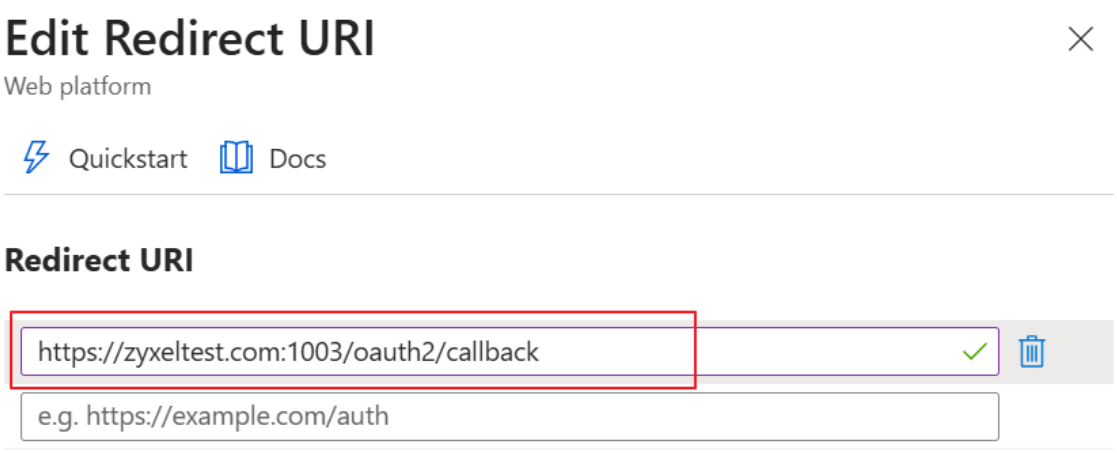


3. Copy the above “Redirect URI” and back to Entra Portal Overview > Add a Redirect URI > Add a platform > Web.



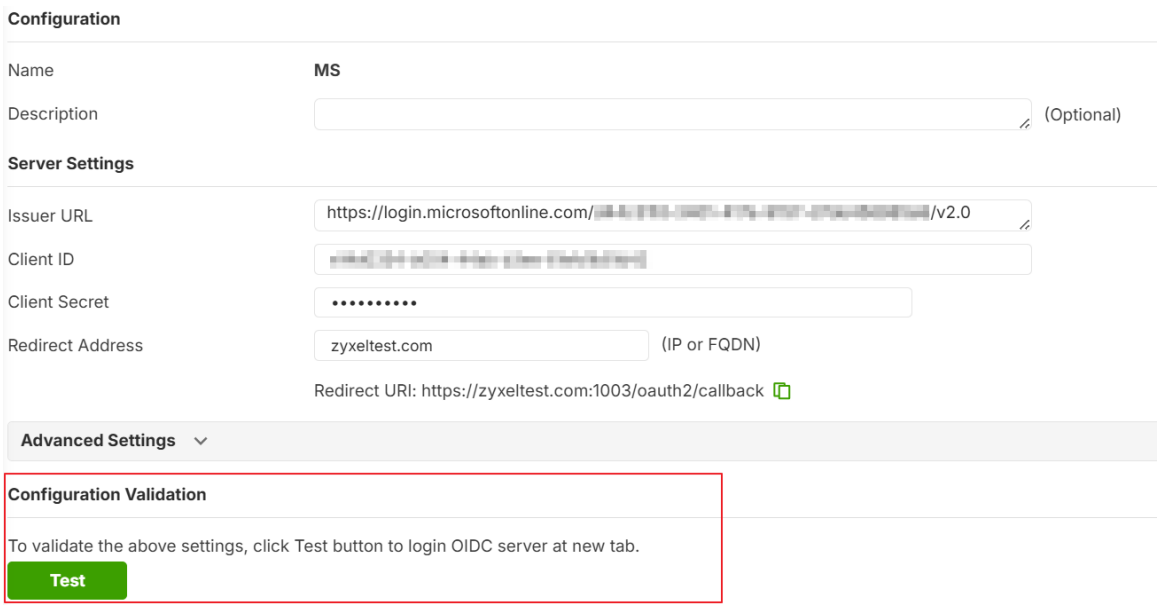


4. Paste the URI and Configure

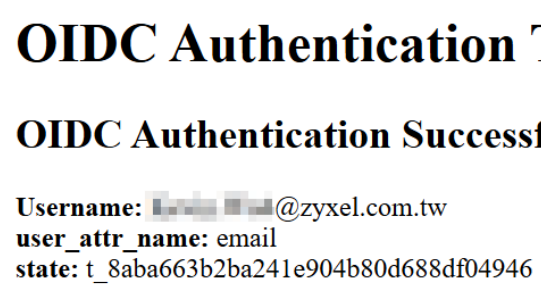


5. Go back to the USG FLEX H, OIDC Server page, at Configuration Validation.

6. Click Test on the Firewall



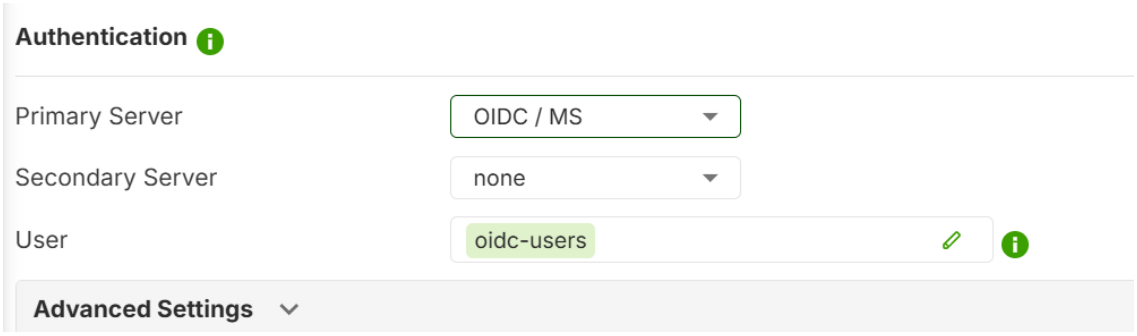
7. You should see "OIDC Authentication Successful."



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.

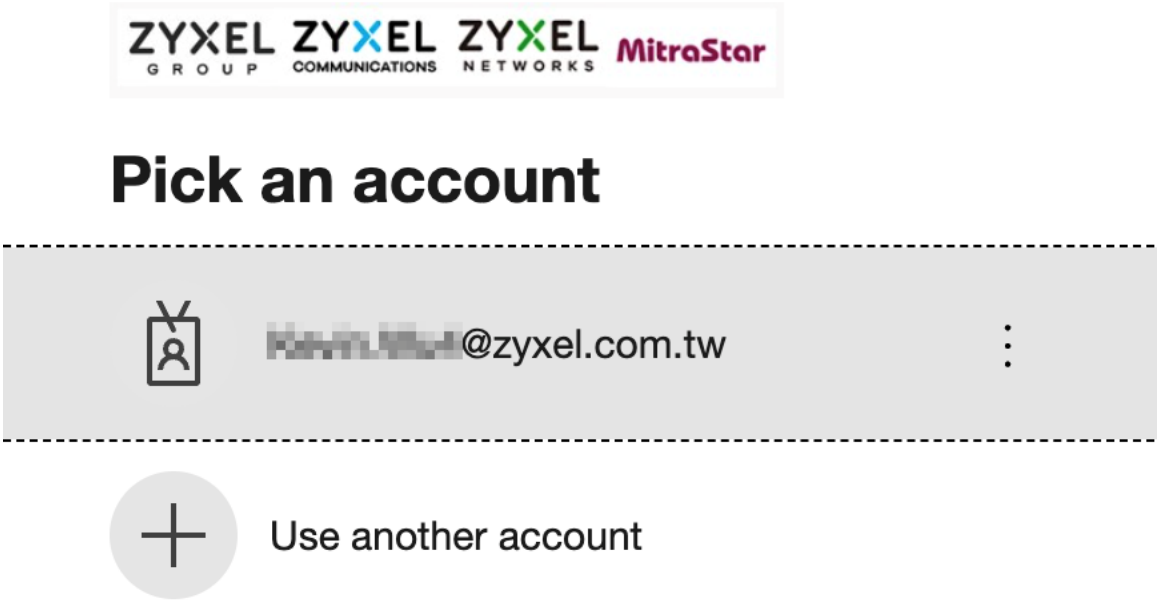


Verification

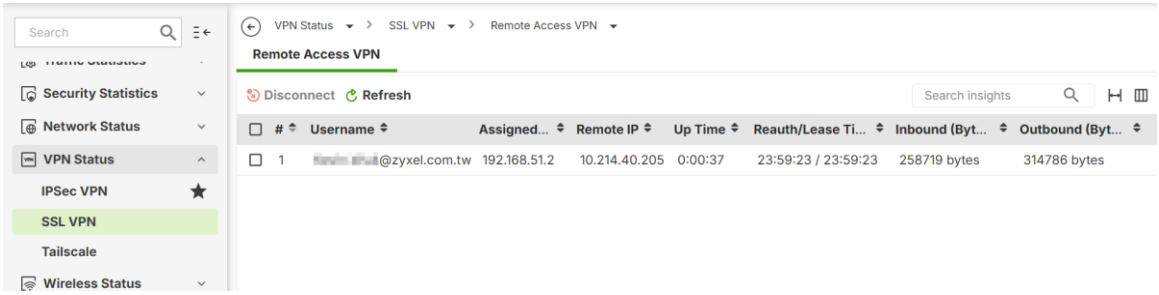
1. Connected VPN via OpenVPN Connect Client

2. A browser will automatically open the Microsoft login page.

3. Authenticate with your Microsoft account

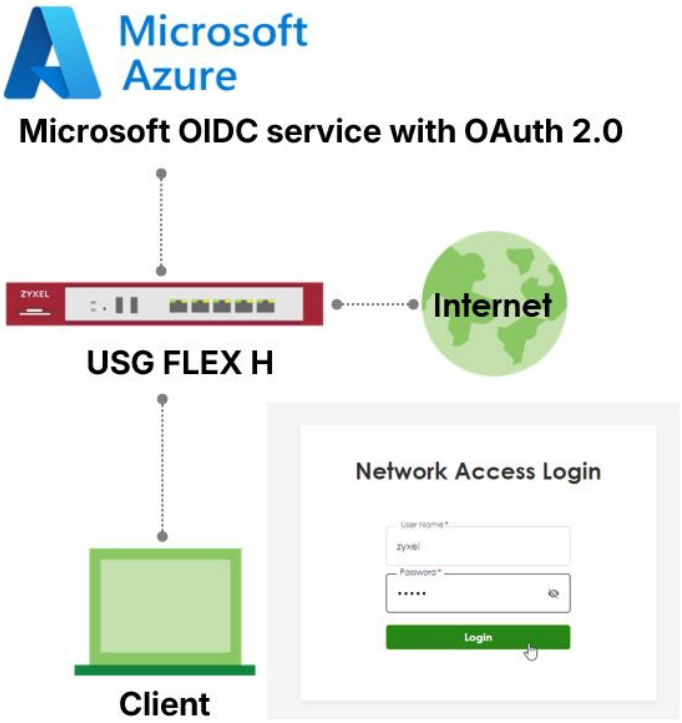


4. Check status at VPN Status > SSL VPN > Remote Access VPN.



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.



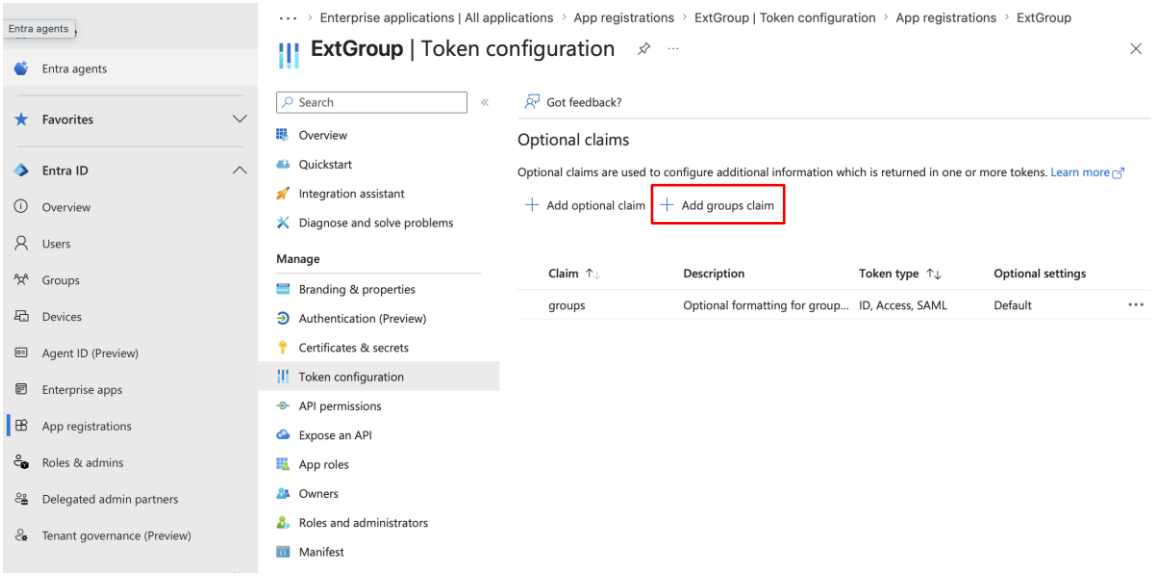
Before You Begin

Before you begin, make sure you have:

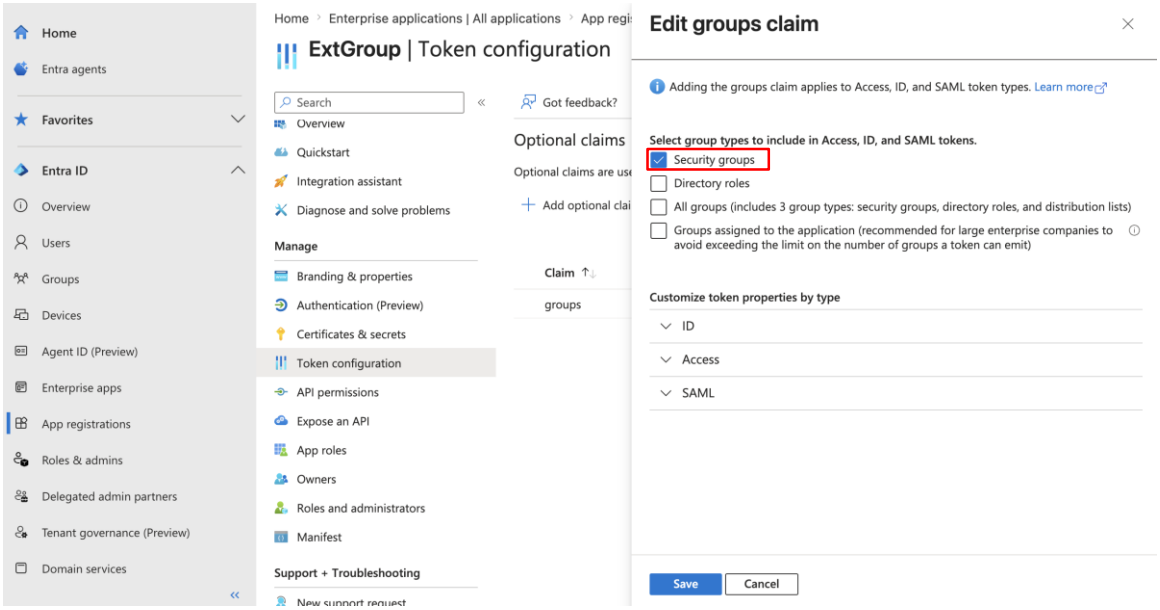
- Your firewall has completed the setting with Microsoft Entra ID, please refer to chapter: Captive Portal authentication with Microsoft Entra ID.
- There are already Users and Groups in your Entra.

Add groups claim

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

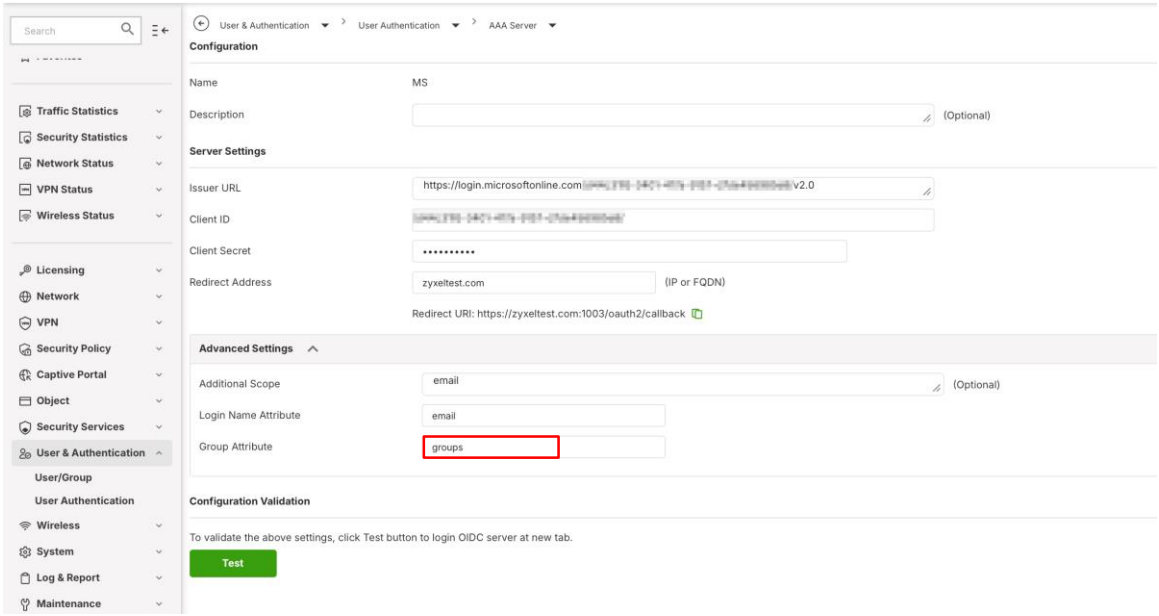


We recommend **only selecting 'Security groups'**. Choosing 'All Groups' may bloat the token with unnecessary data, potentially causing errors or overage claim issues.



Add Group Attribute on H series

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



Click Test to list the groups ID to which this user belongs.

OIDC Authentication Test

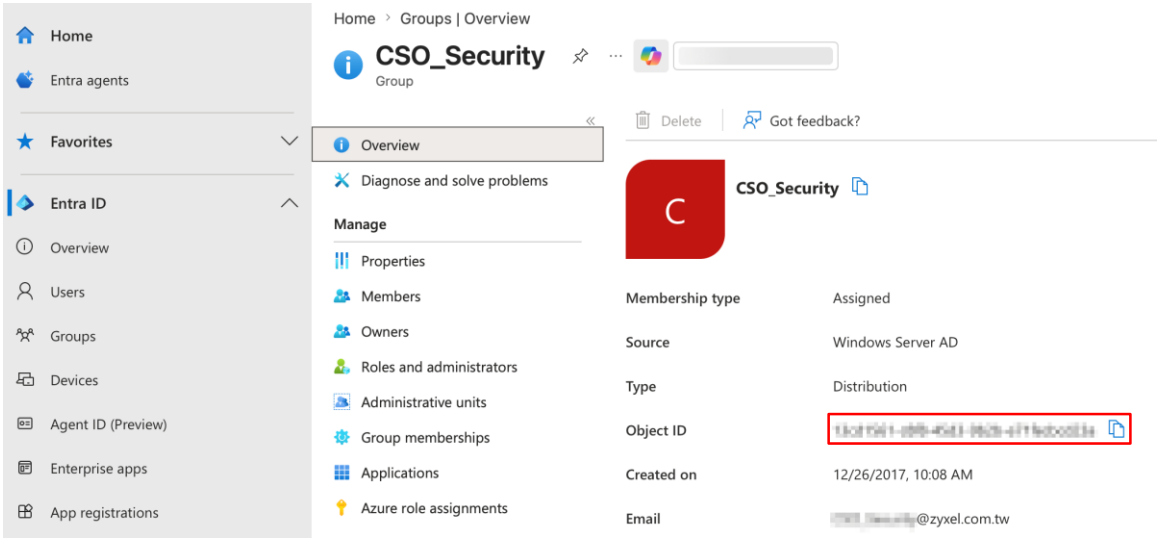
OIDC Authentication Successful (Verified)

Username: [redacted]@zyxel.com.tw
user_attr_name: email
group_attr_name: groups
group_list: [redacted]

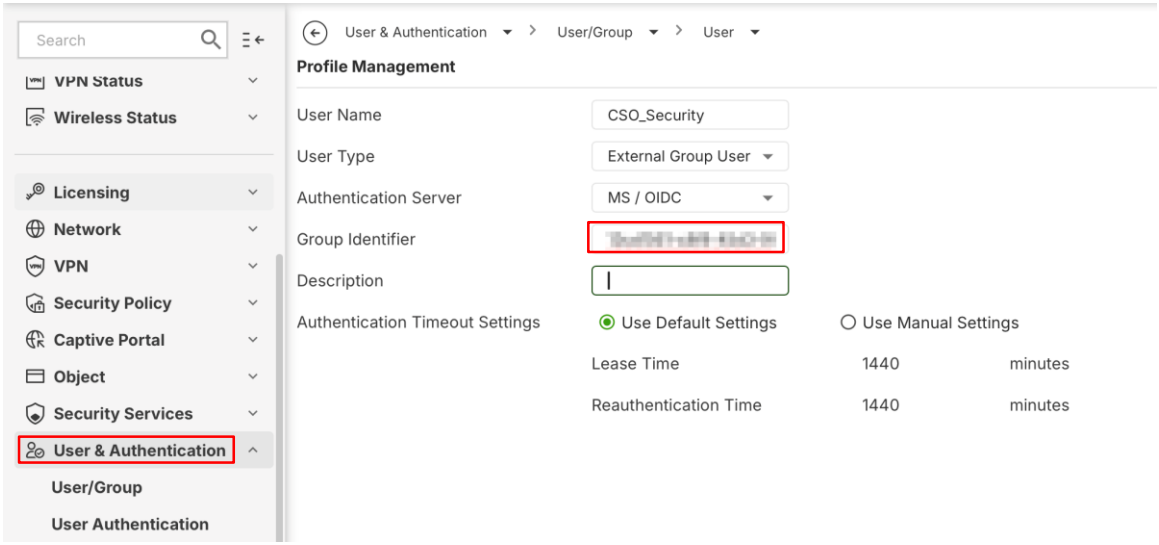
ID Token Claims

- **aud:** [redacted]
- **iss:** https://login.microsoftonline.com/[redacted]/v2.0
- **iat:** 1776667058
- **nbf:** 1776667058
- **exp:** 1776670958
- **email:** [redacted]@zyxel.com.tw
- **groups:** [redacted]
- **nonce:** [redacted]

Find your Group Object ID in Entra Portal and copy object ID to clipboard.

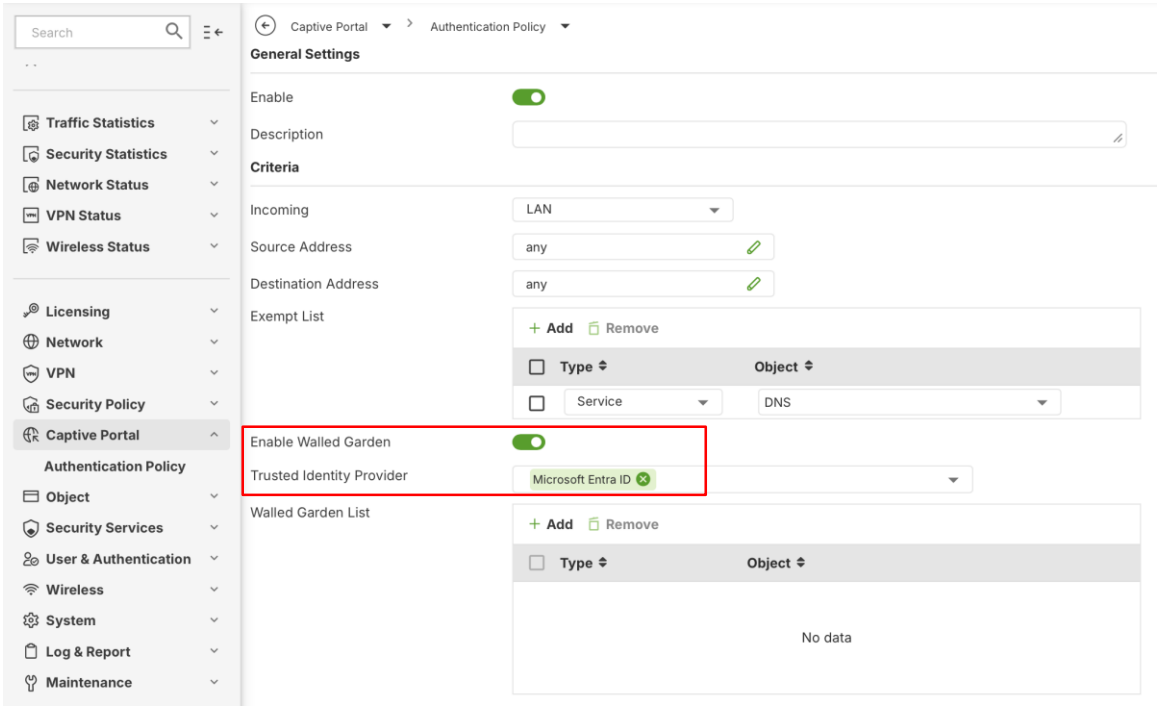


Navigate to User & Authentication > User Authentication > User/Group, Add User with type External Group User, and paste the Group Identifier.

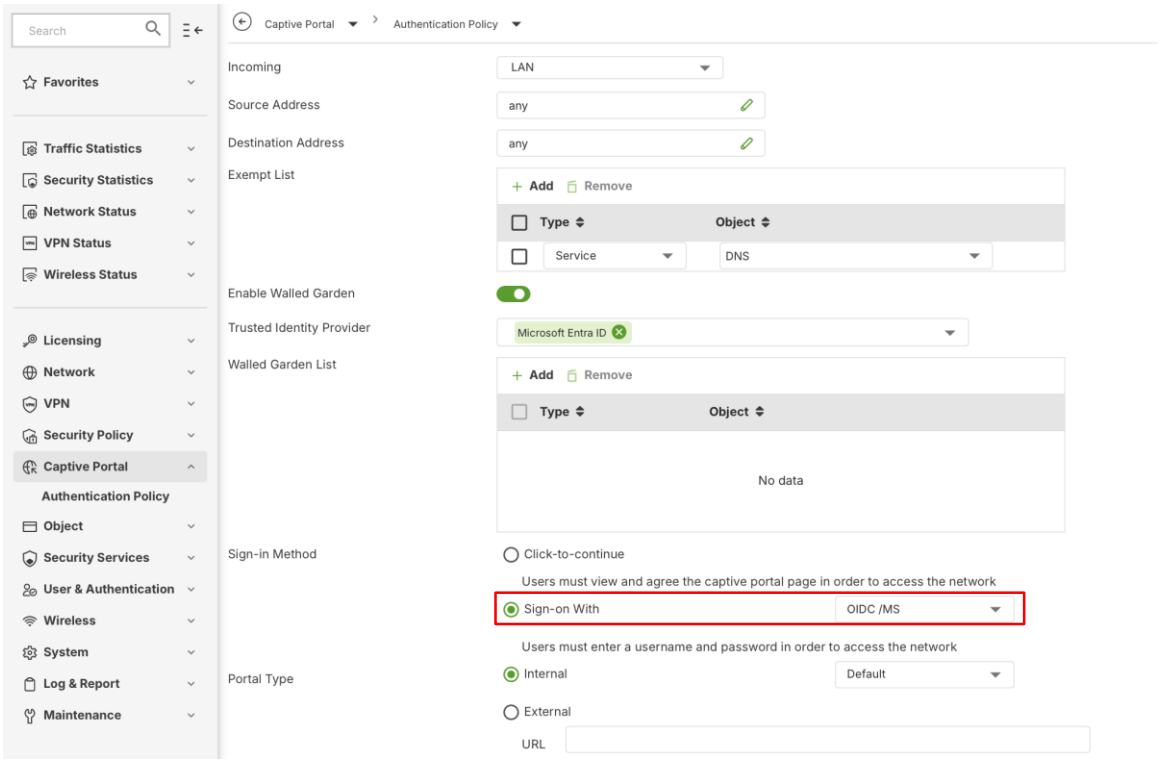


Add Captive Portal Policy

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



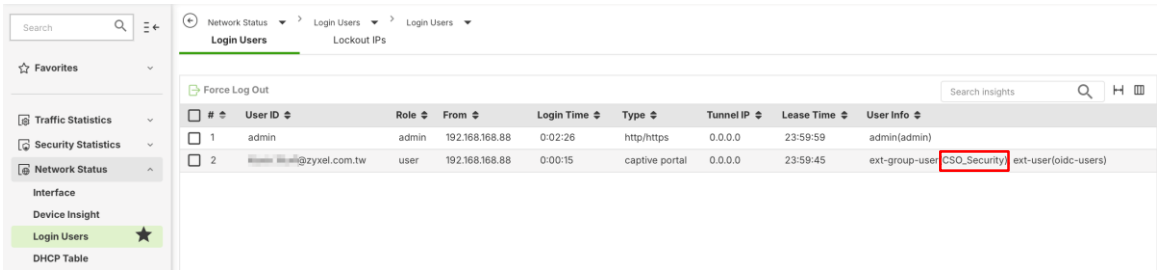
Select Sign-in Method to OIDC server.



Verification

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

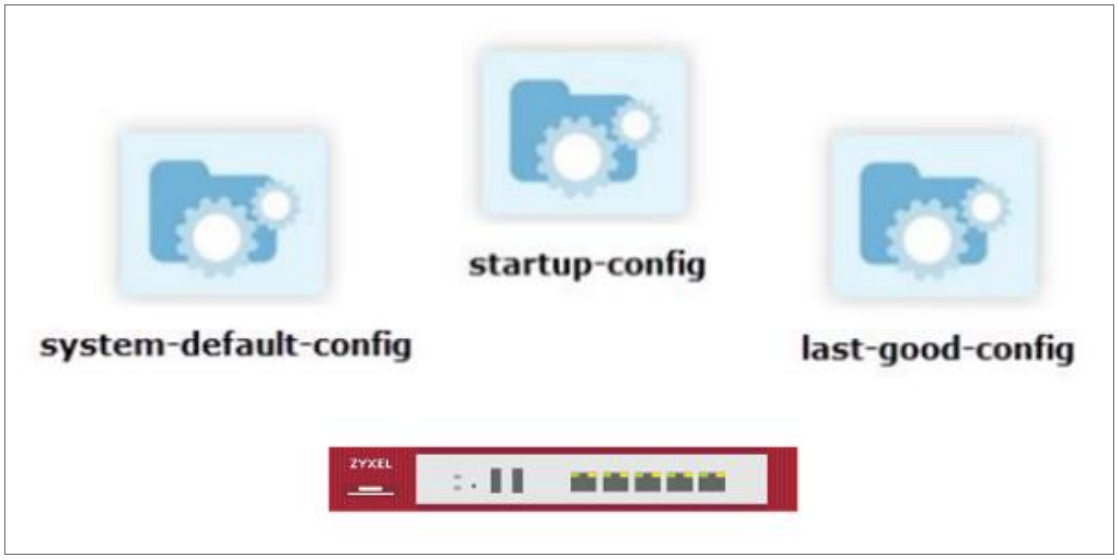
Network Status > Login Users.



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.

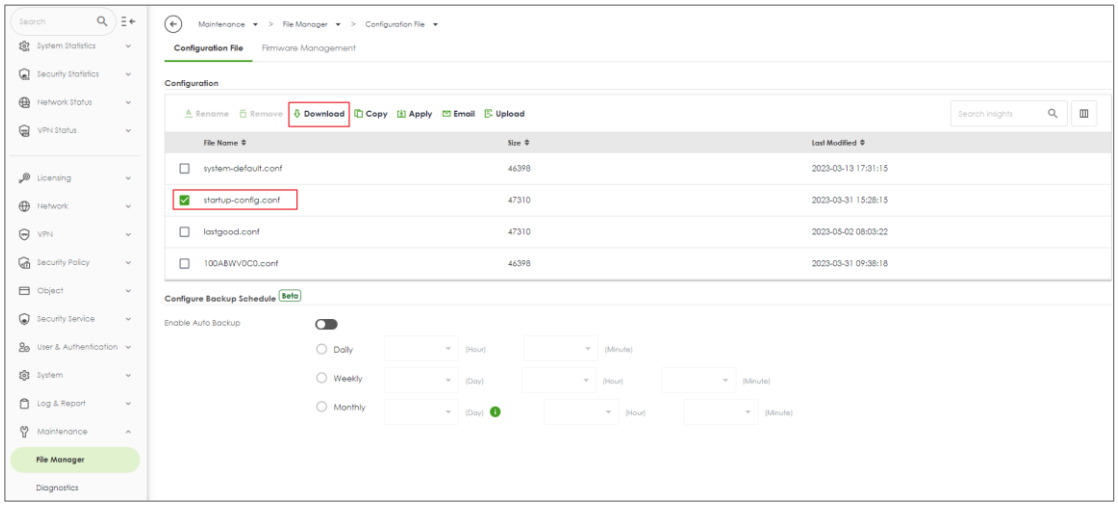
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

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

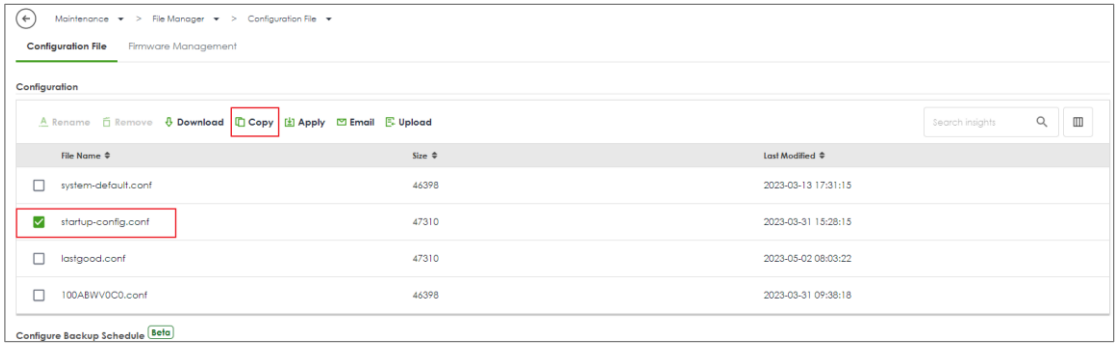
Select the statup-config.conf and click “Download”.



Copy the Configuration Files

Maintenance > File Manager > Configuration File

Select the file and click “Copy”.



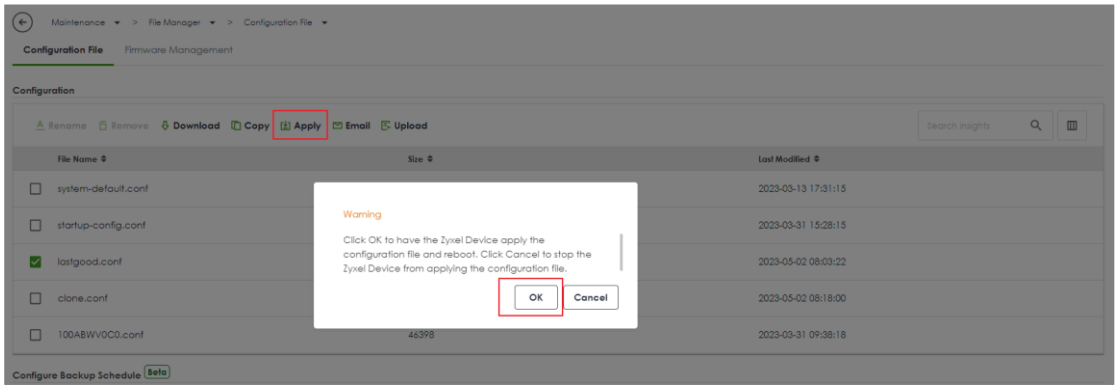
A pop-up screen will appear allowing you to edit the Target file name.

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

Apply the Configuration Files

Maintenance > File Manager > Configuration File

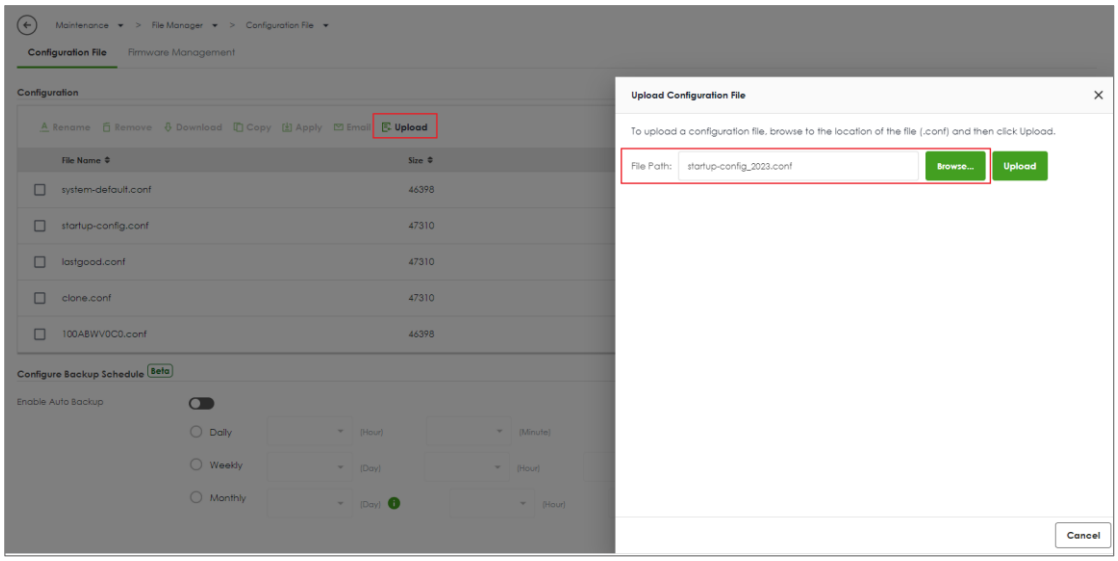
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when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



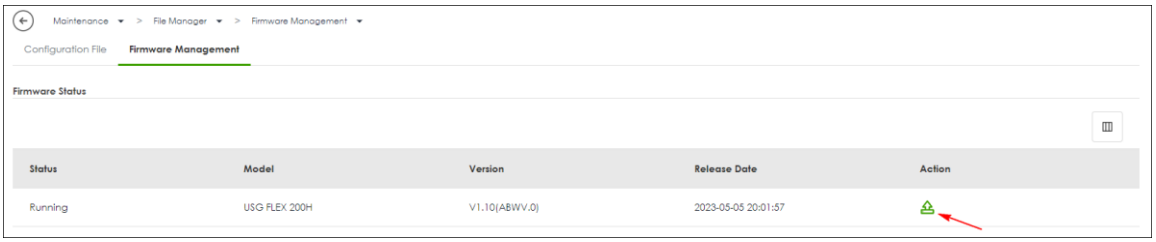
How to Manage Firmware

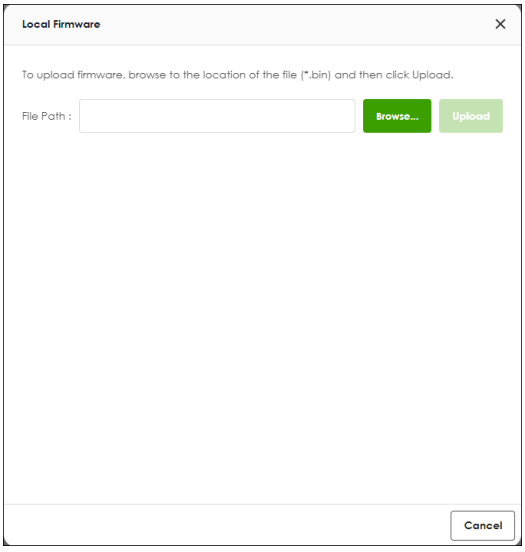
For management convenience, administrators have the capability to upgrade the firmware effortlessly either from a PC or using the cloud firmware upgrade function. Additionally, the firmware upgrade can be scheduled to occur automatically within a preconfigured timeframe.

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

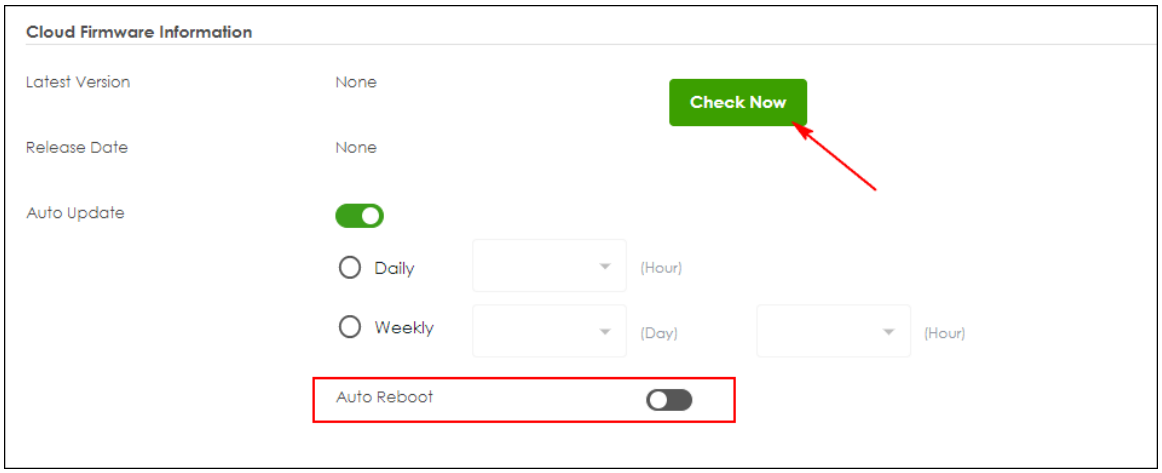




Cloud Firmware Upgrade

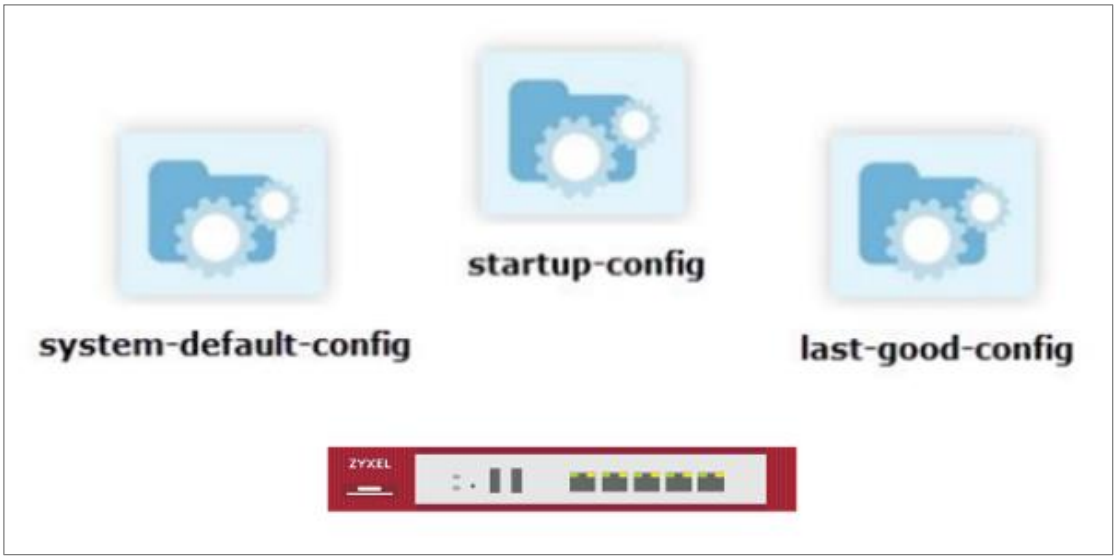
The cloud firmware upgrade function allows you to verify the most recent firmware version by clicking the "Check New" button.

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.



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.

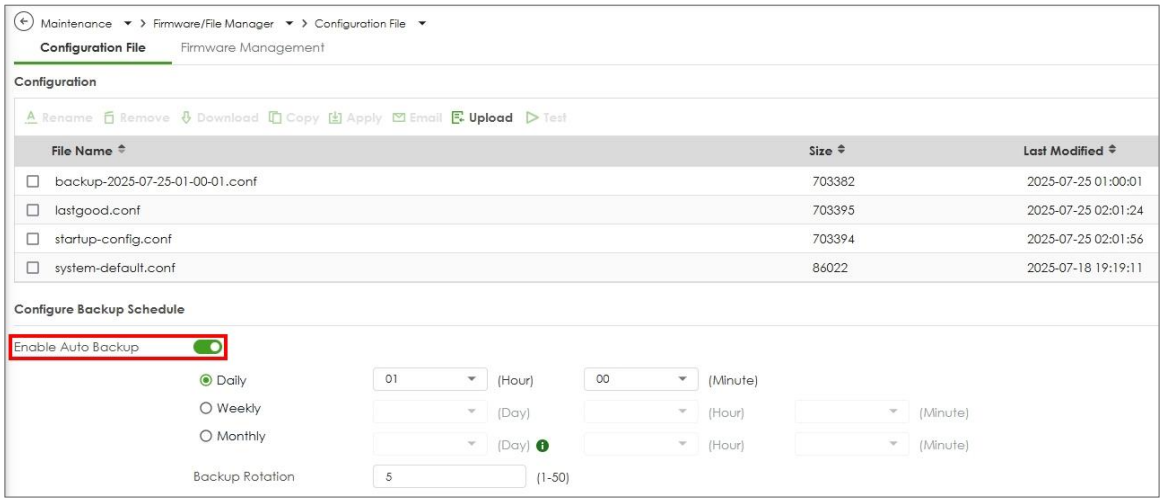


Note: The **system-default.conf** file contains the default settings. This configuration file is included when you upload a firmware package.

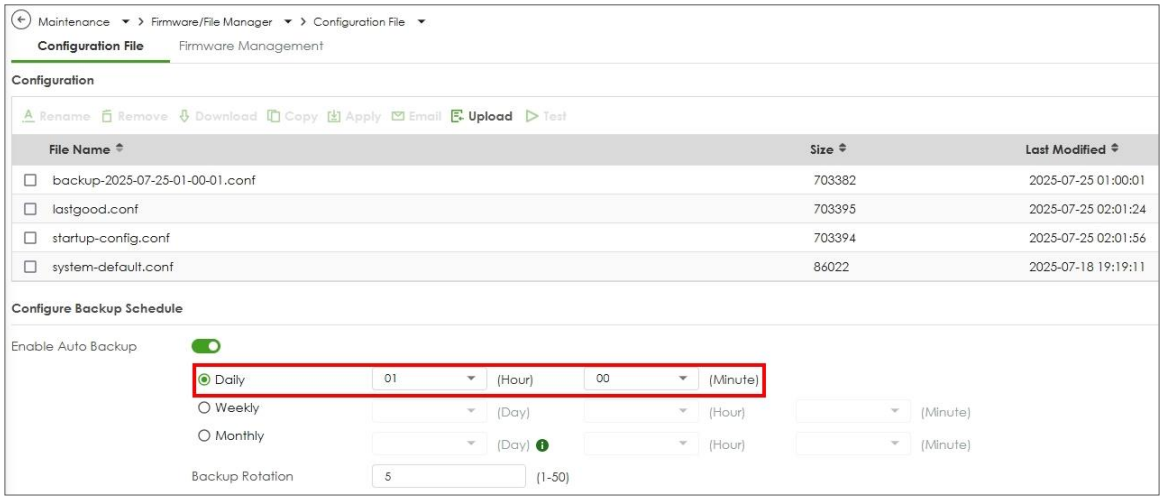
The **startup-config.conf** file is the configuration file that the Firewall is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

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

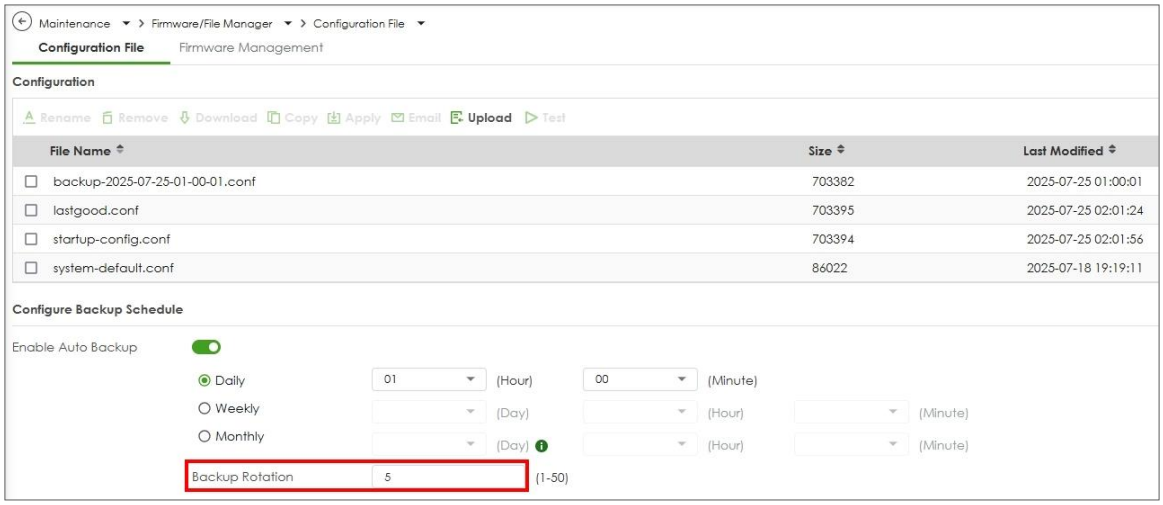
Go to Configuration Backup Schedule section and enable “Enable Auto Backup”.



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



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.

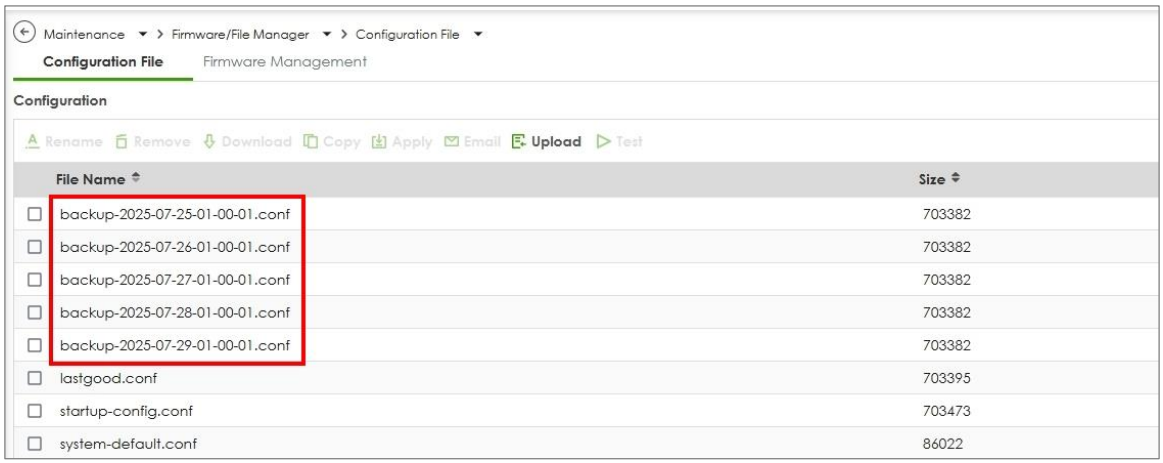


Note: By default, the system allows up to 65 backup files, with a maximum total size of 200 MB.

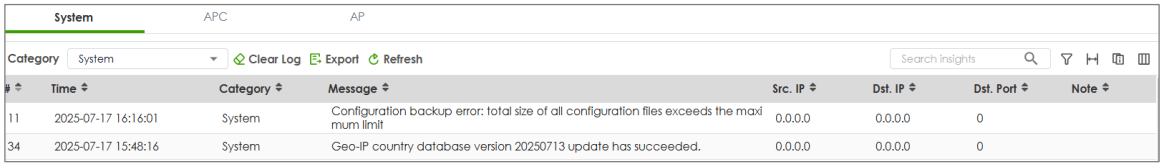
Verification

Maintenance > File Manager > Configuration File

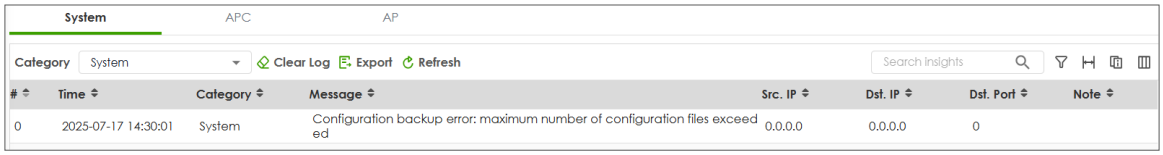
Five scheduled backup configurations are generated based on the scheduled backup settings. The firewall has automatically backed up five files, and it deletes the oldest file before performing an automatic backup.



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.



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.



Chapter 5- Others

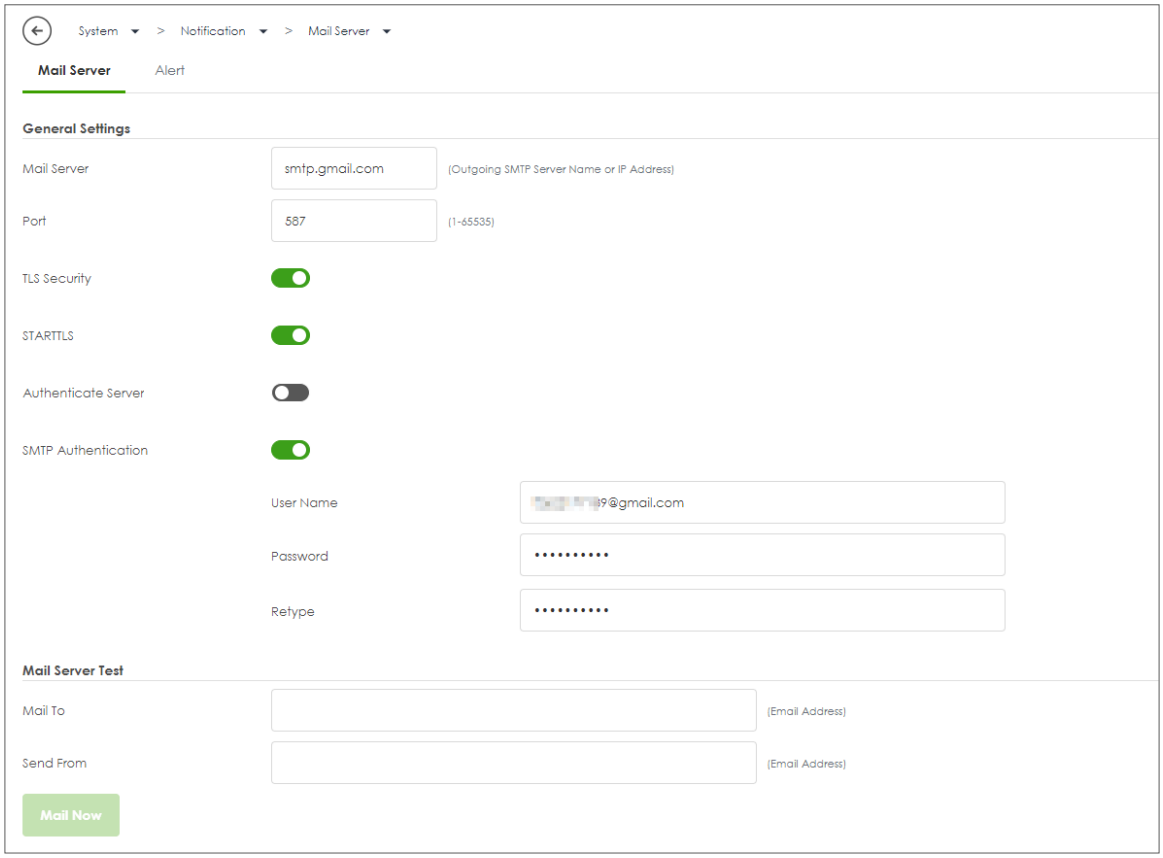
How to Setup and Configure Daily Report

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.

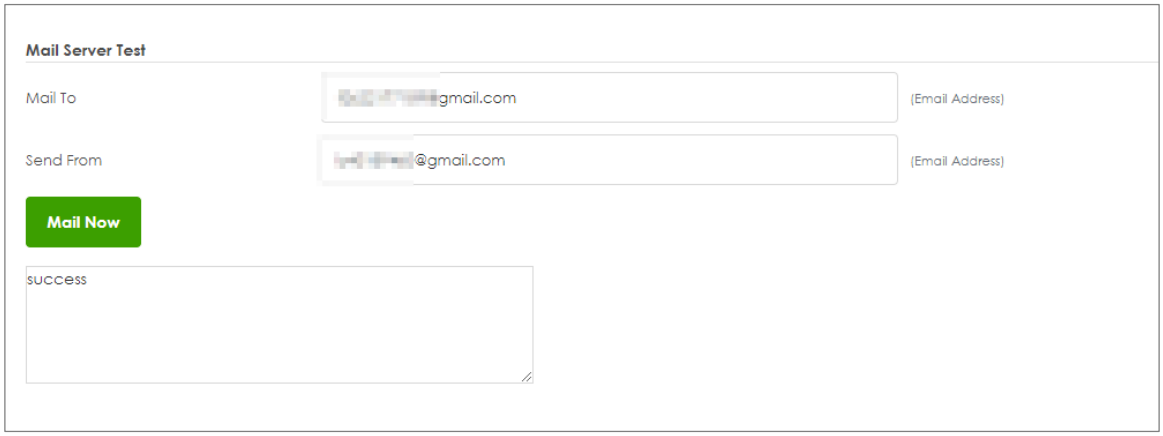
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

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.

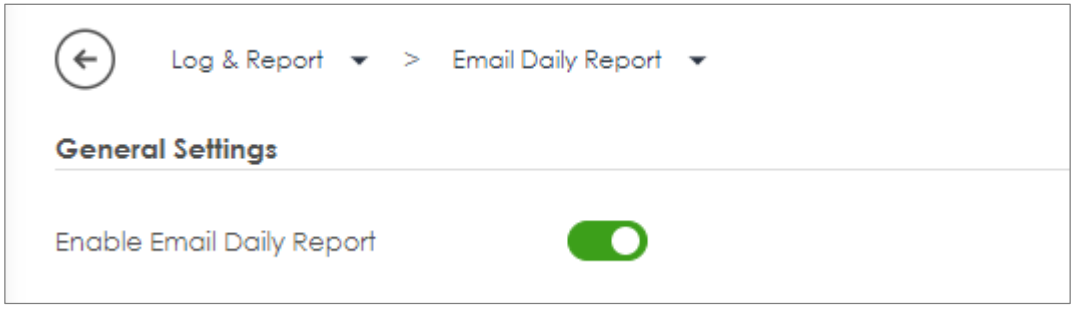


You can verify the correctness of the settings by using the Mail Server Test below. If it is successful, you will receive an email.

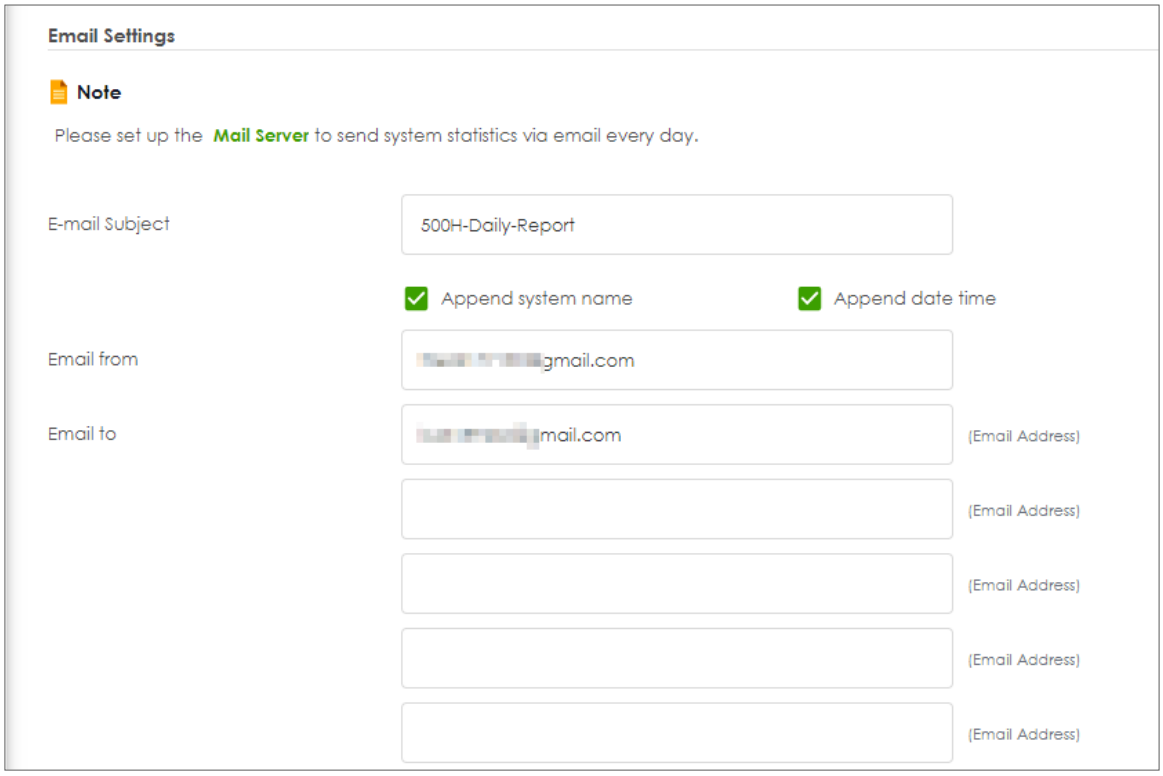


Set Up Email Daily Report

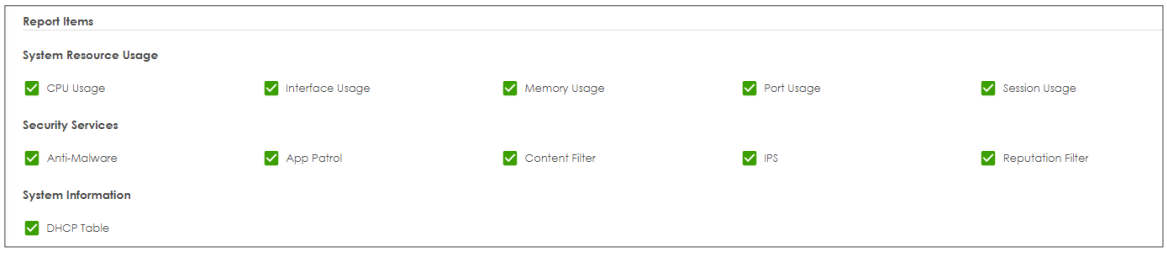
Navigate to Log & Report > Email Daily Report. Enable your Email Daily Report



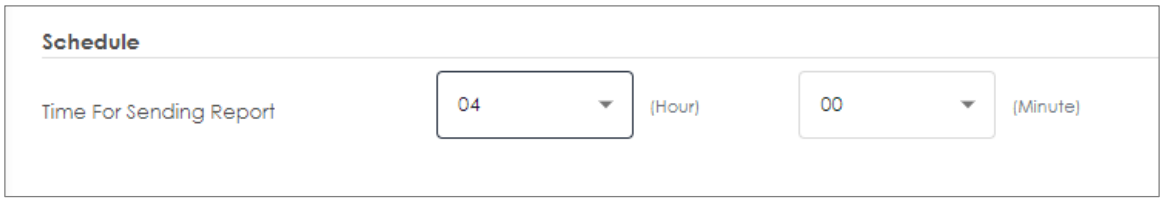
Type your Email Subject and your Sender and Receiver in the field.



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

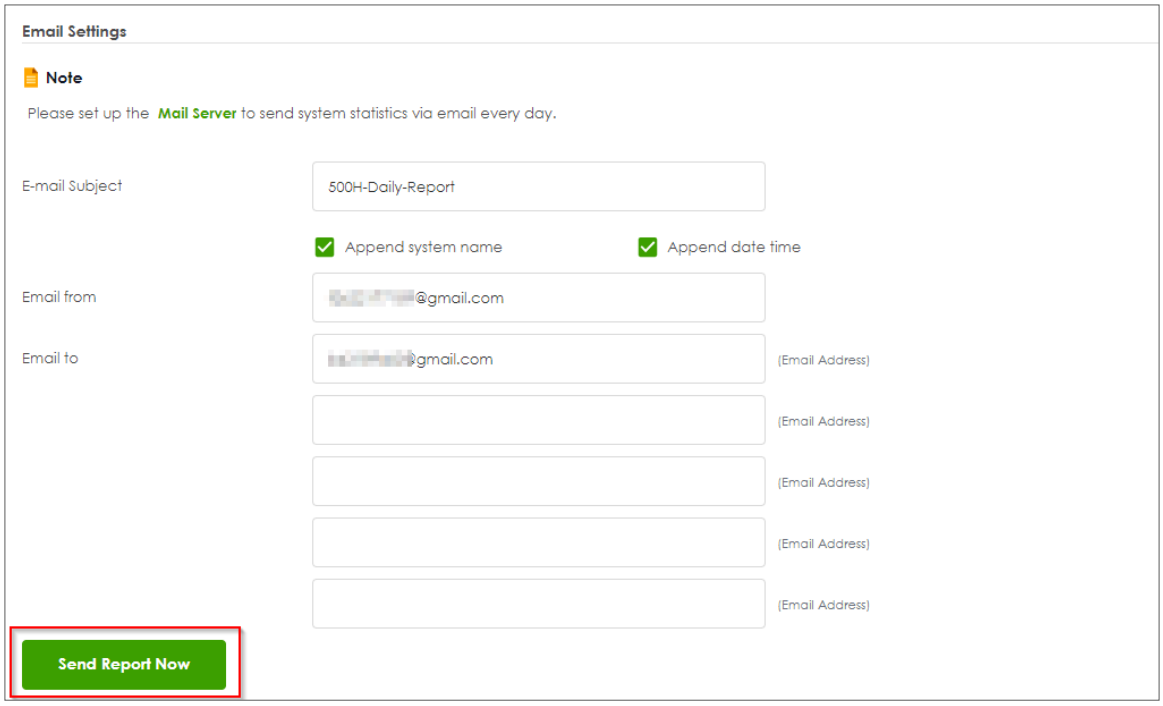


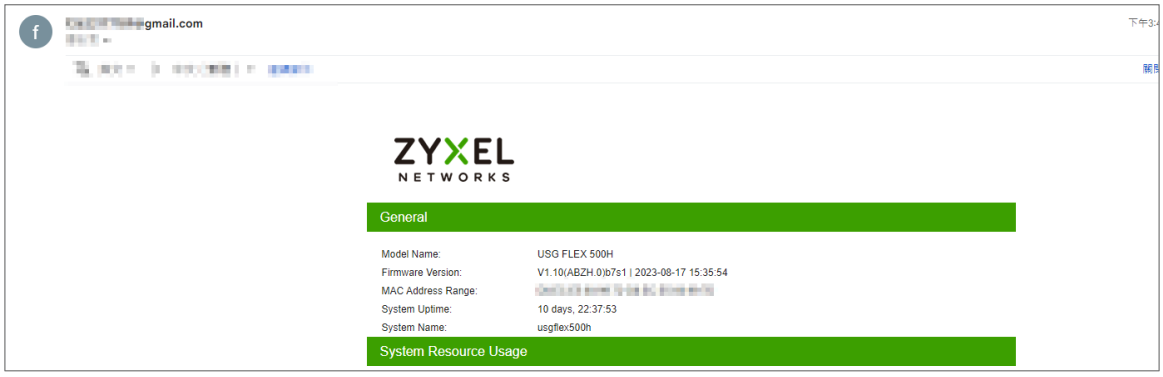
You can set up a Schedule at the bottom of the page



Test the Email Daily Report

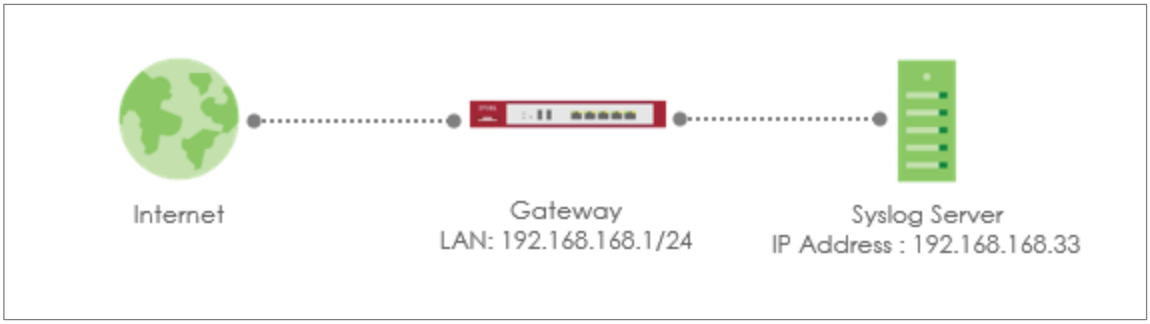
To confirm if the daily report has been set up successfully, click "Send Report Now."





How to Setup and Send Logs to a Syslog Server

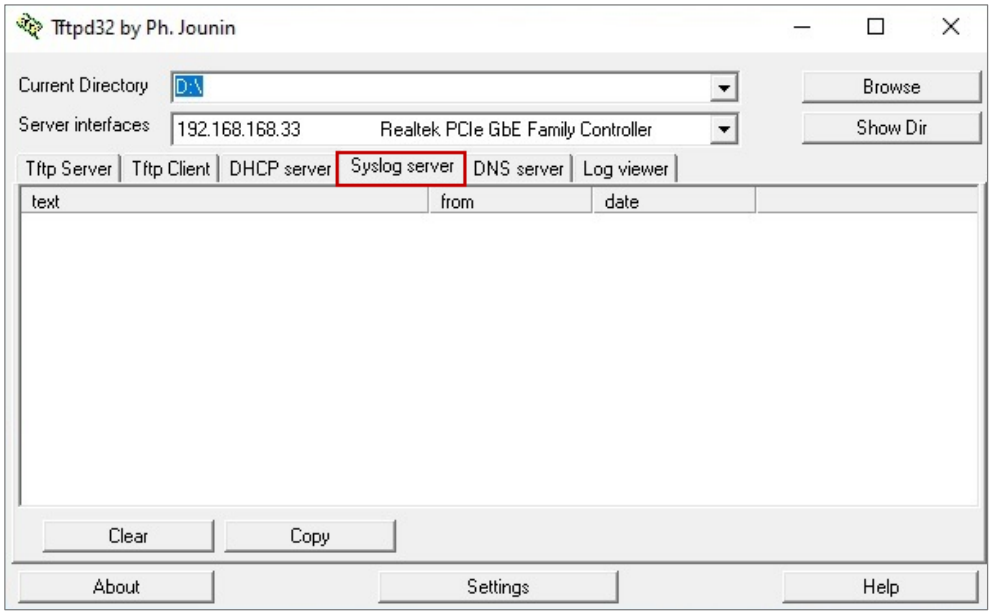
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system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

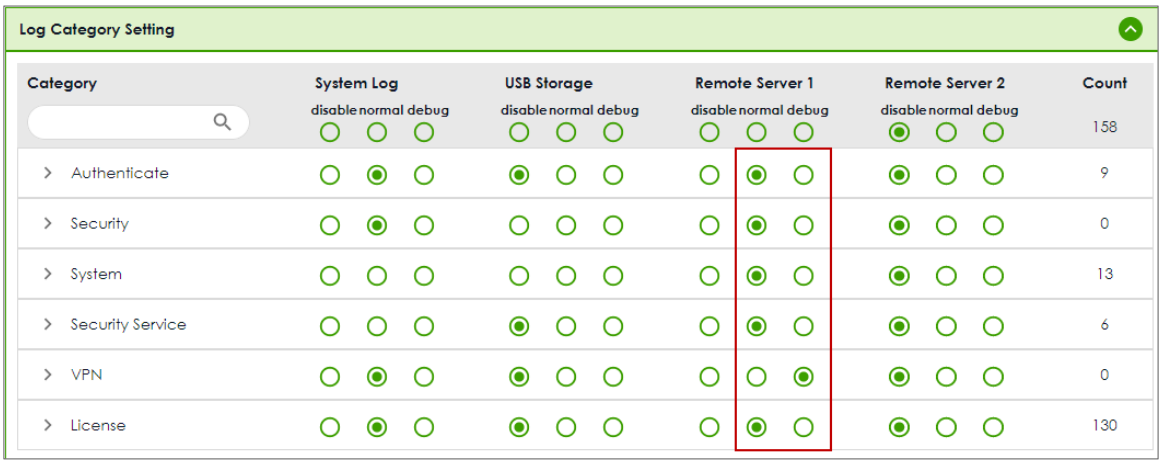
Set Up the Syslog Server

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

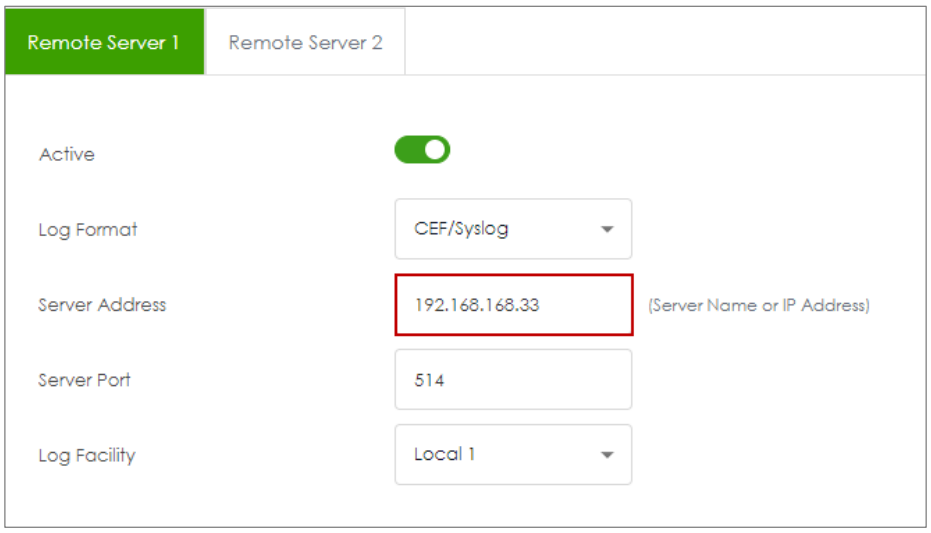


Set Up Remote Server Setting on the Gateway

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.

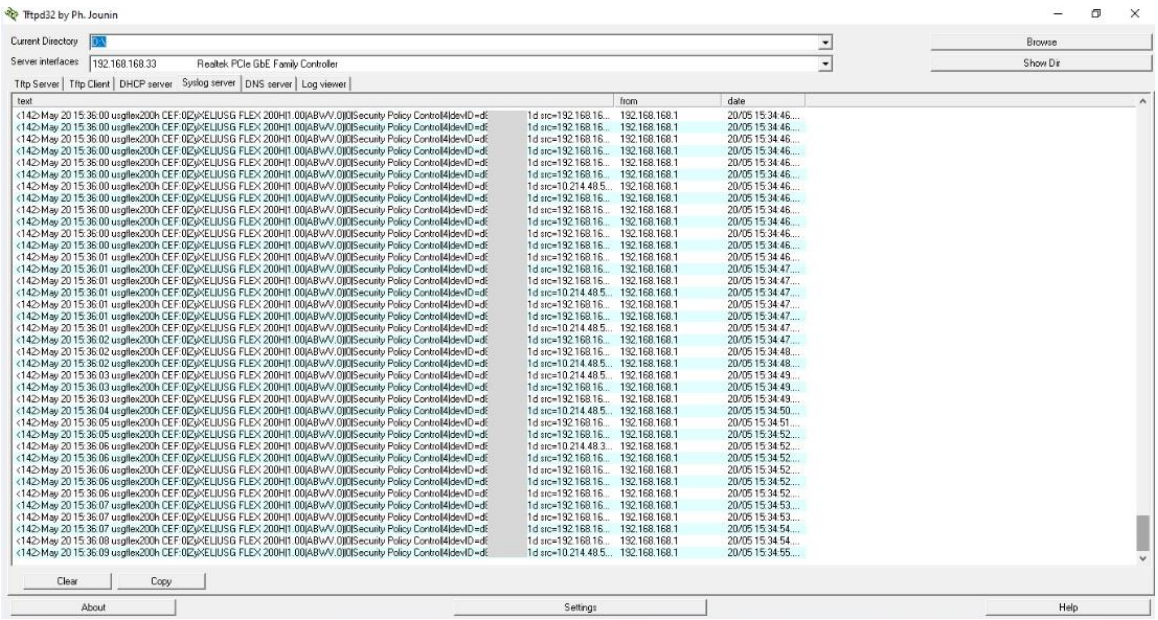


Go to Log & Report > Log Settings > Remote Syslog Server. Set Log Format to be CEF/Syslog and type the server name or the IP address of the syslog server. Turn on “Active” to send log information to the server.



Test the Remote Syslog Server

Check logs on the syslog server.



How to Setup and Send logs to the USB storage

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

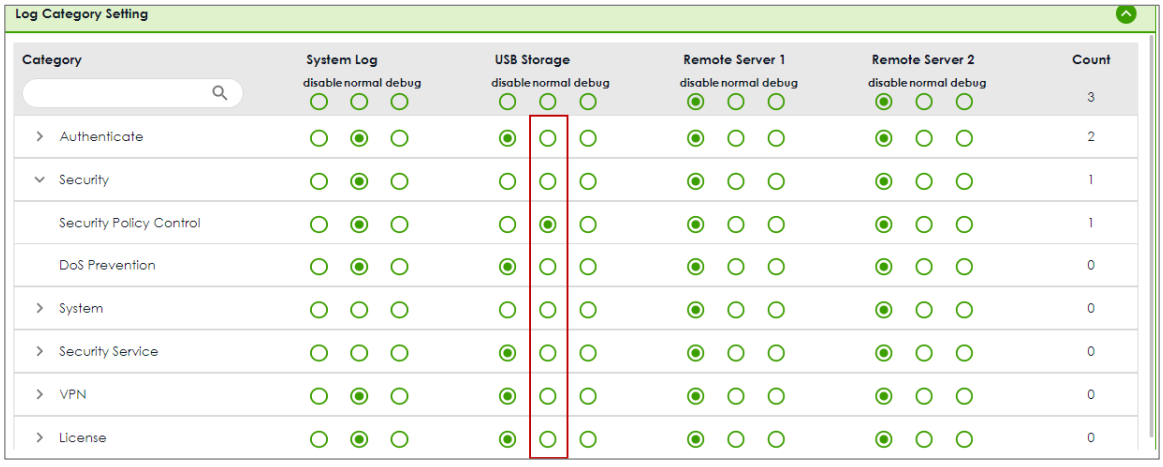
Note: The USB storage must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10). The USB port can provide max. 900mA output power. You might need to connect external power for the USB storage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

USB Storage device

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

Set Up the USB storage on the Gateway

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

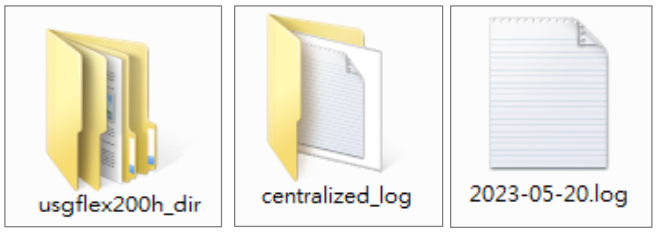


Go to Log & Report > Log Settings > USB Storage. Turn on “Enable USB storage” to store the system logs on a USB device.

Check the USG Log Files

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

You can also connect the USB storage to PC and find the files in the following path. \Model Name_dir\centralized_log\YYYY-MM-DD.log



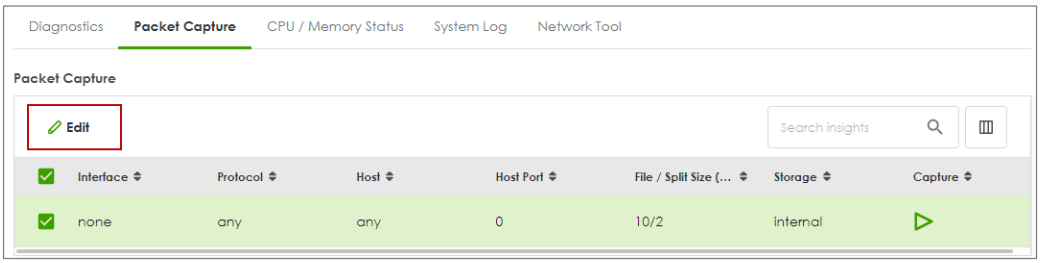
How to Perform and Use the Packet Capture Feature

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

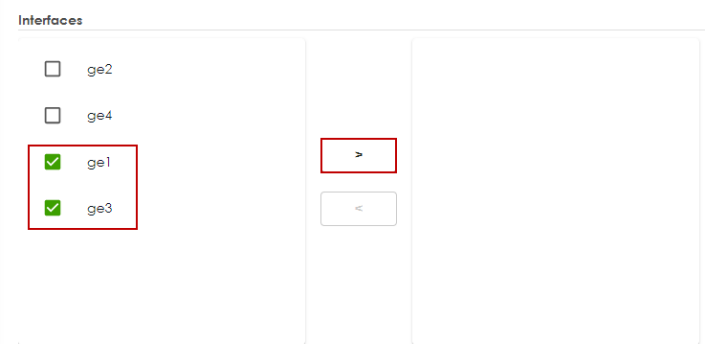
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the Packet Capture Feature

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

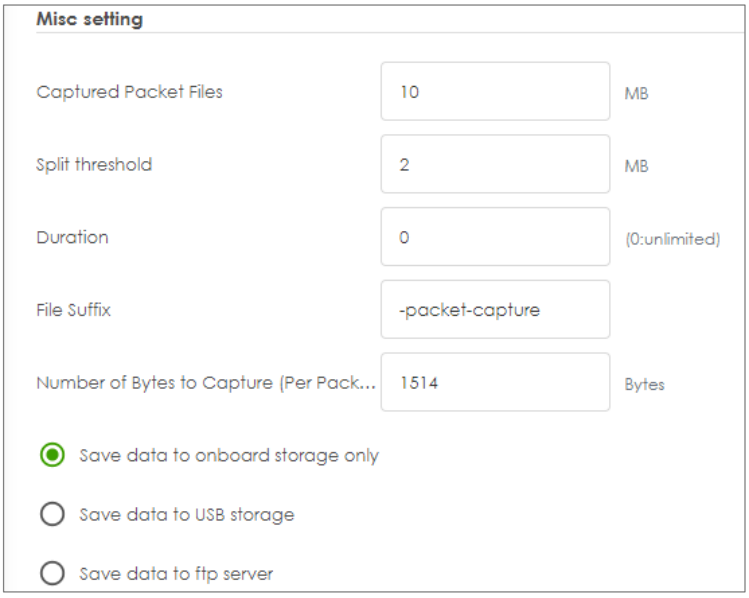


6. In Interfaces, select interfaces for which to capture packets and click the right arrow button to move them to the list.

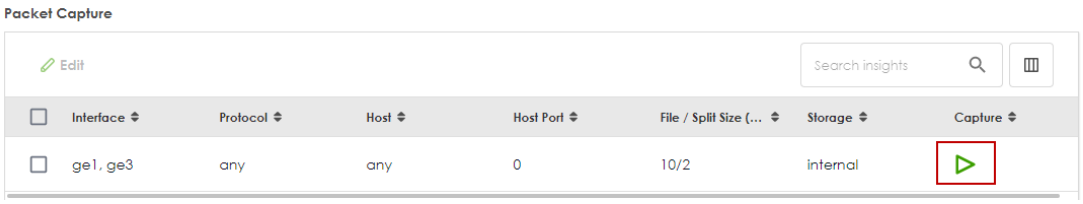


7. In Filter, select IP Version for which to capture packets. Select any to capture packets for all IP versions.
   Select the Protocol Type of traffic for which to capture packets. Select any to capture packets for all types of traffic.
   Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

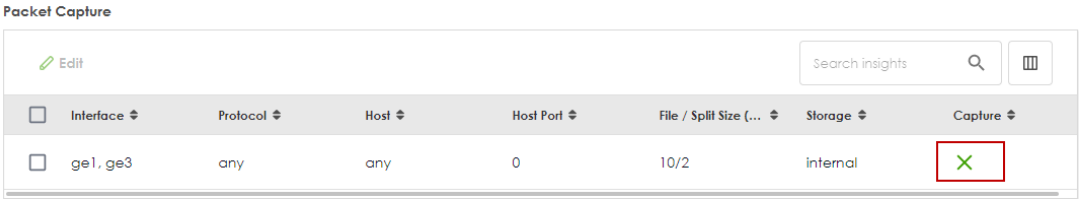
8. In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".



9. Click the icon to start capturing packets.

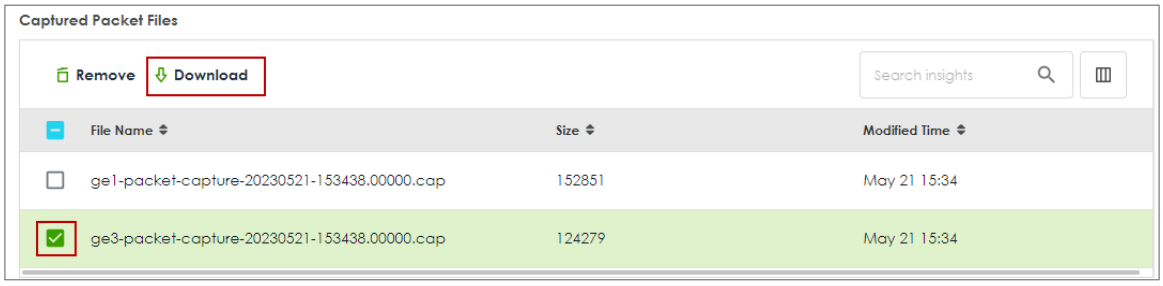


10. Click the icon to stop capturing packets.



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 sniffer and analyze network traffic by intercepting and displaying packets transmitted in the network interface.

Syntax:

cmd traffic-capture <interface name>

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

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

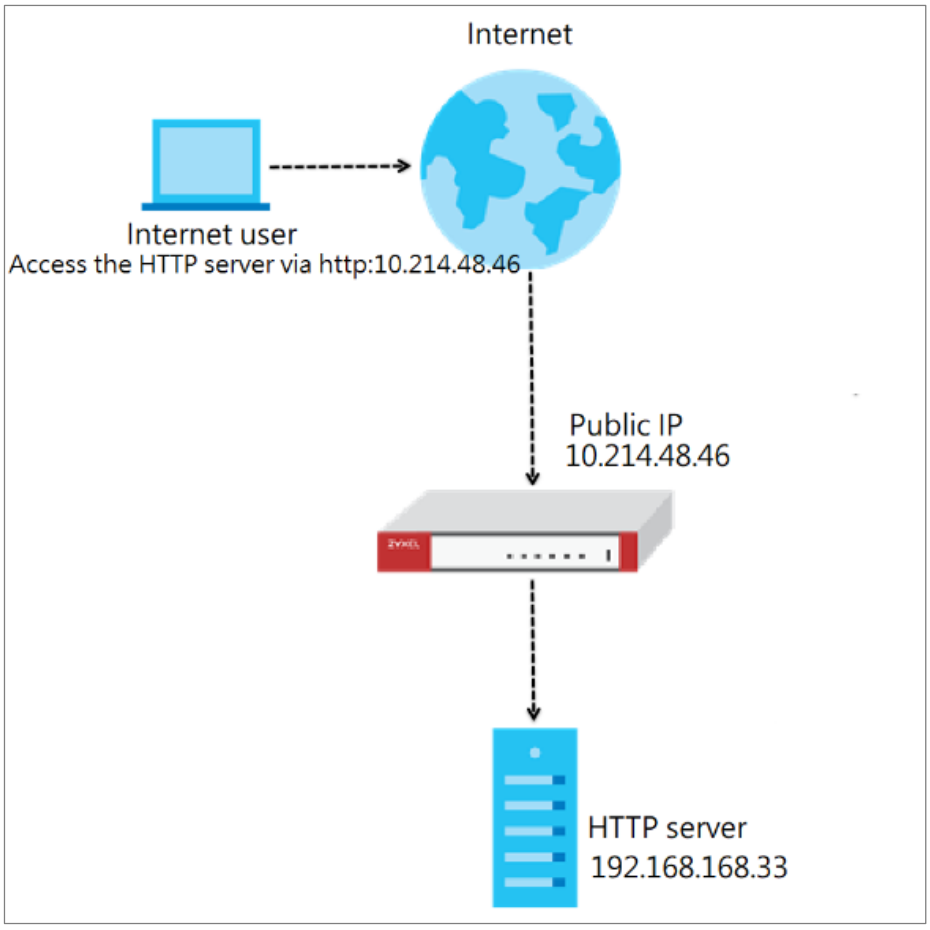
cmd traffic-capture <interface name> filter “port <port number>”

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

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


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

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



Set Up the NAT

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

- Input the rule name

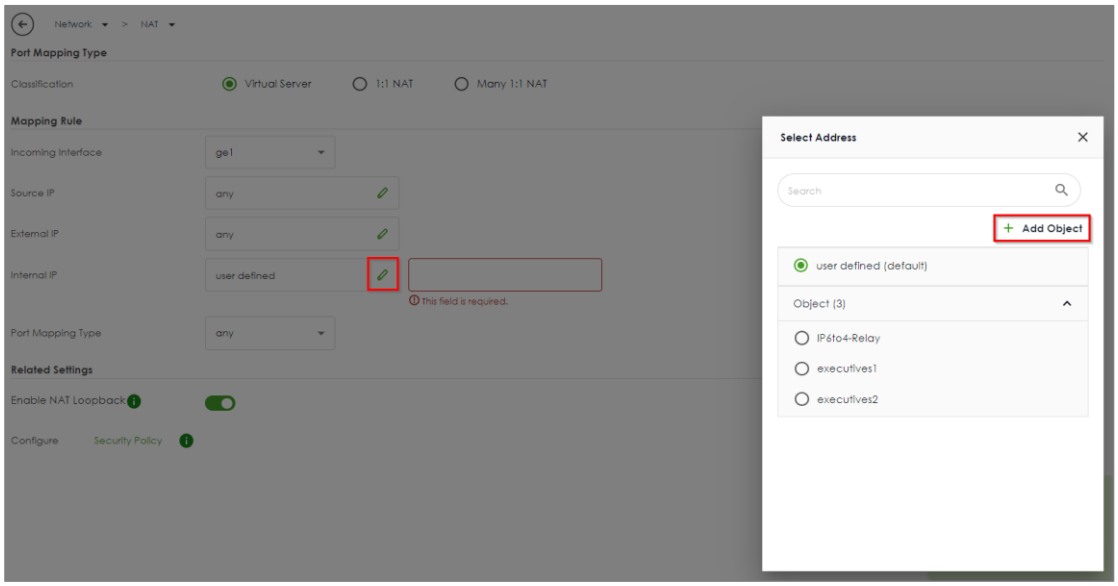
- select Virtual Server

- Incoming Interface: ge1

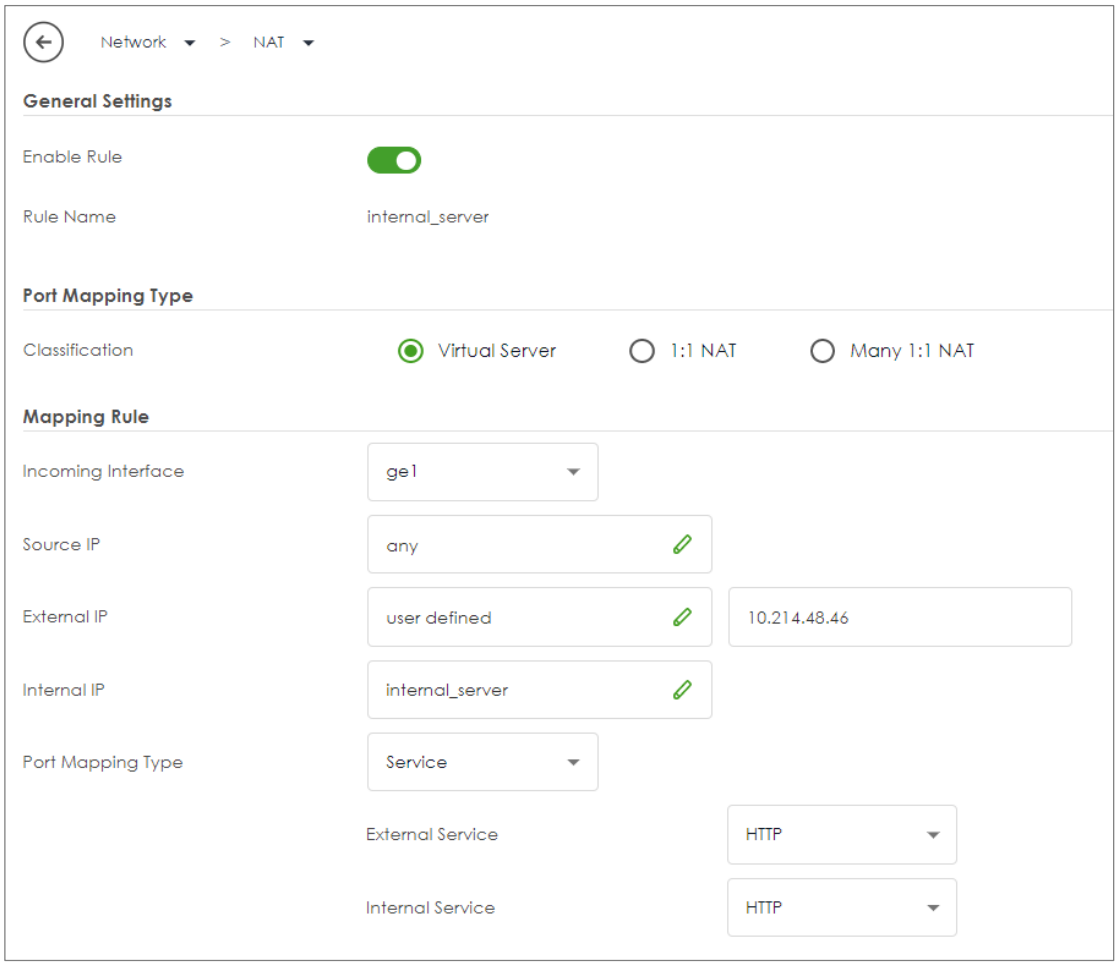
- Configure the Source IP to limit the access by the Source IP. You may select Any

- Configure the External IP. Select Any to choose the ge1 interface IP as the external IP.

- Configure the internal IP. Click +Add Object to create an address object as a host 192.168.168.33 which is the IP address of the internal server.

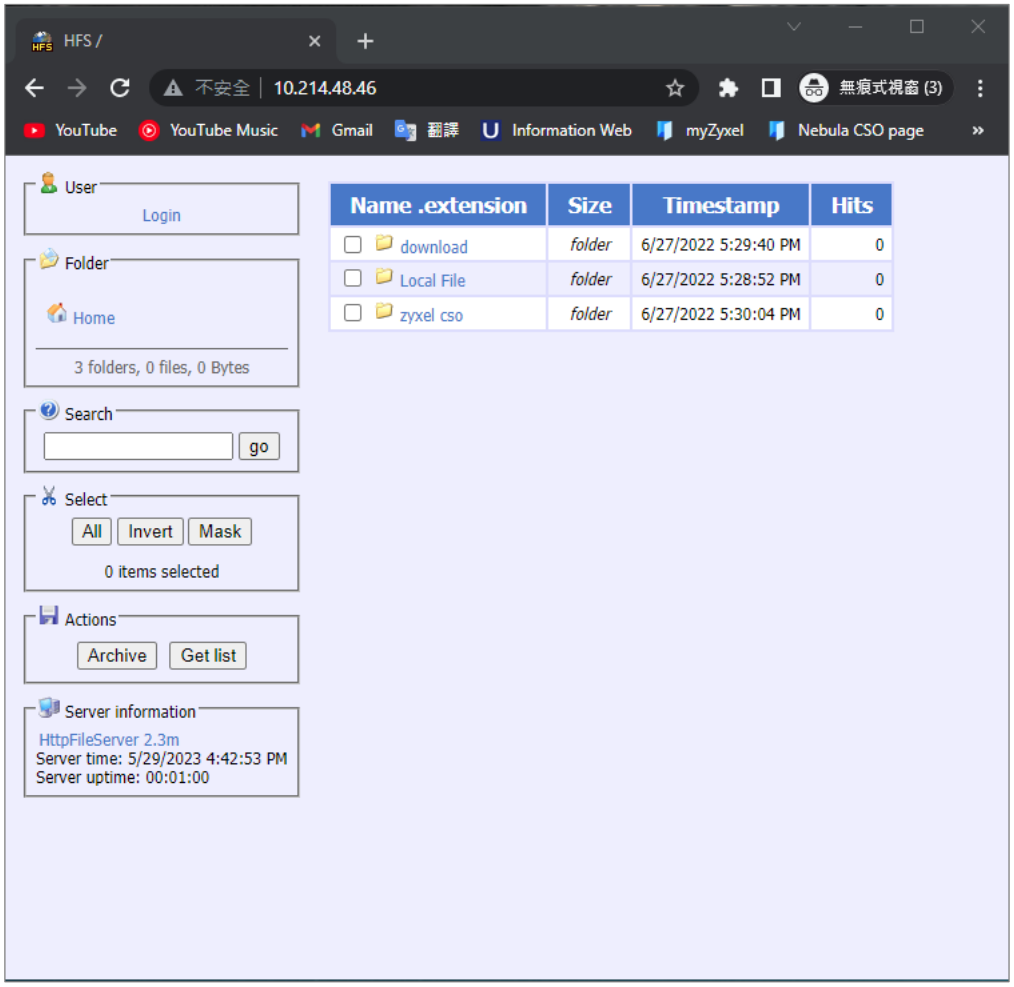


- Port Mapping Type: Select HTTP for both external and internal service.



Test the Result

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

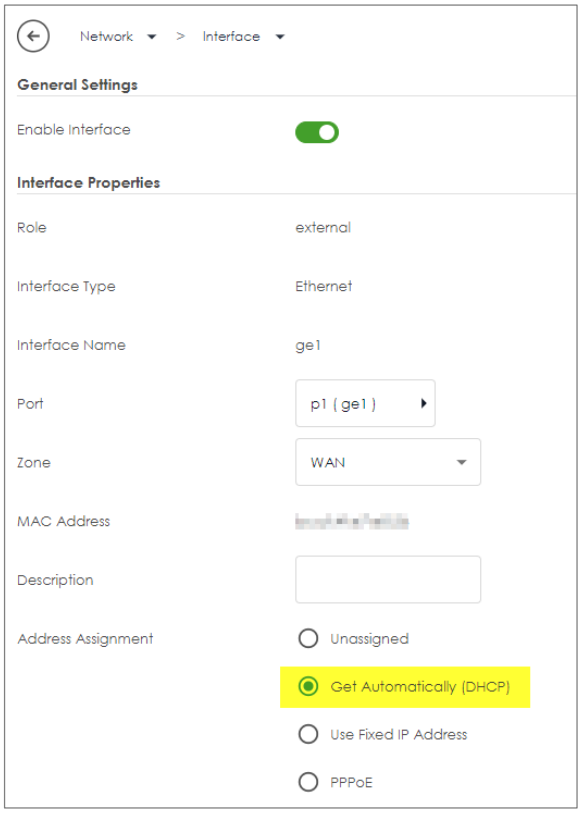


How to Configure DHCP Option 60 – Vendor Class Identifier

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

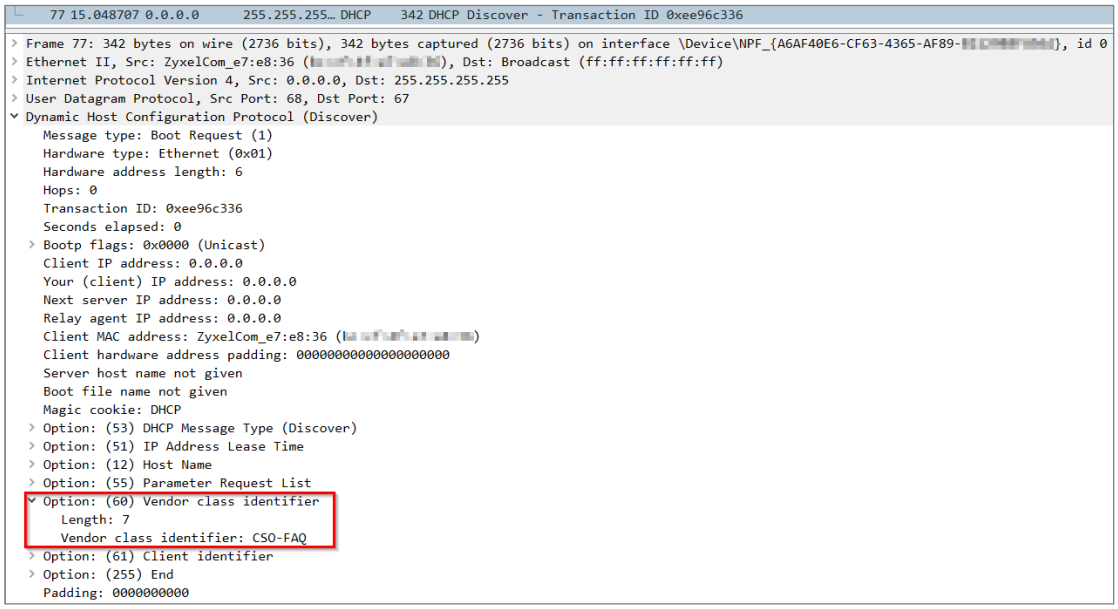
1. Go to Network > Interface > External, and edit the WAN interface.
2. Make sure the WAN interface is set as a DHCP client. Select **Get Automatically (DHCP)** for Address Assignment.



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**

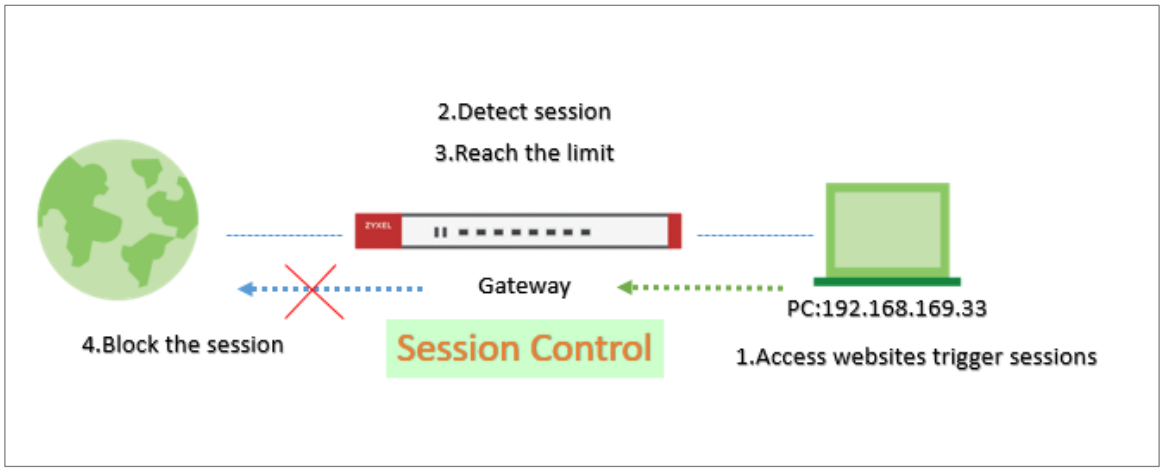
Test DHCP Option 60

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.



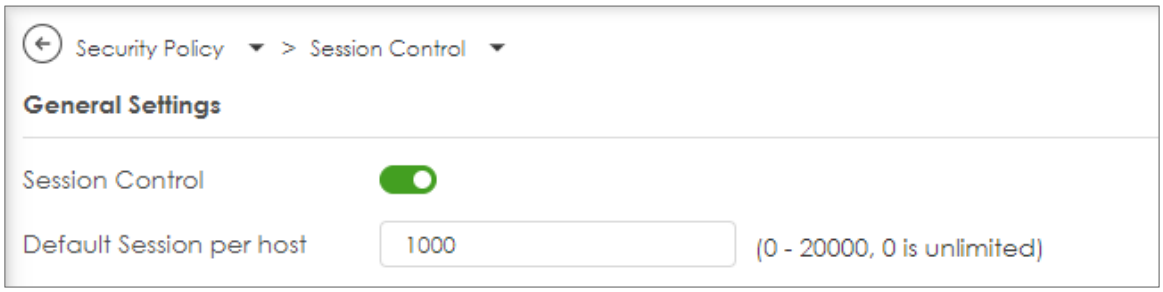
How to Configure Session Control

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.

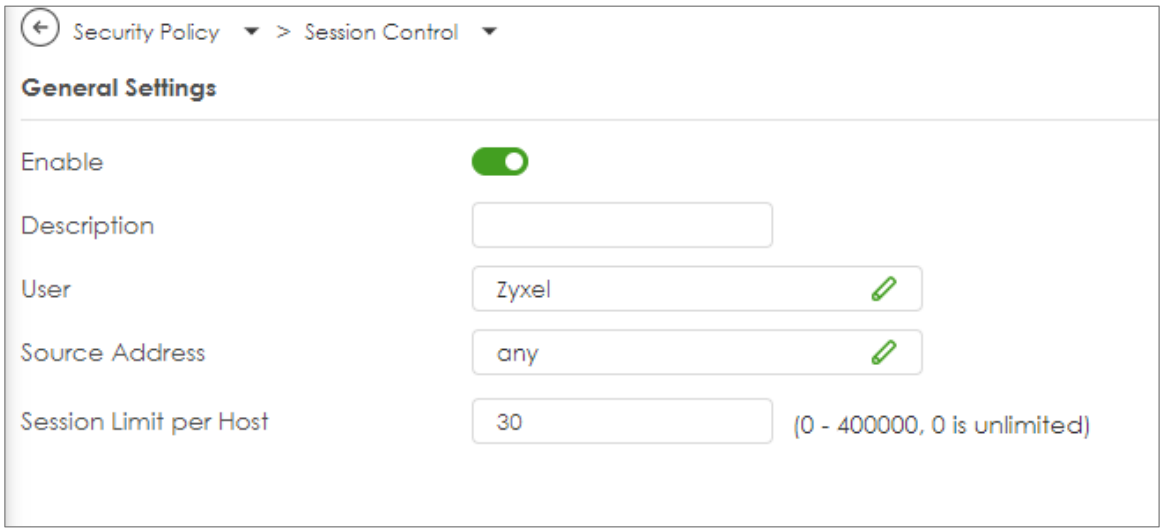


You can field in the value of the Session per hosts you would like to limit.

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

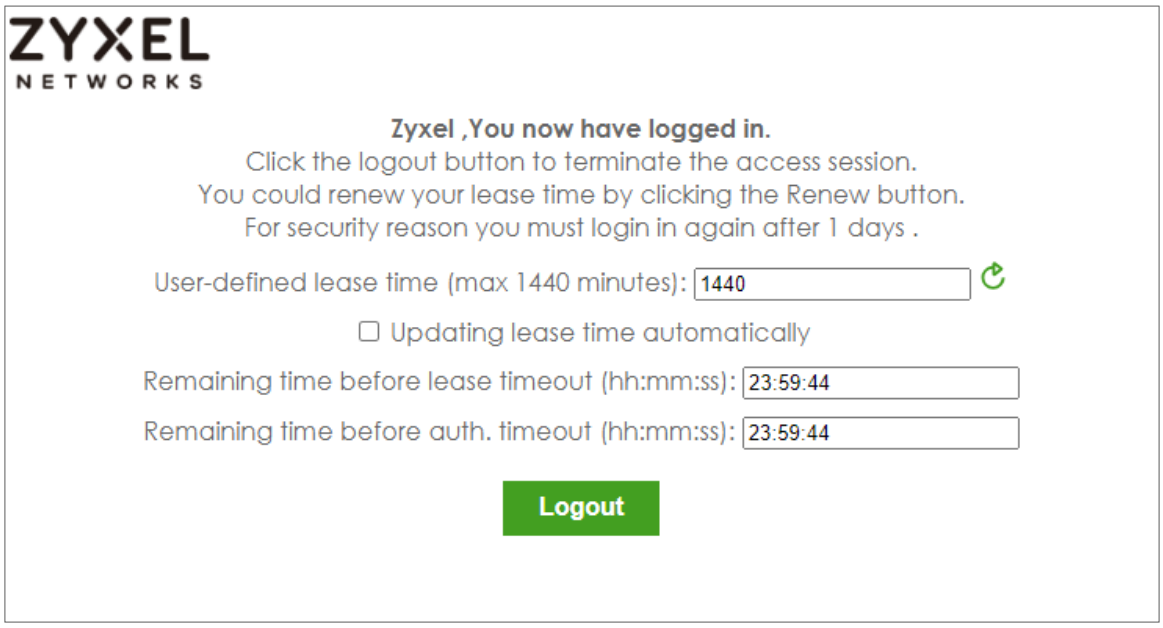
To limit a user's session. You can set up specific rules for each user

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



Test the Result

Log in as User: Zyxel



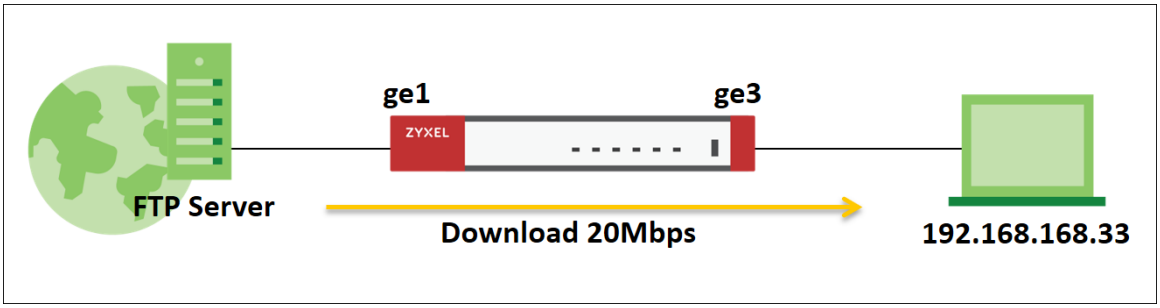
Try to access web browser to hit the session limit

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

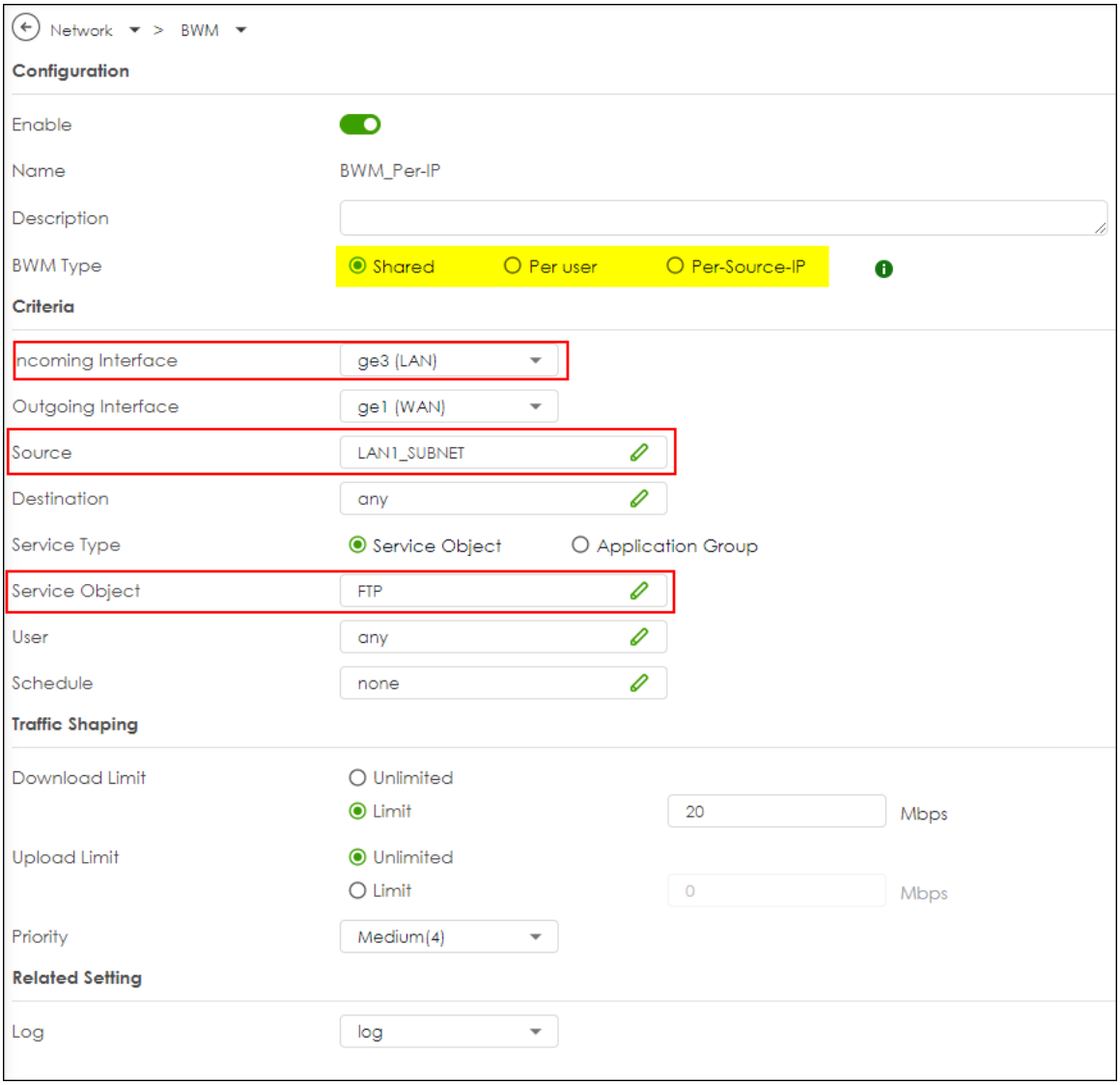
This example illustrates how to use USG Bandwidth Management (BWM) for controlling FTP traffic bandwidth allocation. By specifying criteria such as incoming interface, outgoing interface, source address, destination address, service objects, application group, and user, you can create a sequence of conditions 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.



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.

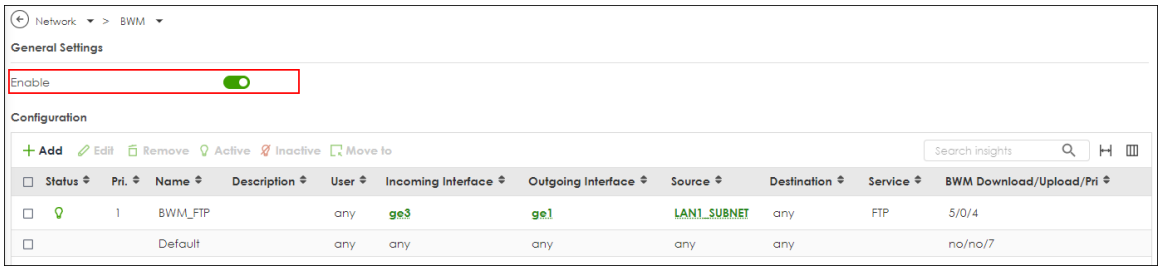
(3) Per-Source-IP

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.

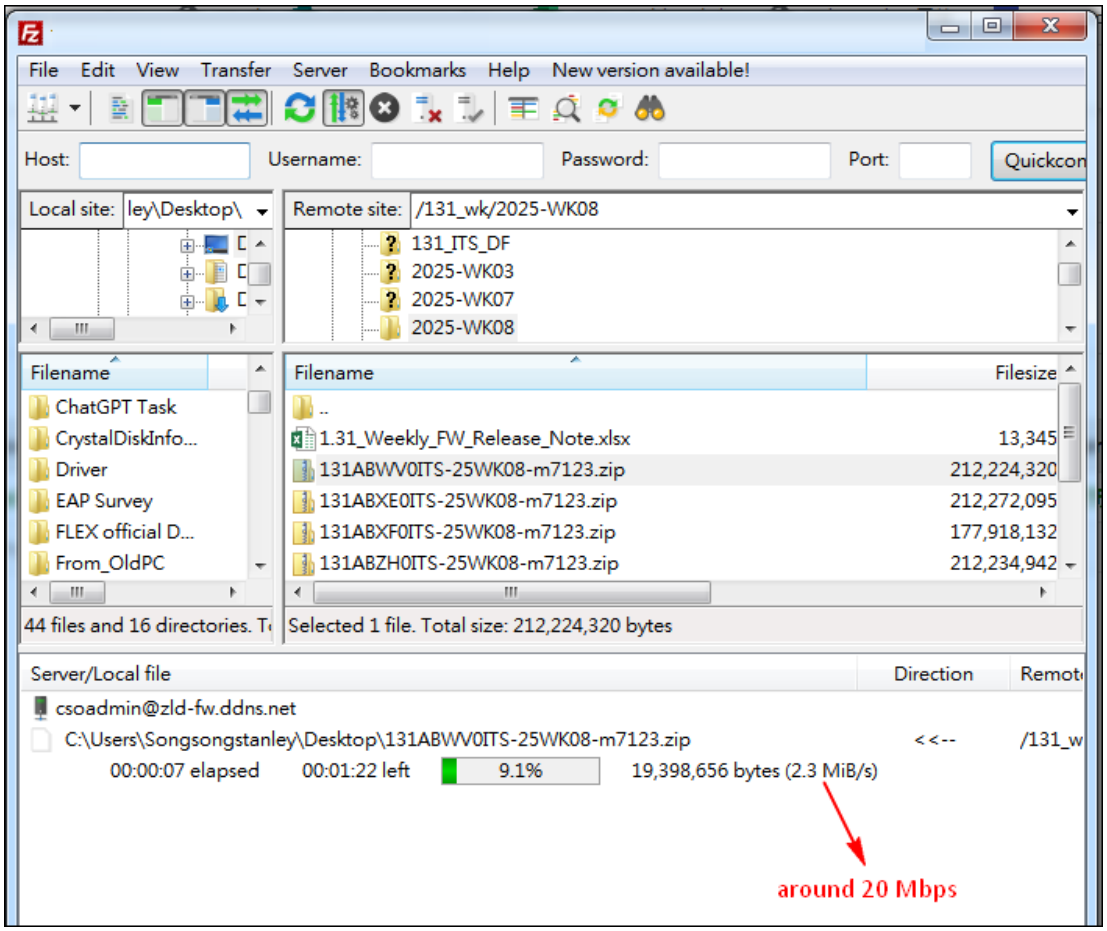
Note: If you select the “Per User” option or configure “User” as a condition, the Captive Portal service must be enabled, and the PC must be authenticated by the firewall first.

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

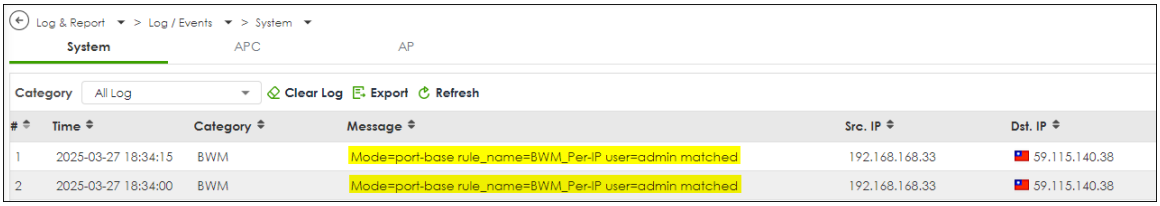


Test the Result

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

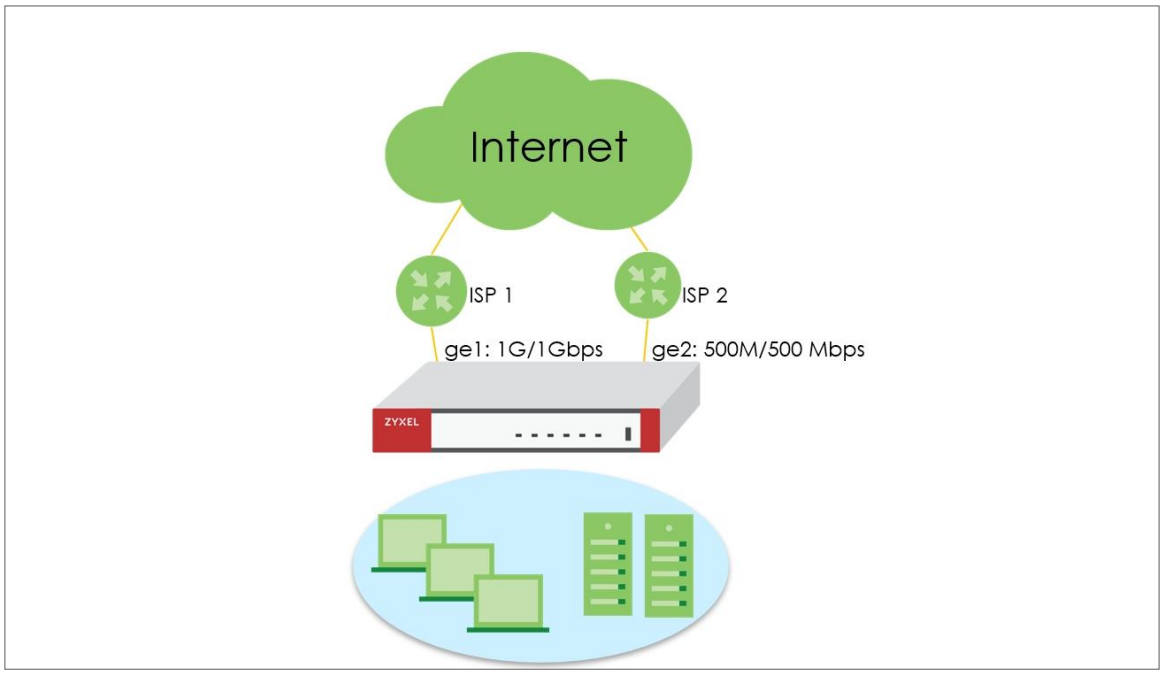


Go to Log & Report > Log/Events and select BWM to check the logs.



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.

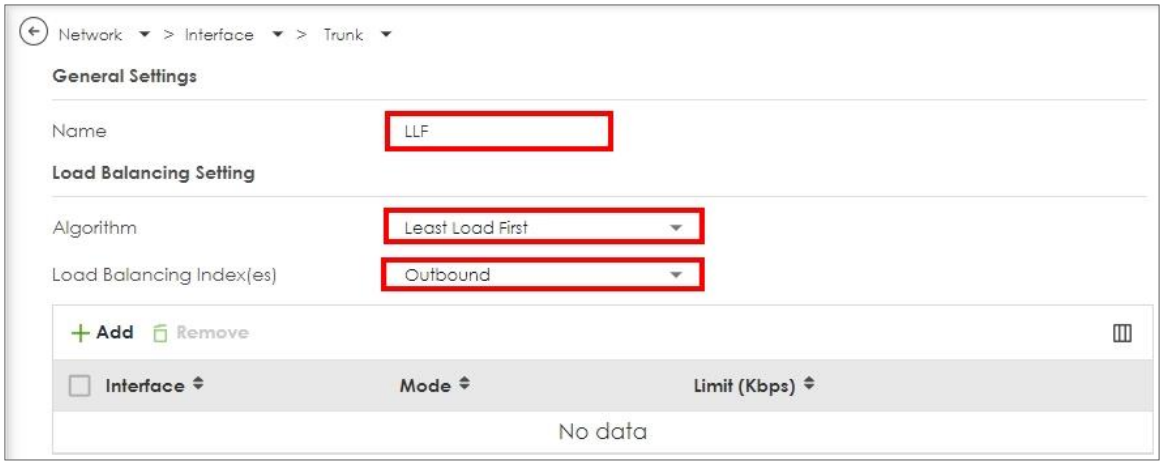
Spillover

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.*



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

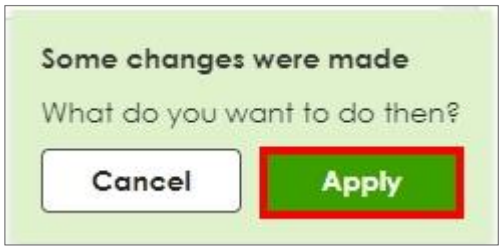
Limit(Kbps): 1024000

Member: ge2(Wan)

Mode: Active

Limit(Kbps): 512000

Click **Apply** to save changes.



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

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

Algorithm: Spillover

Load Balancing Index: Outbound

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

Member: ge1(Wan)

Mode: Active

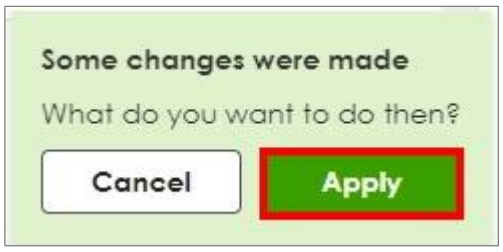
Limit(Kbps): 819200

Member: ge2(Wan)

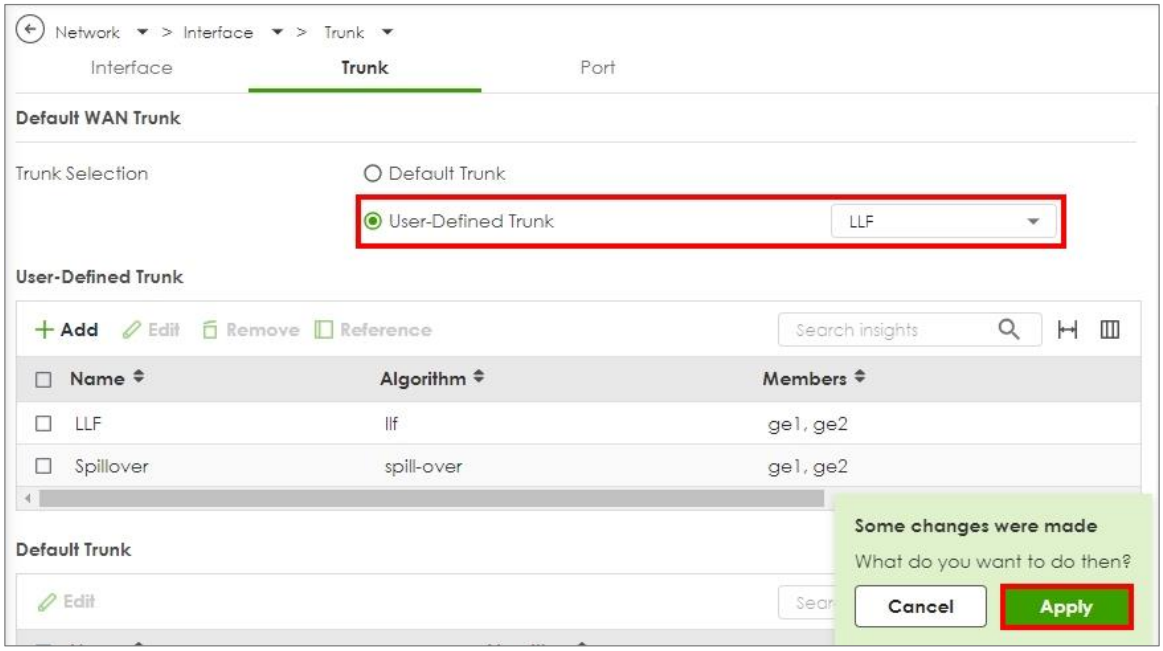
Mode: Active

Limit(Kbps): 512000

Click **Apply** to save changes.



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.



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.

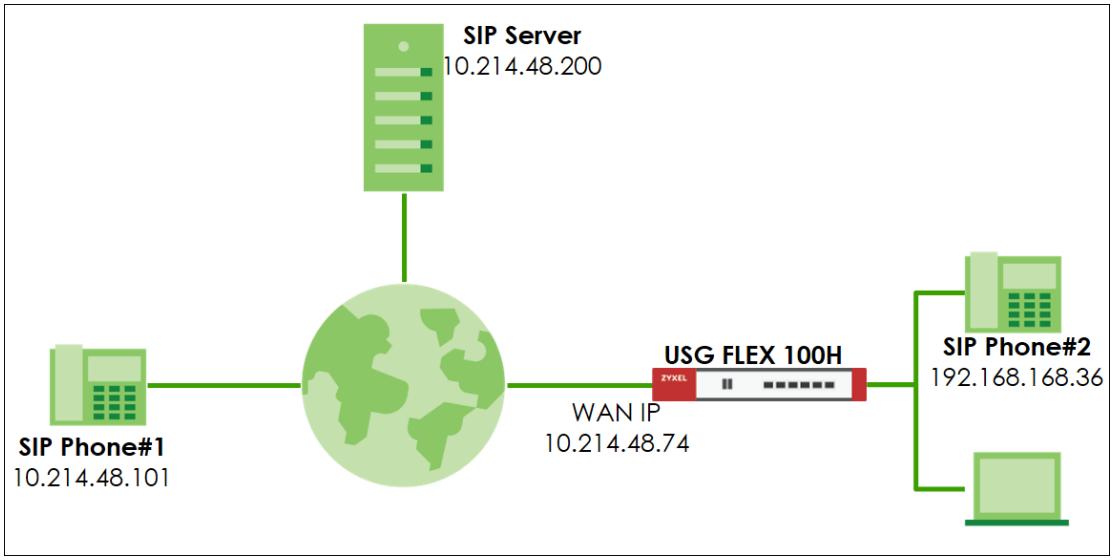
4) Host B generates ICMP traffic to 8.8.8.8.

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?

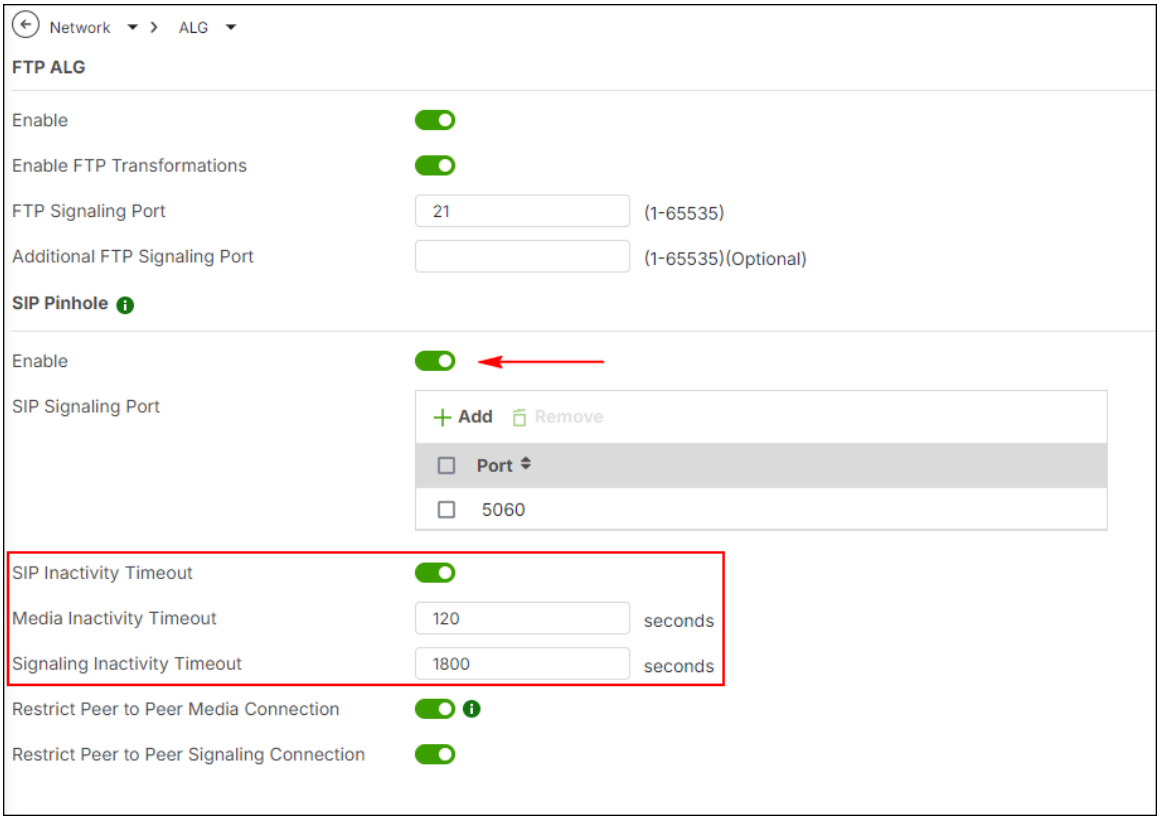
SIP pinholes ensure the persistence of registered SIP sessions and RTP sessions during NAT operations. This prevents issues such as dropped calls or non-functioning phone calls caused by expired SIP/RTP sessions on the firewall.

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.

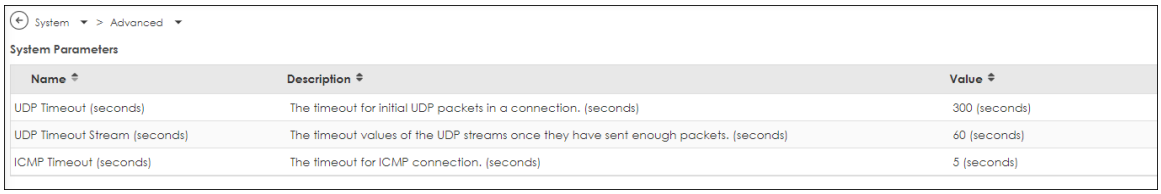


SIP Signaling port:

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)



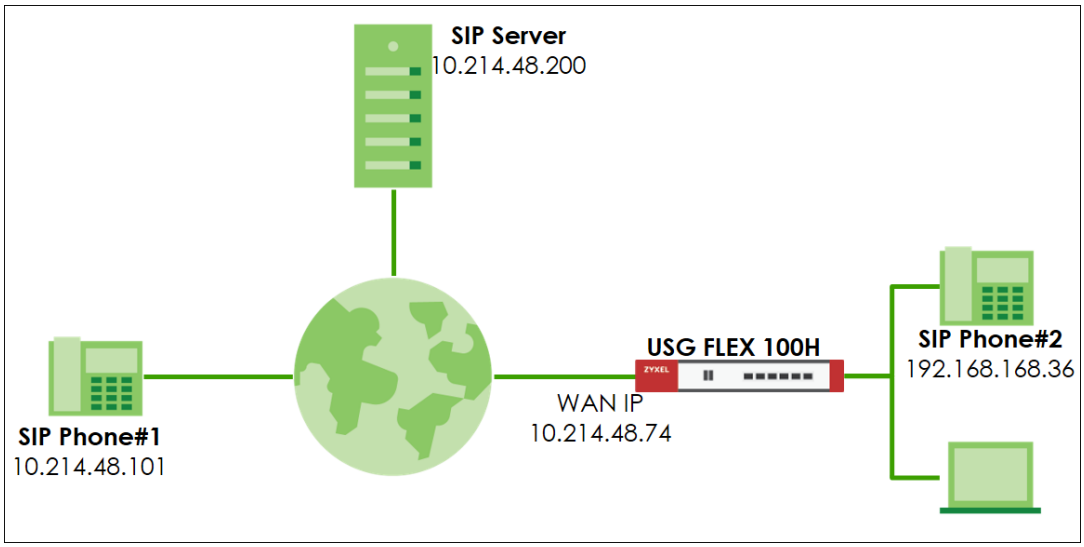
You can configure Media(RTP) and Signaling(SIP) timeout for your SIP phone, it could keep the sessions on firewall to prevent lost incoming phone call due to session expired.

Peer to Peer connection restriction:

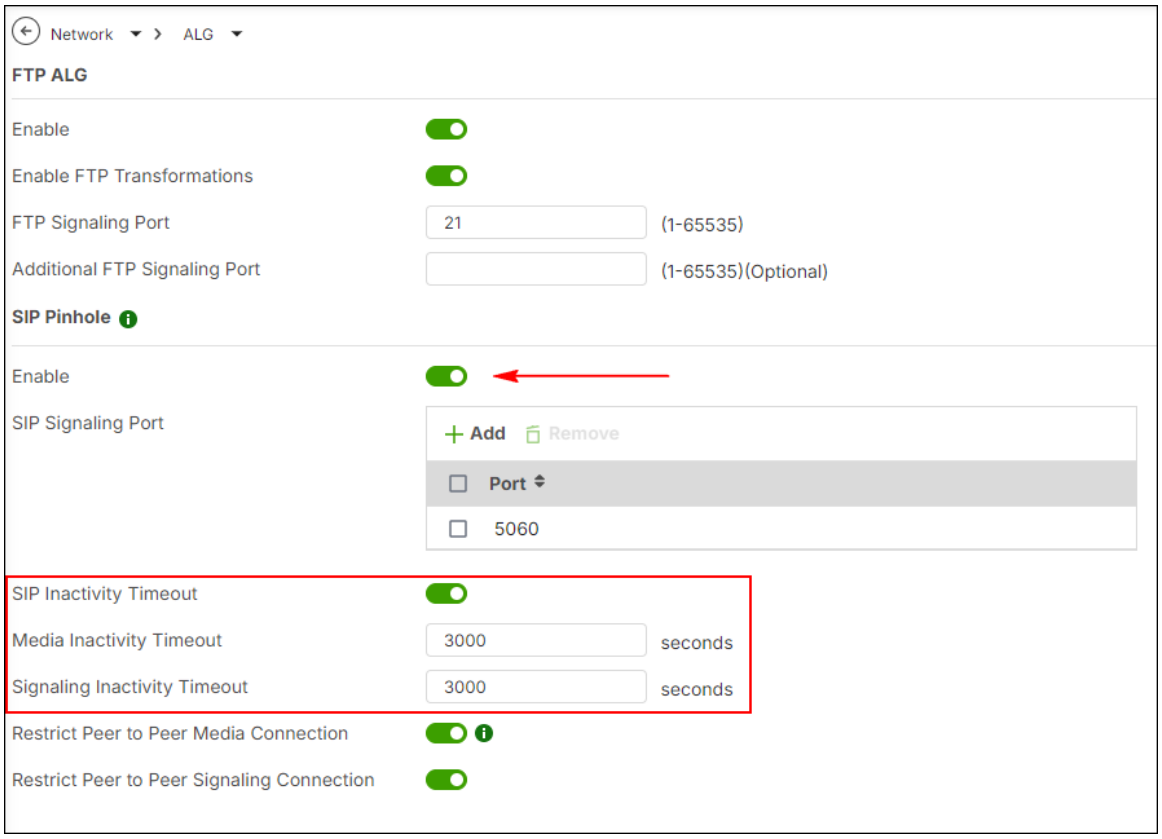
It is for incoming STP/RTP traffic. If the source IP address doesn't match to exist sessions, then firewall will drop the incoming traffic.

Test the Result

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



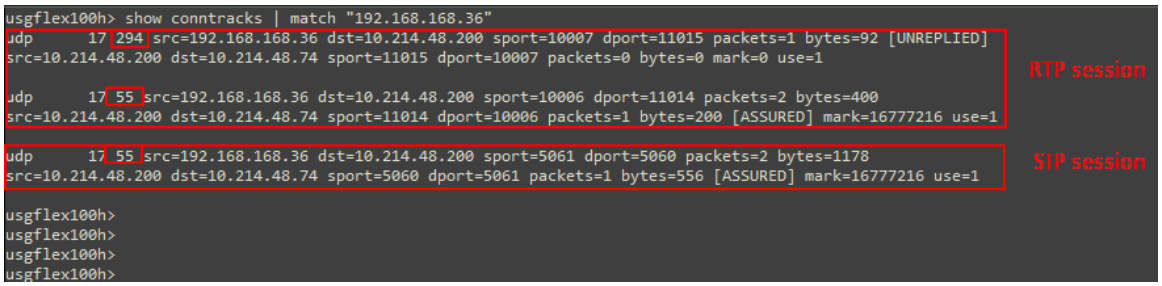
Turn on SIP ALG feature and enable “SIP Inactivity Timeout” service, also have an extend Signaling(SIP) and Media(RTP) inactivity timeout as 3000 seconds.



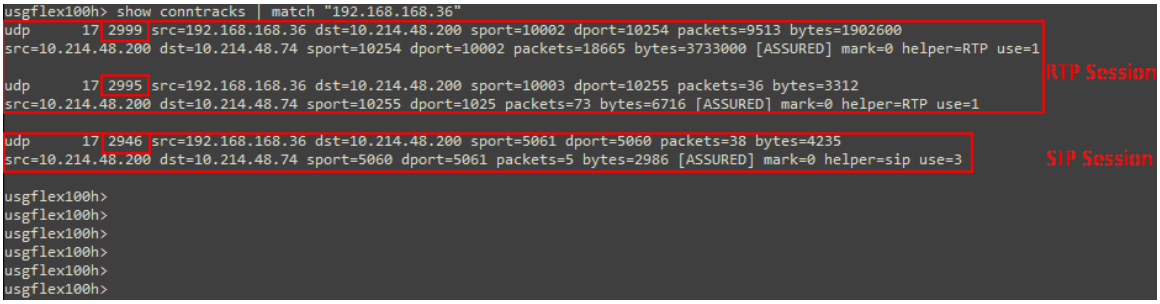
Use CLI command to check exist sessions has been extended successfully.

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

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

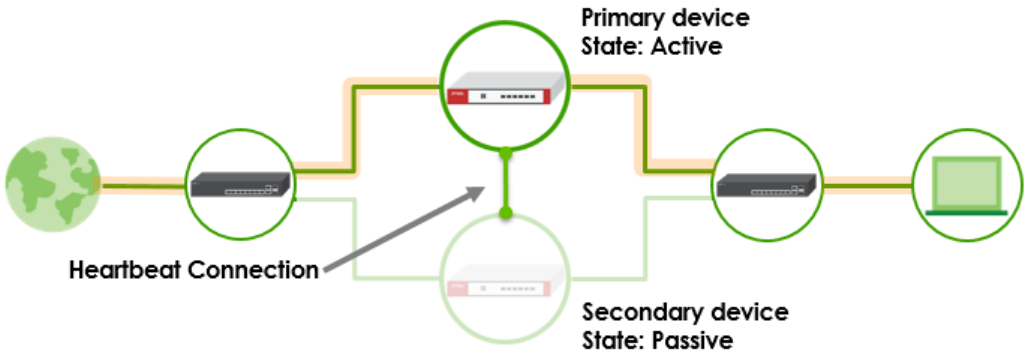


After enabling the SIP ALG feature, system will extend the timeout value.



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.

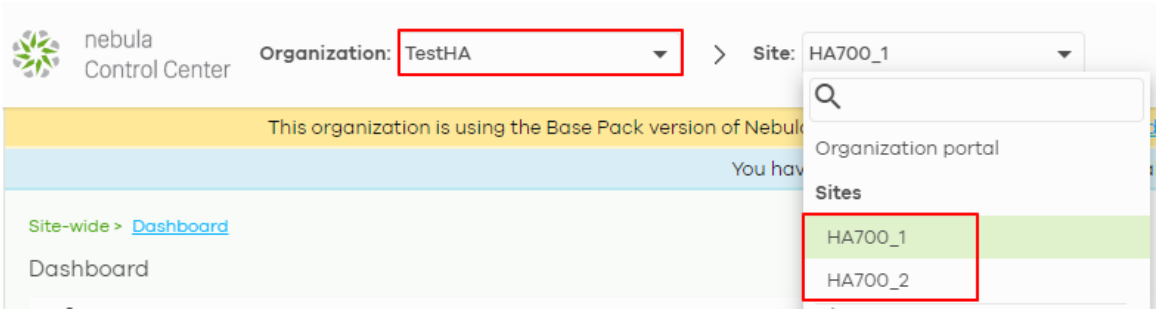


Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H.This example was tested using USG FLEX 200H (Firmware Version: uOS 1.35).

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.

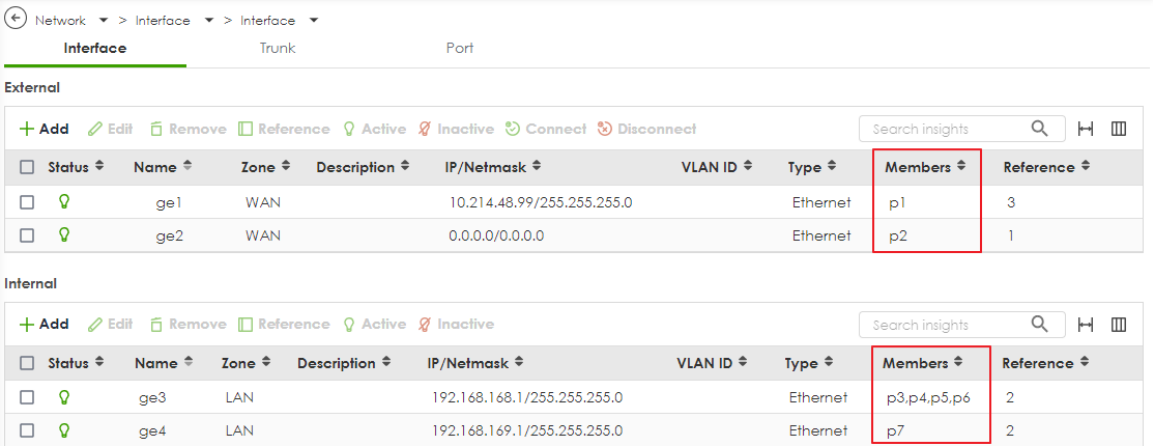
Note: It is highly recommended to complete device registration steps on Nebula before pairing HA.

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.

> Note: Heartbeat port for HA synchronization
>
> USG FLEX 200H/200HP: P8
>
> USG FLEX 500H/700H: P12

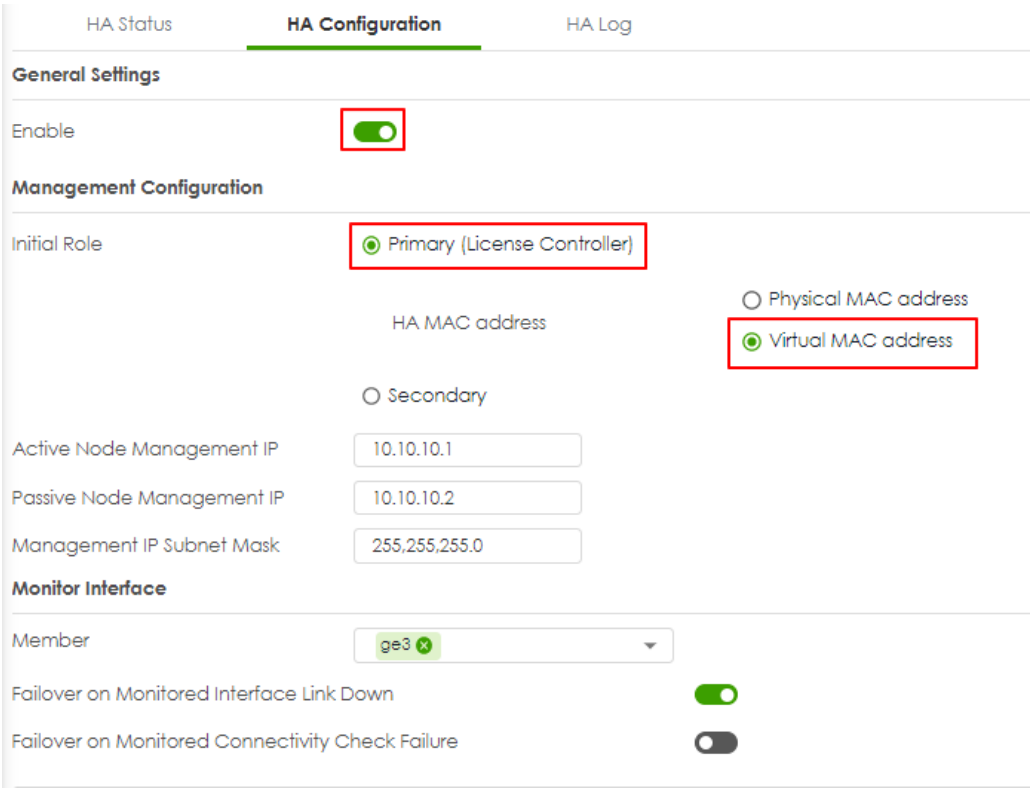
Go to Network > Interface and make sure p8 doesn't belong to any interface.



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.

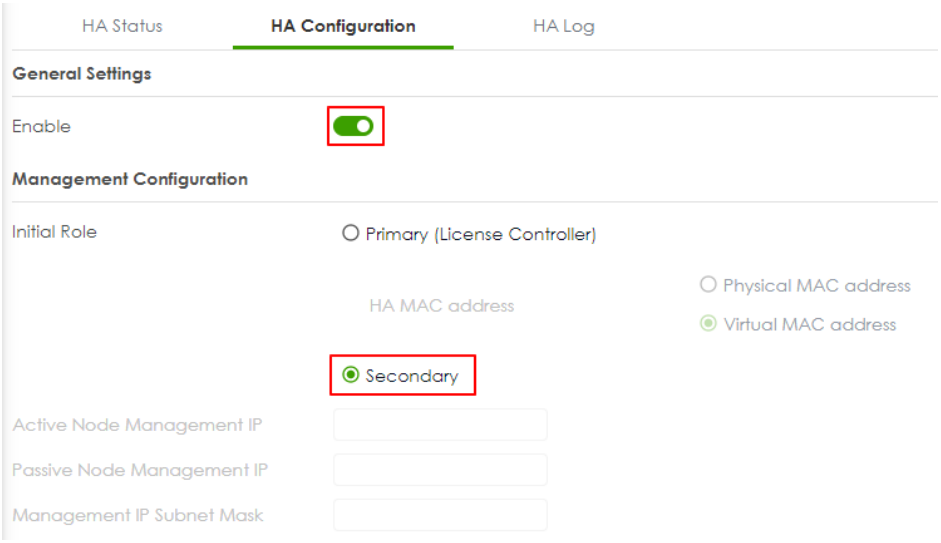
     D8:EC:E5:XX:XX:1D -> D**6**:EC:E5:XX:XX:1D
   - Configure Management IP for active and passive role. The two management IPs must be different but in the same subnet.
   - Select monitor interfaces. HA failover will be triggered when monitored interface is down. Turn on "**Enable**" to enable Device HA and Apply.



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.

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.



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.

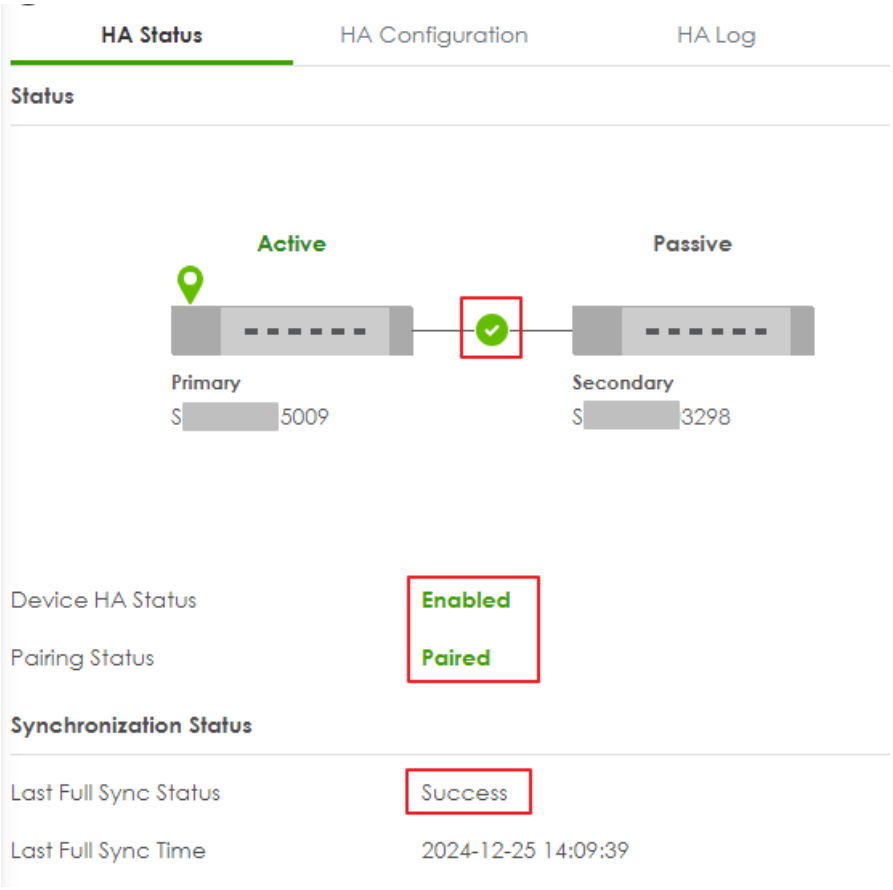
> Note: The heartbeat port of the primary and secondary device must be connected directly to each other (not through a switch).

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 paring status.

Pairing status: Paired

Last Full Sync Status: Success



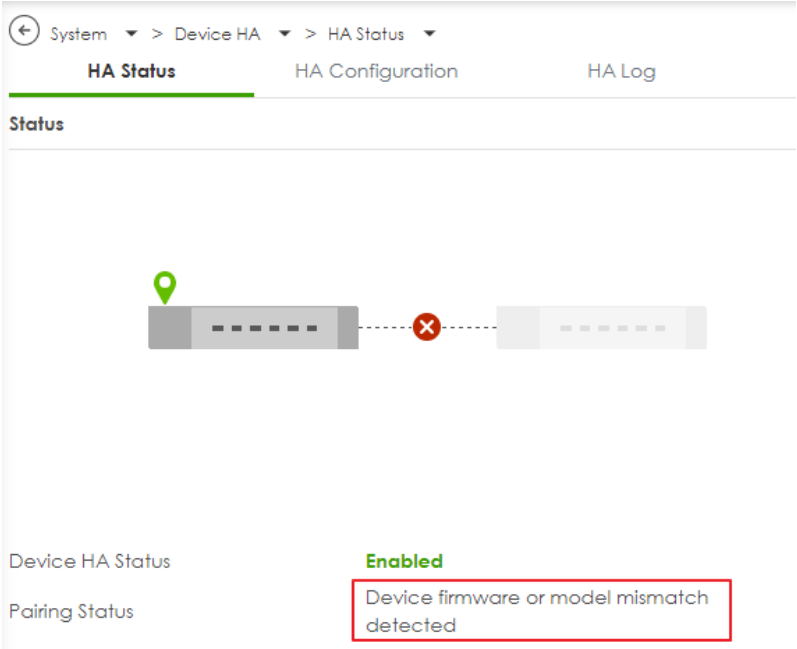
You can also enter the command on the primary device to check HA status.

usgflex200h> show state vrf main device-ha status

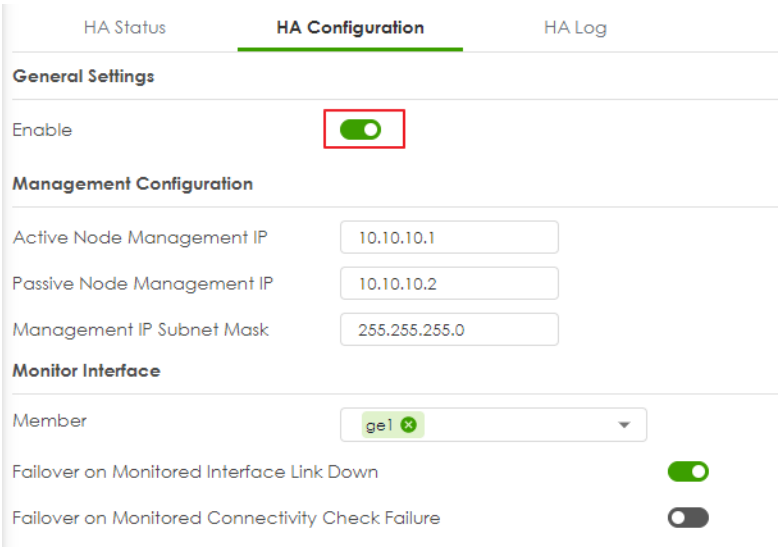
Synchronization can take up to 5 minutes or so. Once it has finished synchronizing, you can verify if the settings are synchronized by accessing the passive device through Passive Node Management IP. Once pairing is complete, the secondary device's license will automatically be transferred to the primary 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      5009
        icon-color on
        ..
    passive
        role secondary
        sn S22      3298
        icon-color on
        ..
    ..
```

If Paring Status is not "Paired", check what the error message is and resolve the error. In this example, the error is "Device firmware mismatch". Check the firmware version on primary and secondary again and make sure firmware version on both devices are identical.



Note: After the error is resolved (Upgrade two devices to the same firmware version), you can keep the heartbeat port connected on both devices, and disable and enable HA on the **primary** device to trigger pairing again.



HA Synchronization

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

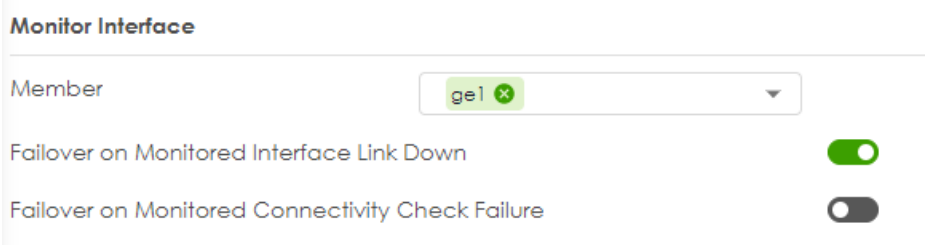
Note: All configuration changes must be made on the active device. Do NOT manually configure the passive device.

Connect the network cables to the secondary device

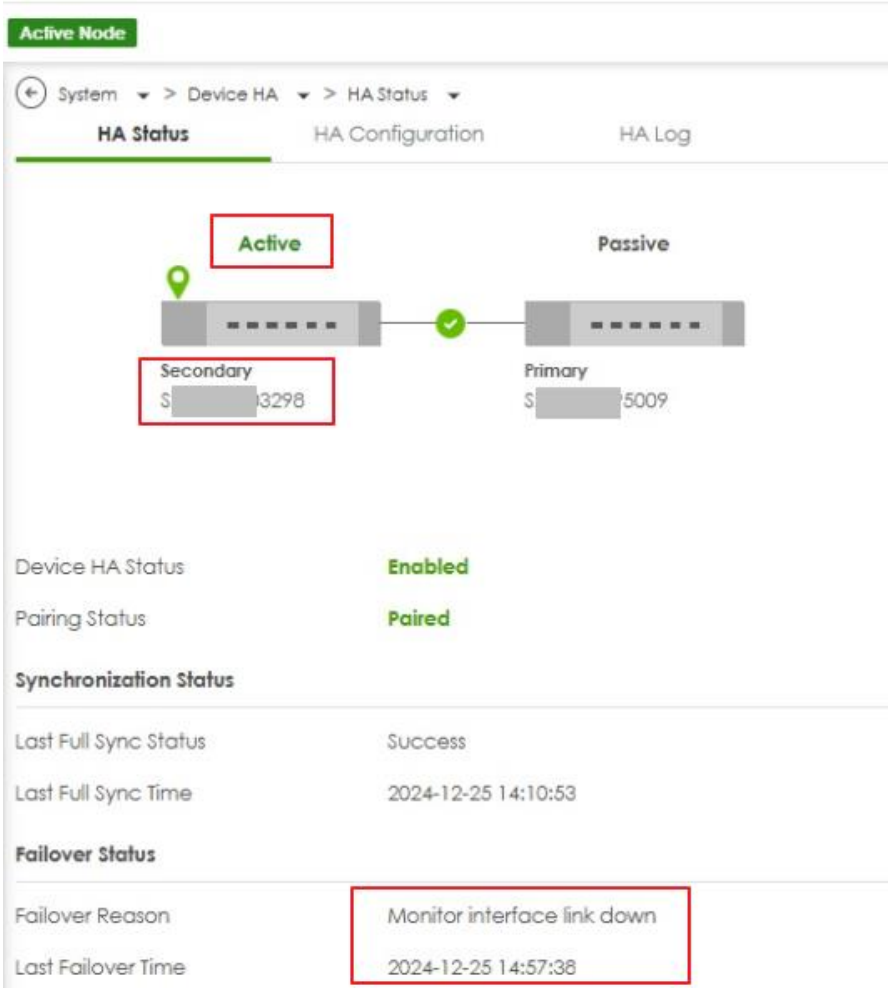
Once the devices have been properly synchronized, connect all network cables to wan and lan interfaces of the secondary devices.

Test HA Failover

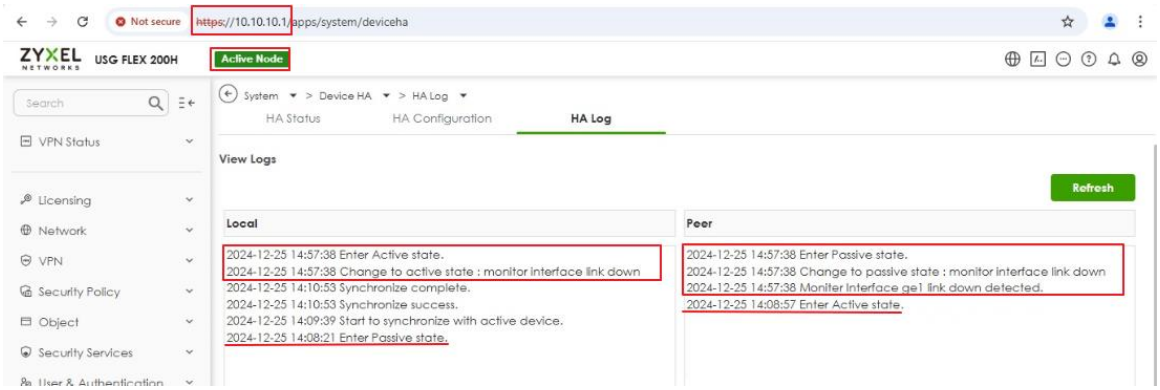
1. In this example, ge1 is the monitored interface. Unplug the Ethernet cable of ge1 interface from the primary device to trigger HA failover.



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.



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

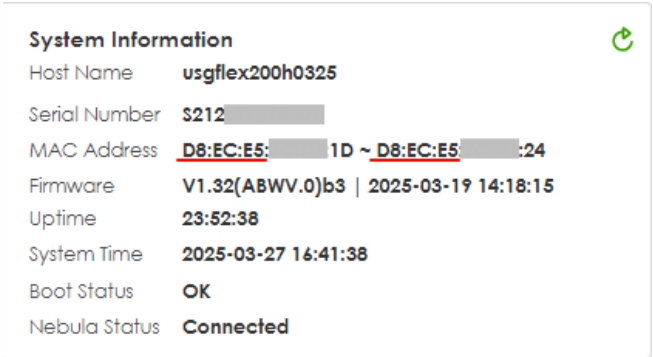


3. To prevent excessive failover flapping, the firewall includes a mechanism. By default, the Device HA failover count limit is 5. When this failover count reaches limitation, failover will be stopped. The failover count automatically resets every 5 days. You can use the command to check the failover count.
   usgflex200h> show state vrf main device-ha summary

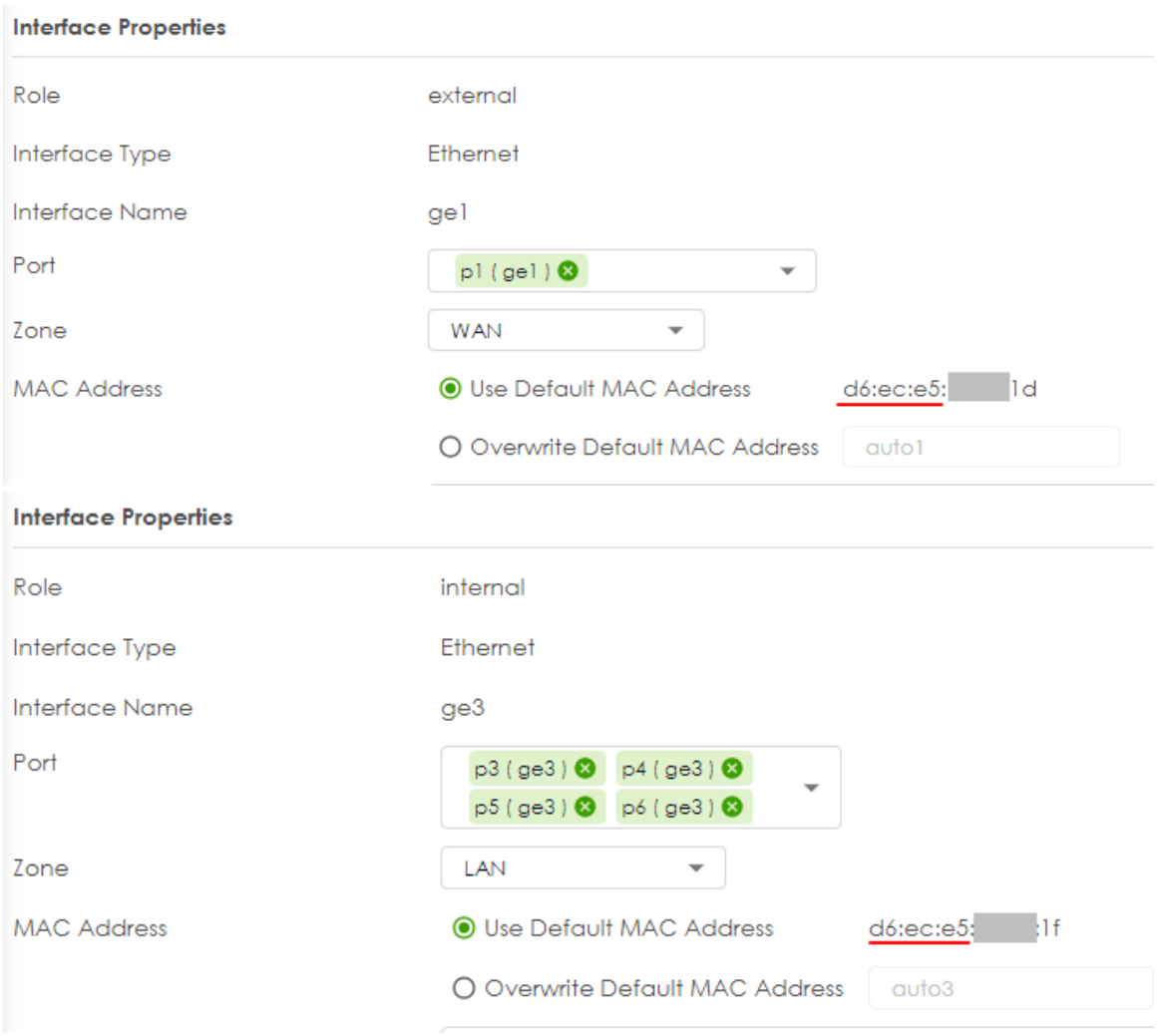
Check Virtual MAC Address

Active Device

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



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

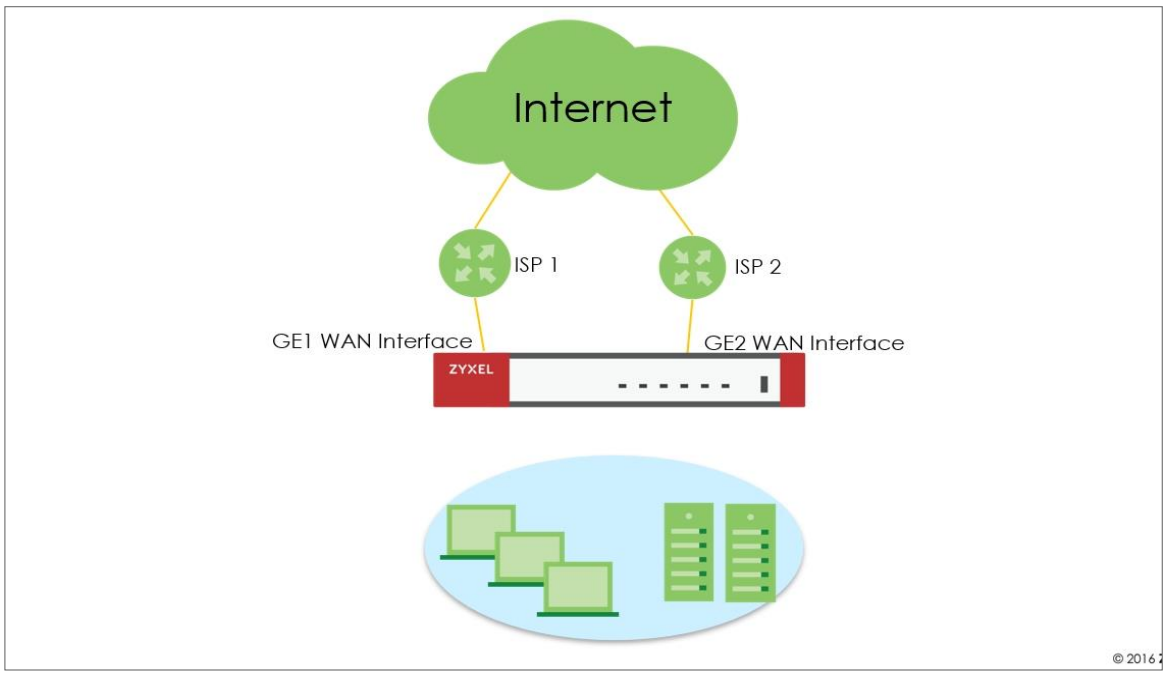


SYS LED Status

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

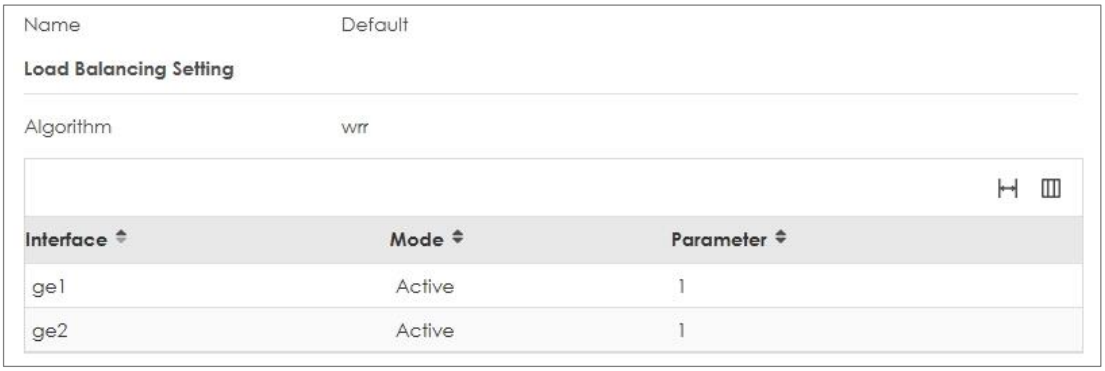
The Packet Flow Explorer is a powerful tool for analyzing and understanding routing-related issues. When used correctly, it offers a basic overview of your firewall's configuration without requiring an in-depth examination. This example demonstrates how to check the routing and SNAT status using the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



2. A static route is configured to route traffic to 8.8.8.8 from the GE2 WAN interface.

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

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
```

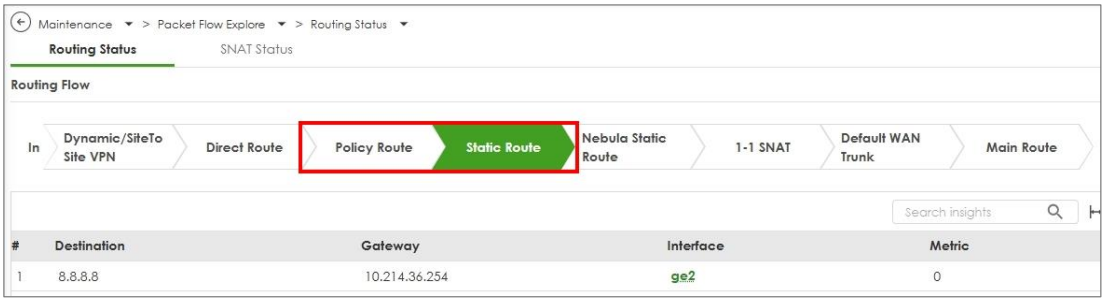
   We're unable to see packets to 8.8.8.8. Let's capture the packets on the GE1 WAN interface instead.

   cmd traffic-capture ge1 filter "host 8.8.8.8"

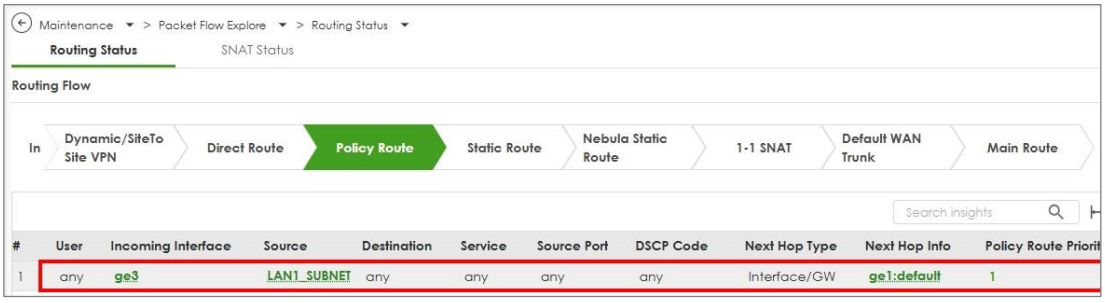
```
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:59:42.856870 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34317, lengt
09:59:42.862565 d2:ec:32:78:a1:18 > 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
09:59:43.869372 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34318, lengt
09:59:43.874648 d2:ec:32:78:a1:18 > 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
09:59:44.882064 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34319, lengt
09:59:44.886659 d2:ec:32:78:a1:18 > 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
09:59:45.895564 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34320, lengt
09:59:45.898654 d2:ec:32:78:a1:18 > 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
```

   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.

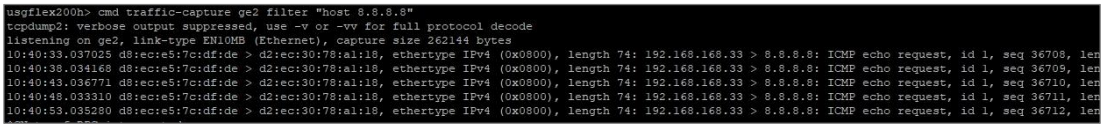


As we can see, the policy route has a higher priority than the static route, causing traffic to 8.8.8.8 to be affected by the policy route.

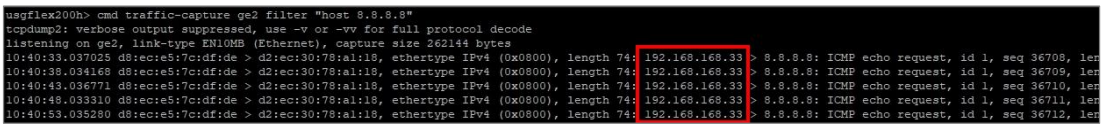


We can try temporarily disabling the policy route to see if traffic to 8.8.8.8 goes through the GE2 WAN interface.

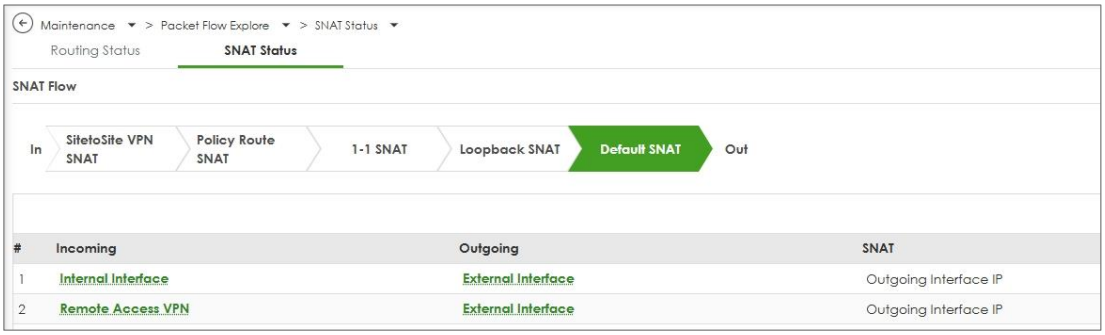
cmd traffic-capture ge2 filter "host 8.8.8.8"



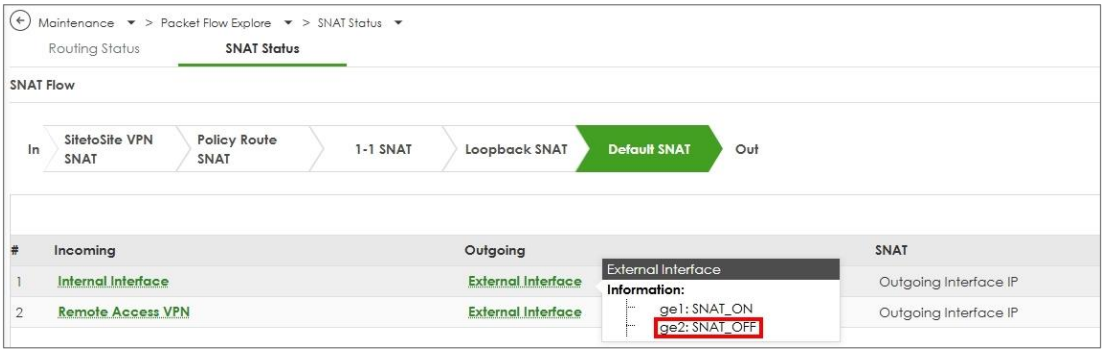
Now we can see the traffic to 8.8.8.8 appearing on the GE2 WAN interface. However, there is no ICMP response from the uplink router. Upon checking the source IP, it is the LAN host's IP, but it should be the GE2 WAN interface IP. The result shows that the firewall GE2 WAN interface does not have source NAT.



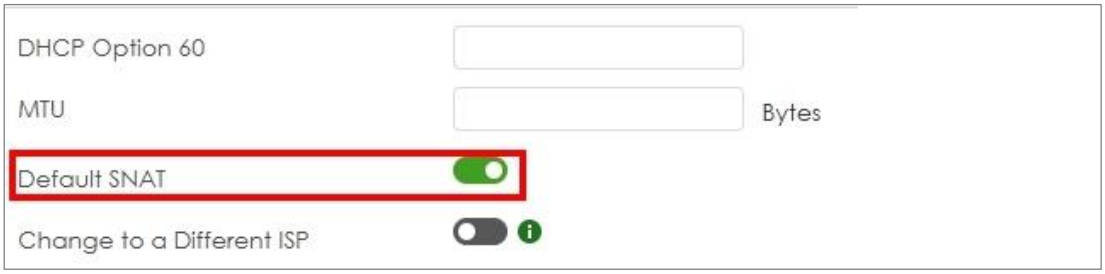
4. Go to ***"Maintenance > Packet Flow Explorer > SNAT Status"*** to check for possible issues.



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.



We can go to ***"Network > Interface > Interface"***, and double click ge2 to tick SNAT.



The above scenario is a simple example for checking routing and SNAT status in Packet Explorer.

Test the Result

Generate ICMP traffic from LAN hosts to 8.8.8.8 and confirm if the traffic is sent out through the GE2 WAN interface.

1. Run the command ***ping 8.8.8.8 -t*** in the Windows Command Prompt to check if it has an ICMP response from 8.8.8.8.

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

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=3ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
```

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

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
15:51:47.733935 d8:ec:e5:7c:df:de > d2:ec:30:78: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, lengt
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
15:51:48.751677 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, lengt
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, lengt
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, lengt
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, lengt
```


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.

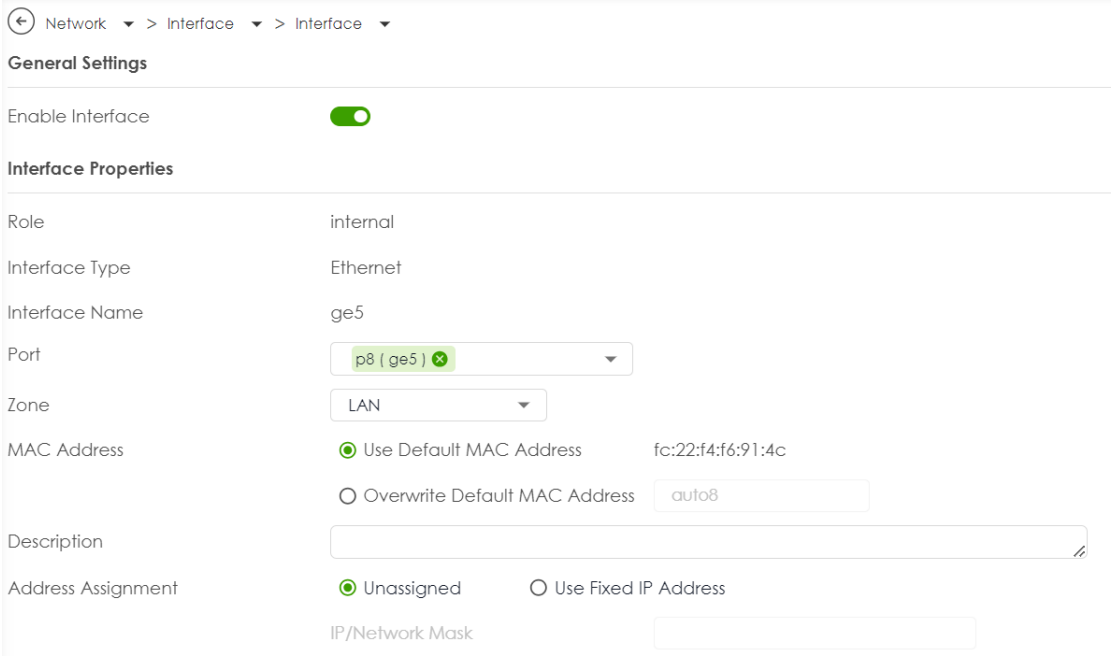
Prerequisites of Ethernet interface member

To be a member of LAG interface, the Ethernet interface must Meet all of the following conditions:

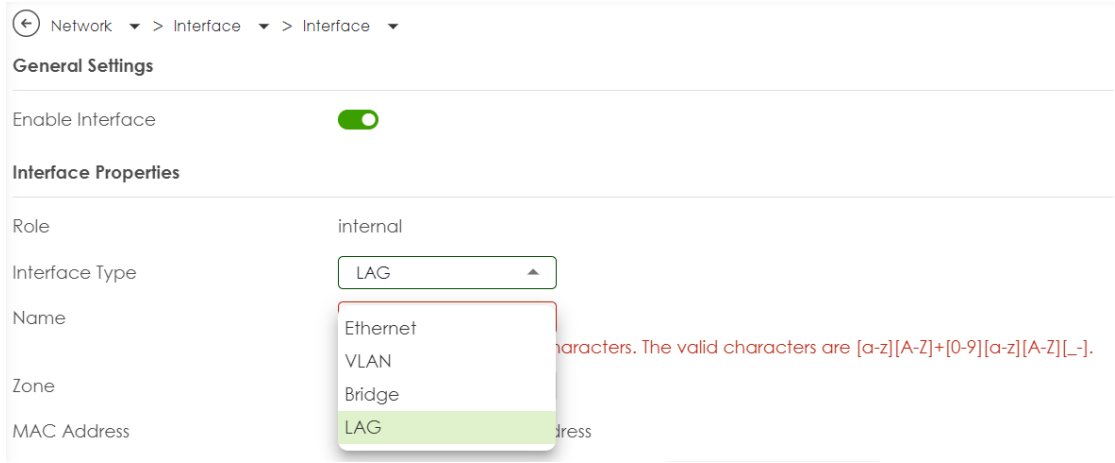
1. The Ethernet interface can only bind to one port. And the port cannot be used by other VLAN interface.
2. The Ethernet interface cannot be a member of other bridge, or LAG interface.
3. It does not have an IP address (must be set to unassigned).
4. It cannot have MAC address overwrite settings, must 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.



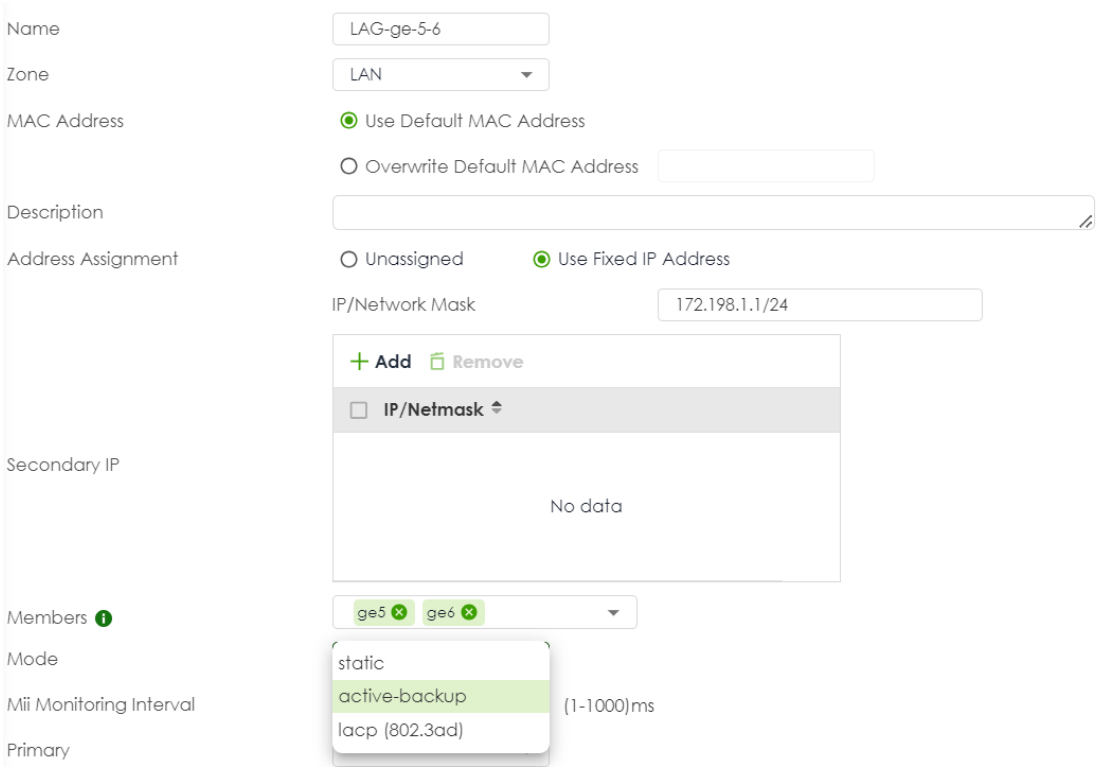
2. Click +Add to create an interface and select the Interface Type as LAG.



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

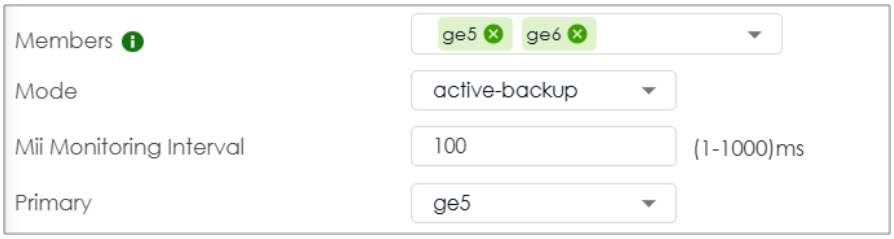


LAG mode: Active-Backup

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

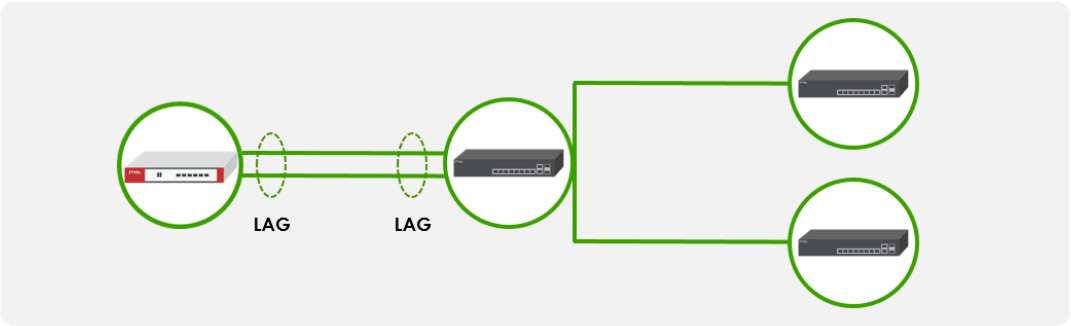
Primary: Allows you to specify which member interface should be preferred as the active link



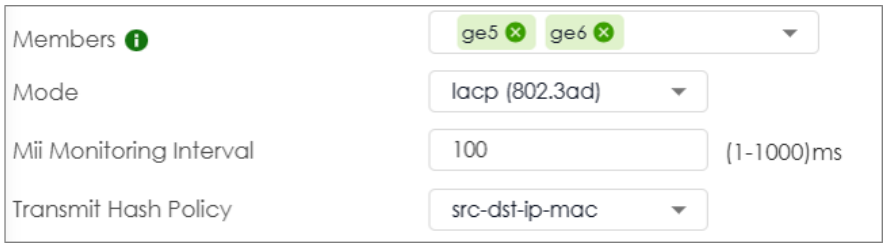
LAG mode: LACP (802.3ad)

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.



LAG Mode: Static

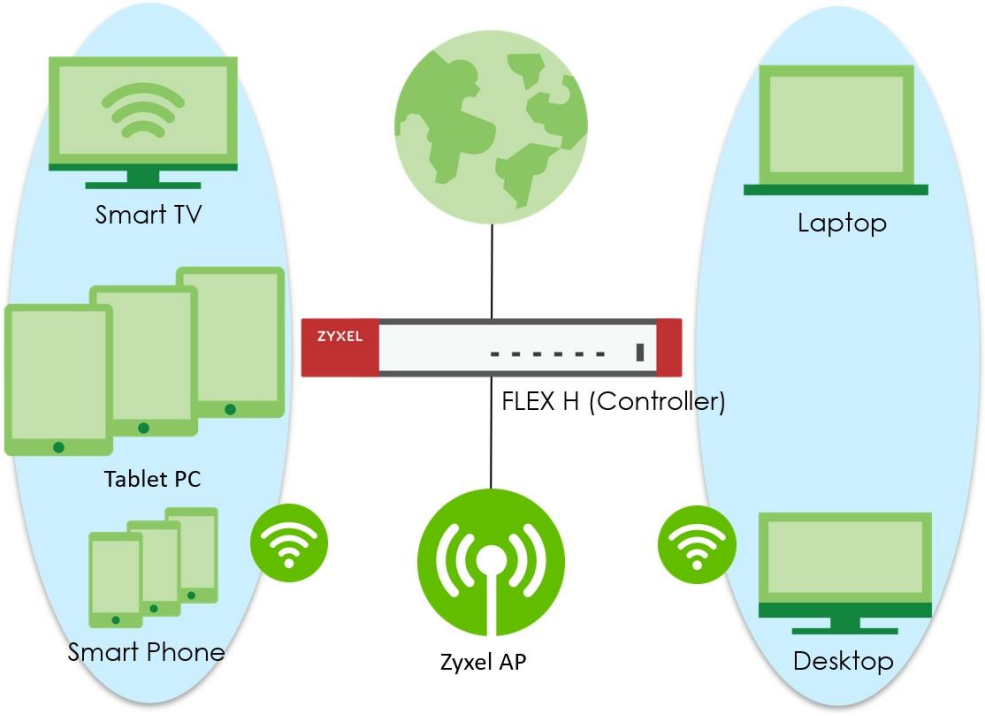
All ports in the LAG group will be always active for link failover and load balancing. The use case is when using legacy networking equipment that doesn't support LACP. When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall. 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.

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.

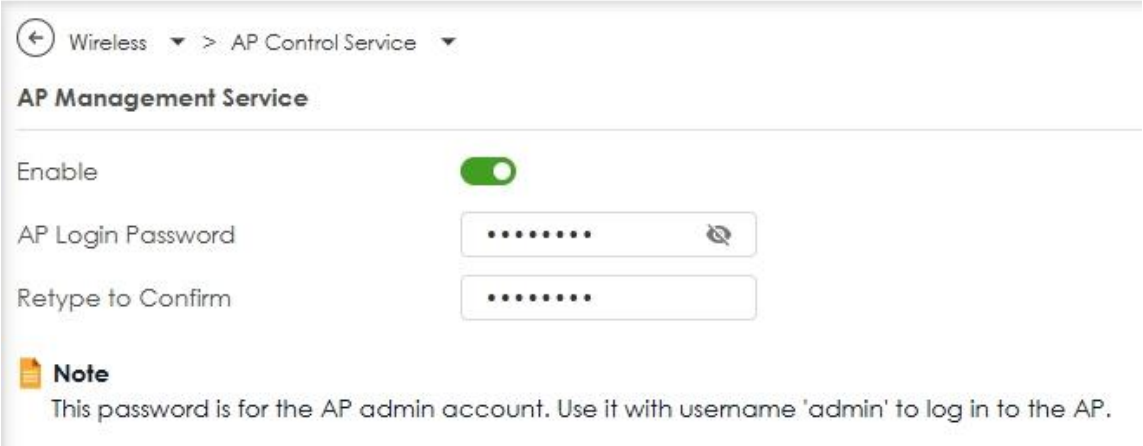


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).

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.

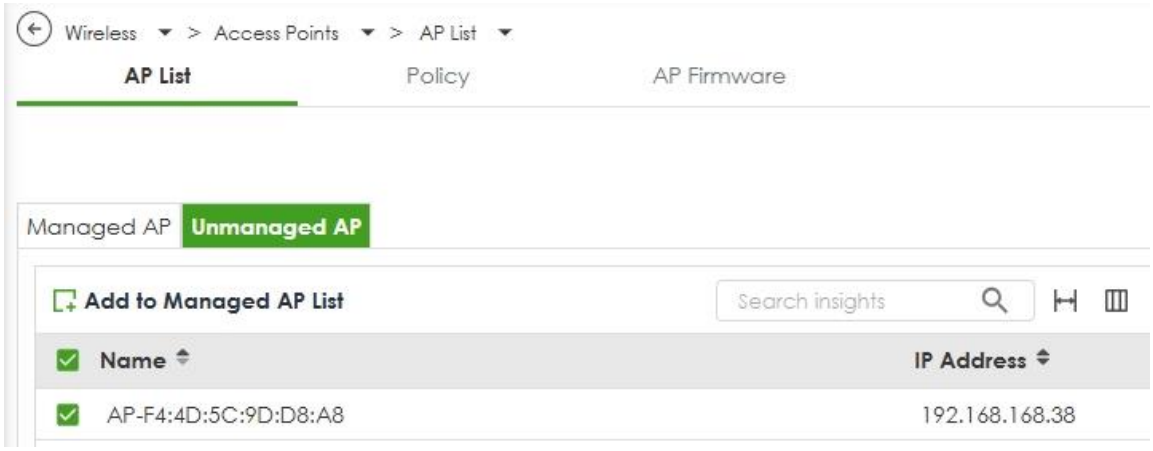
Wireless > AP Control Service



Connect the Zyxel AP unit to the lan interface.

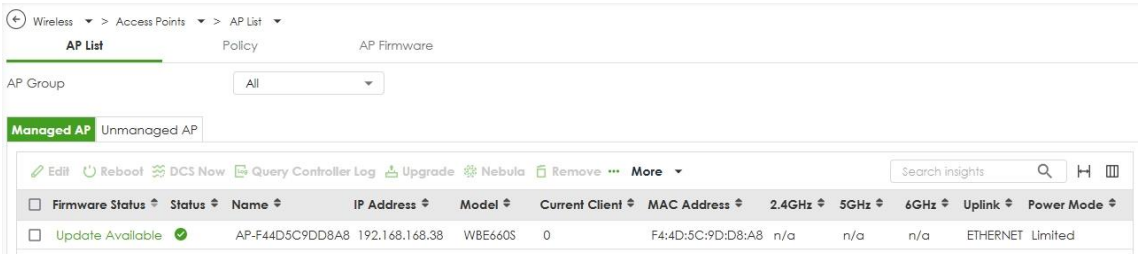
Go to Wireless > Access Points > AP List. The Zyxel AP will be listed under Unmanaged AP tab. Tick the AP and click "Add to Managed AP List.

Wireless > Access Points > AP List > Unmanaged AP



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

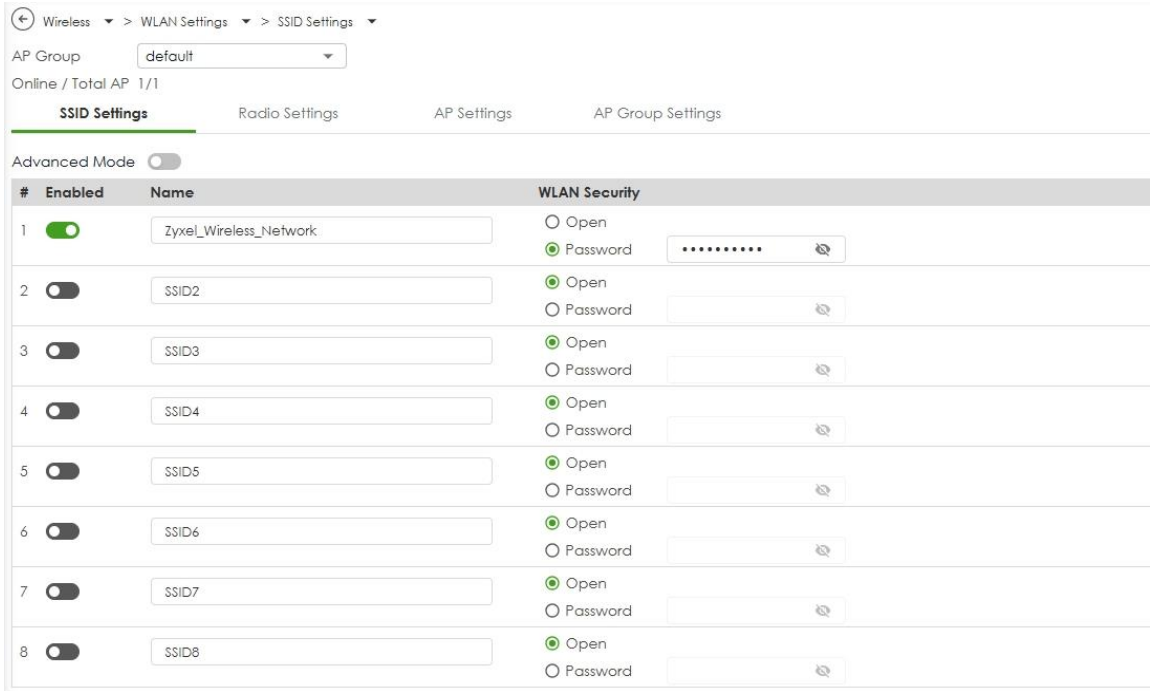
Wireless > Access Points > AP List > Managed AP



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.

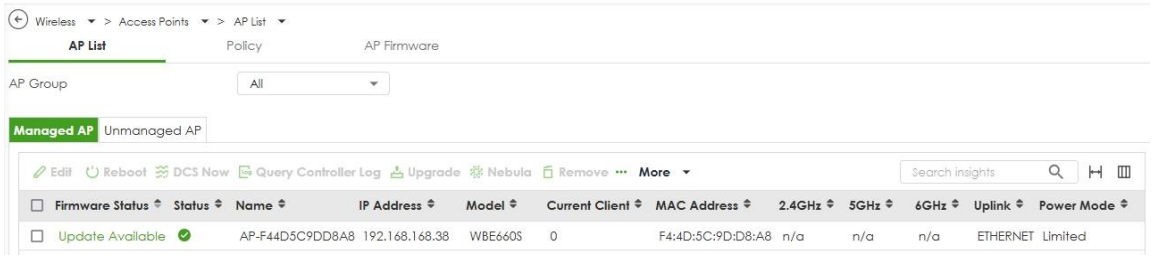
Wireless > WLAN Settings > SSID Settings



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



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

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.

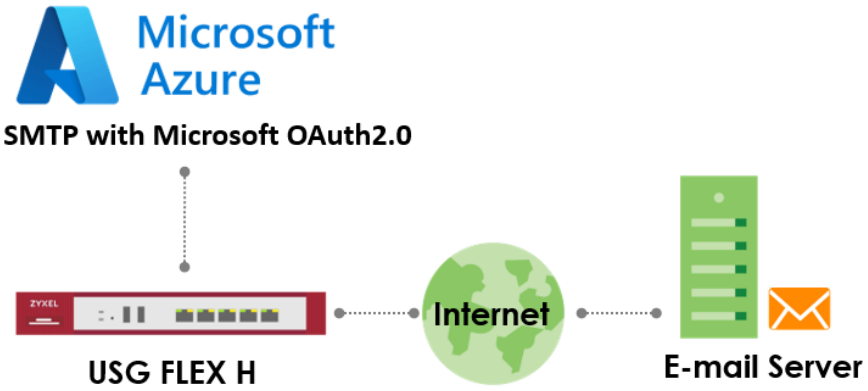
Log & Report > Log / Events > APC

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** –

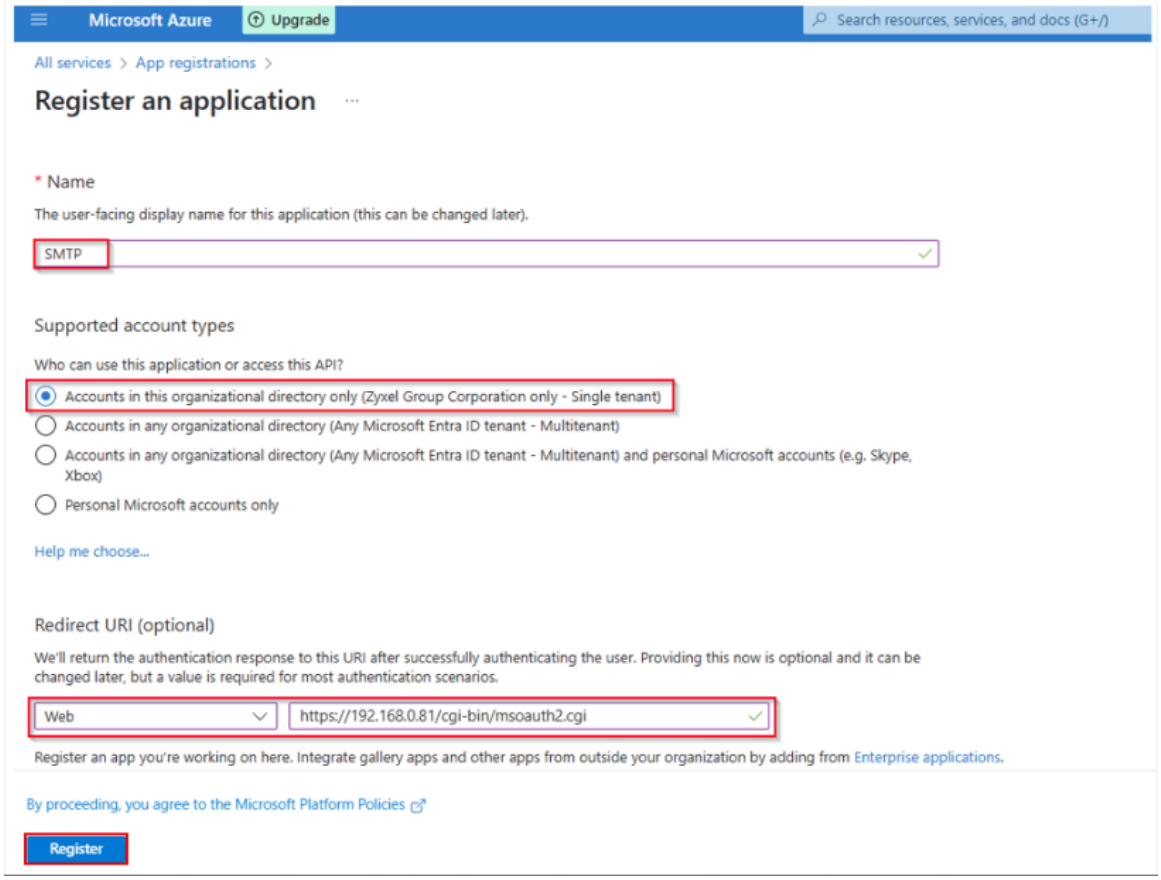
   Name: Enter a descriptive name (e.g., "Gateway SMTP App").

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

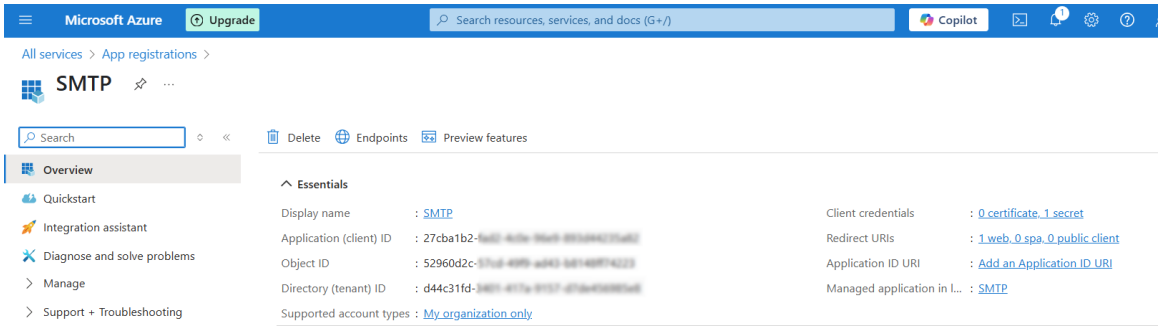
   Redirect URI: The redirect URI specifies where the authorization server should send the user back after successfully authenticating to return an access token to their email account.

   Type: Select "**Web"**.

   URI: Enter *https:///[**device fqdn or ip**]/cgi-bin/msoauth2.cgi*. 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**.

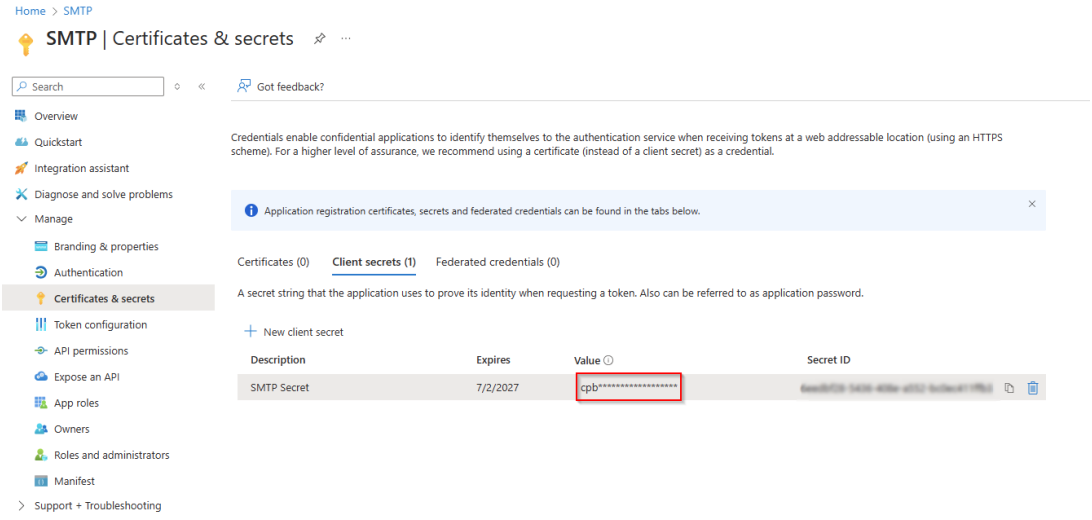


4. **Copy Application IDs** – On the app's **Overview** page, copy the **Application (client) ID** and **Directory (tenant) ID**. These are required for your gateway configuration.



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

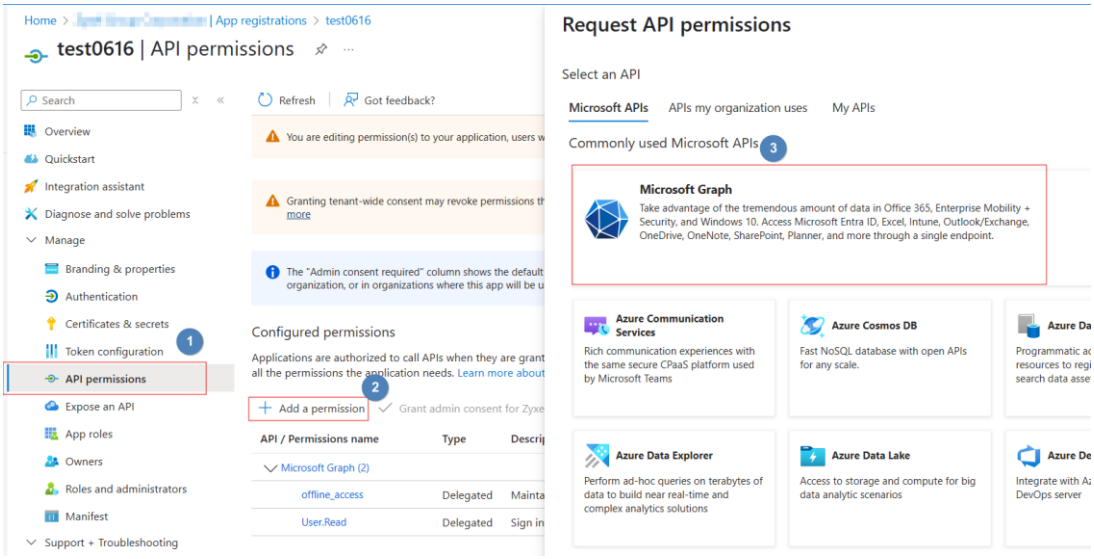
this page. If you lose it, you'll need to generate a new one. This is your “Client Secret”. Store it securely, as it grants access to your application.

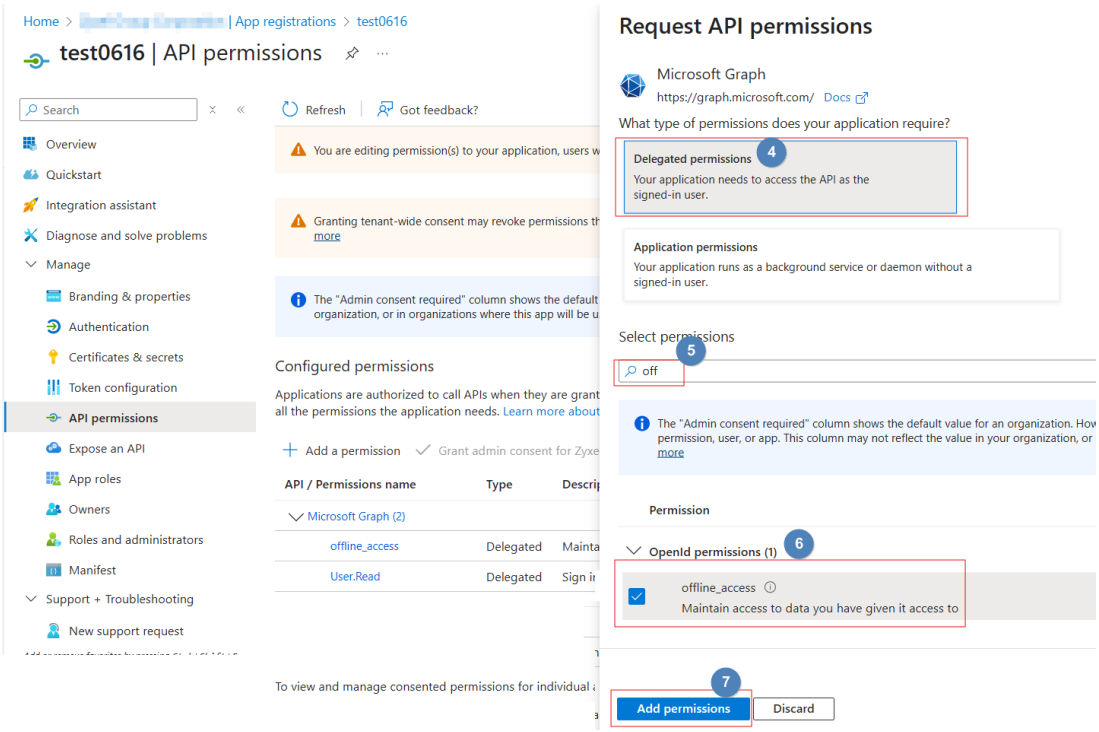


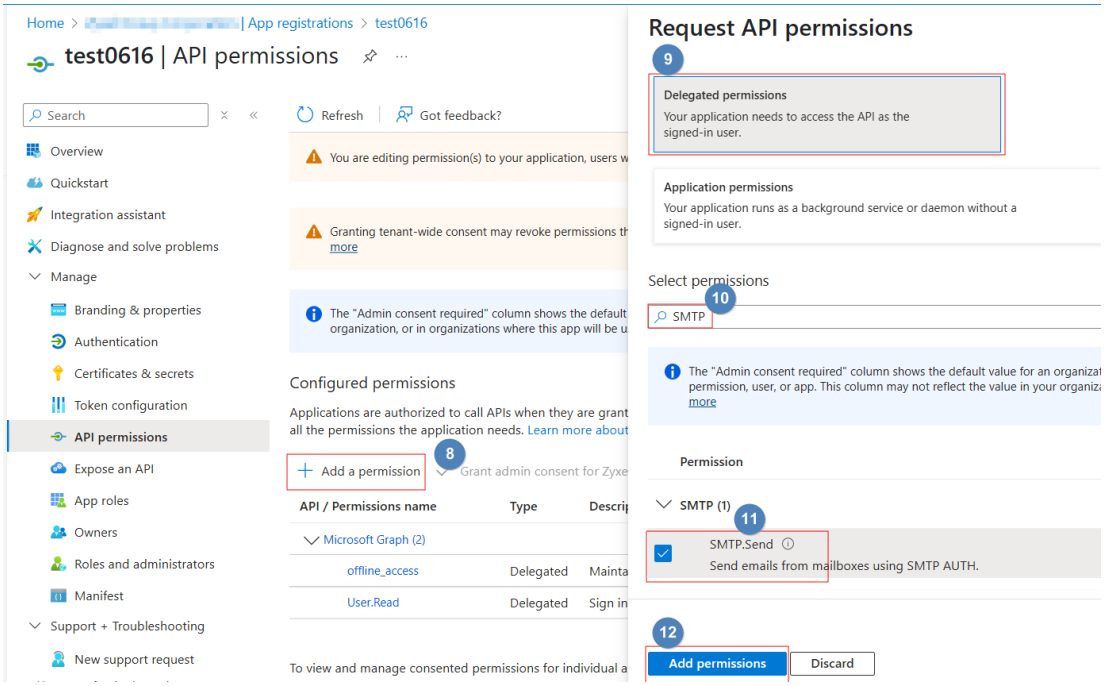
Step 2: Grant API Permissions

Add Permissions:

- From the left-hand navigation of your application's overview page, click on **API permissions > +Add a permission**.
- Select **Microsoft Graph**
- Choose **Delegated permissions** > Search for **offline_access**
- Click **Add permissions**.
- Add 2nd permissions. Click **+Add a permission**
- Select **Microsoft Graph**
- Choose **Delegated permissions** > select **SMTP.Send**
- Click **Add permissions**.

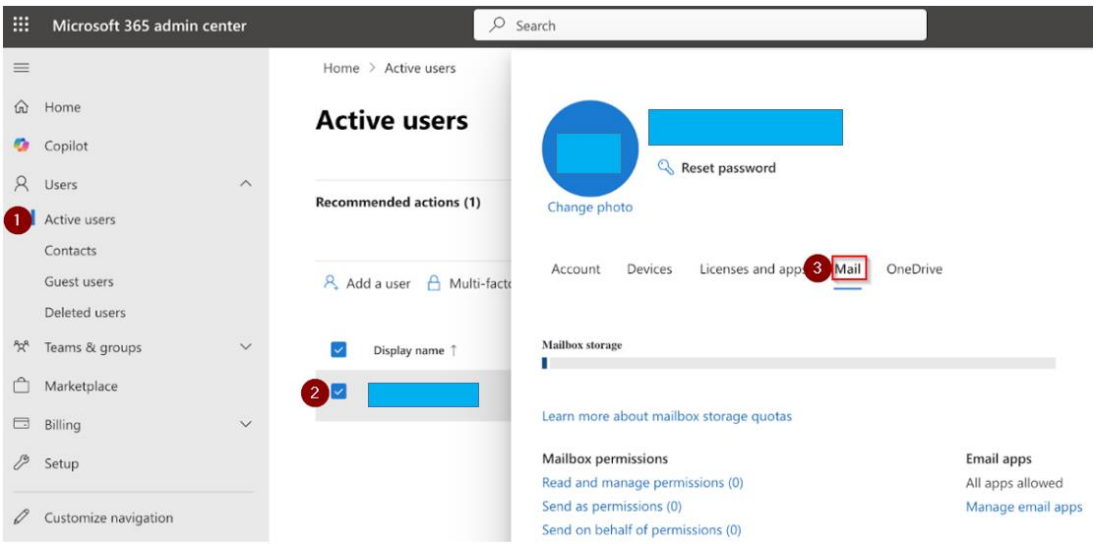




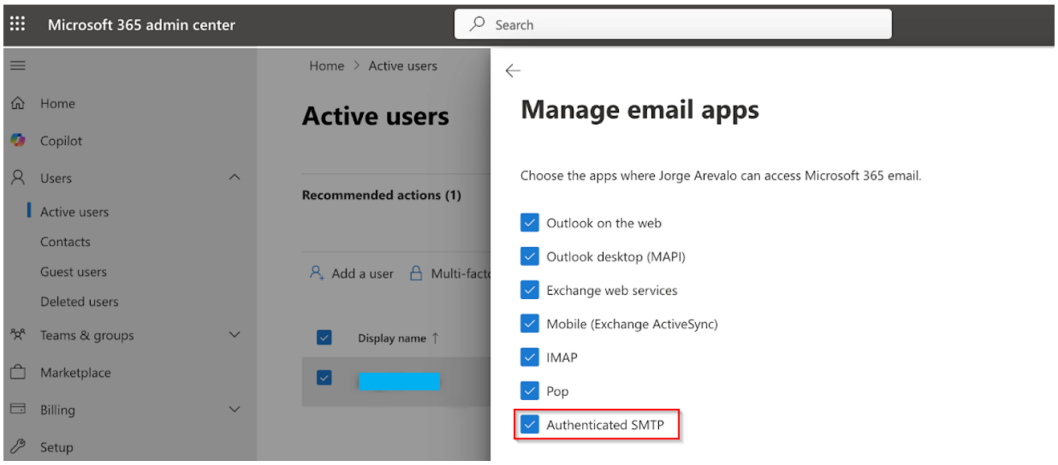


Step 3: Enable SMTP AUTH for the mailbox

1. **Sign in to Microsoft 365 admin center** - Navigate to **Users > Active users** > click the user's mailbox > Select **Mail** tab.

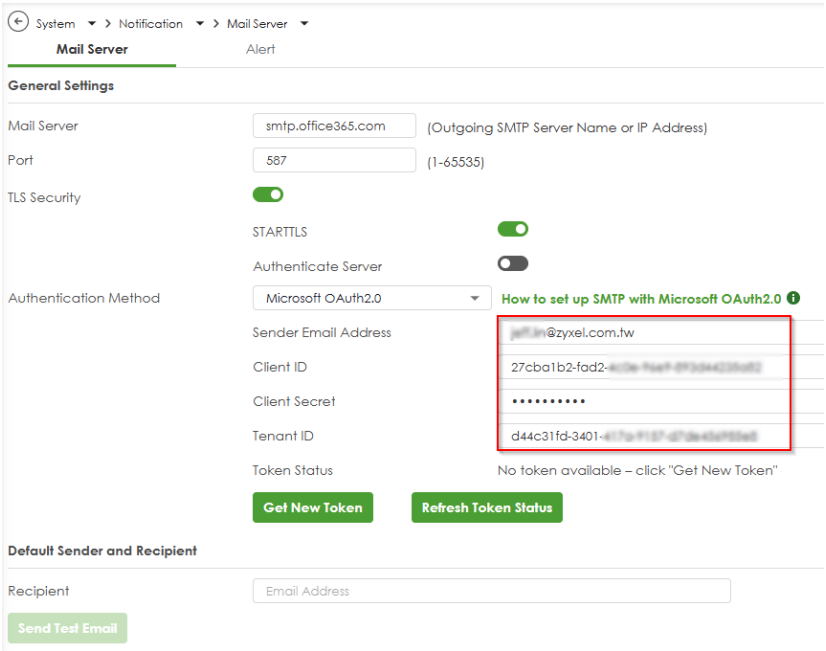


2. Ensure that the checkbox option “Authenticated SMTP” is selected.



Step 4: Configure SMTP in Your Gateway

1. **Access the Gateway GUI**
   - Log in to your device’s configuration interface from internal interface (LAN side).
   - Navigate to **System > Notification > Mail Server**
2. **Enter SMTP Settings**
   - **Mail Server**: smtp.office365.com
   - **Port**: 587 (recommended, supports STARTTLS).
   - **Encryption**: Enable **TLS Security** and **STARTTLS**
   - **Authentication Method**: Select **Microsoft OAuth2.0**.
   - **Sender Email Address**: Enter the Microsoft 365 email address (e.g., sender@yourdomain.com).
   - **Client ID**: Paste the Application (client) ID from Step 1-4.
   - **Client Secret**: Paste the client secret value from Step 1-5.
   - **Tenant ID**: Paste the Directory (tenant) ID from Step 1-4.
3. **Apply Configuration**
   - You must click **Apply** before requesting a token.
   - Click **Apply** to save the configuration on your gateway.



4. **Obtain OAuth 2.0 Token**

   o After applying the configuration, click "**Get New Token**" button.

   o This will **open a new browser tab** to the Microsoft Azure sign-in page.

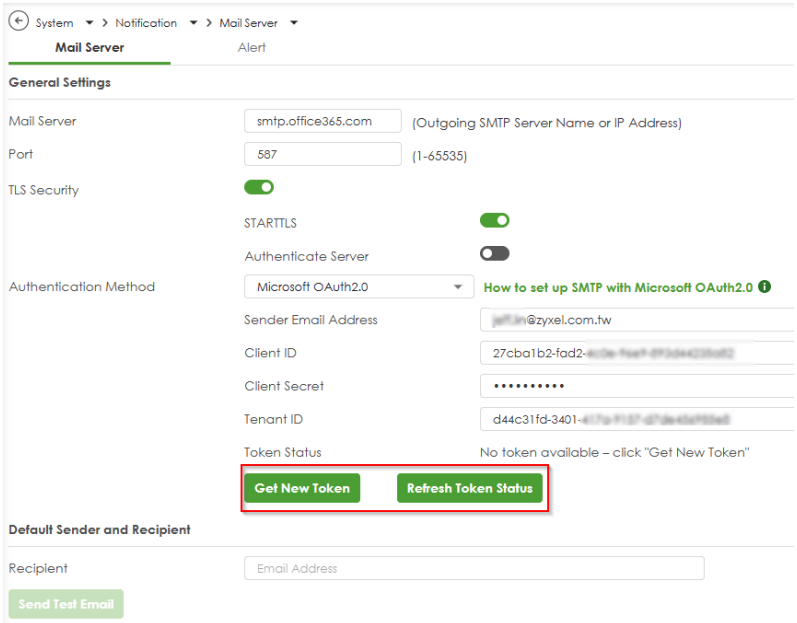
   o Sign in with the Microsoft 365 account associated with the sender email address (e.g., sender@yourdomain.com).

   o Grant permissions when prompted

   o The browser will close automatically upon successful authentication, and your gateway will have securely obtained an authentication token from Microsoft.

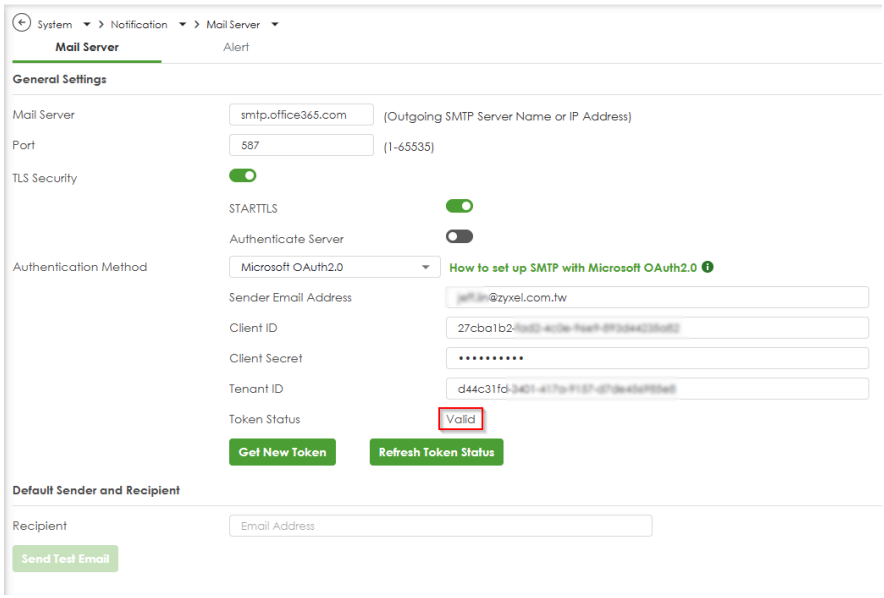
   o The **Token Status** field will update. (e.g., “Valid”).

   o **If the browser does not open**: Click the “**Refresh Token Status**” button to check if the token was successfully obtained or to retry the token retrieval process.



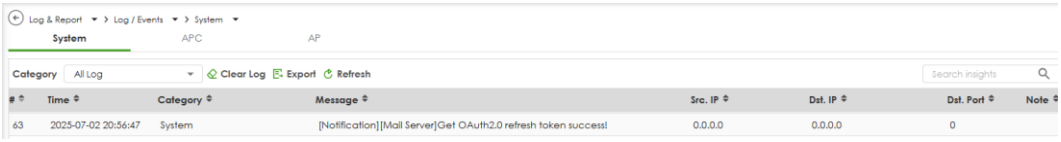
Verify the SMTP with Microsoft OAuth2.0 function

1. Ensure token is successfully acquired.

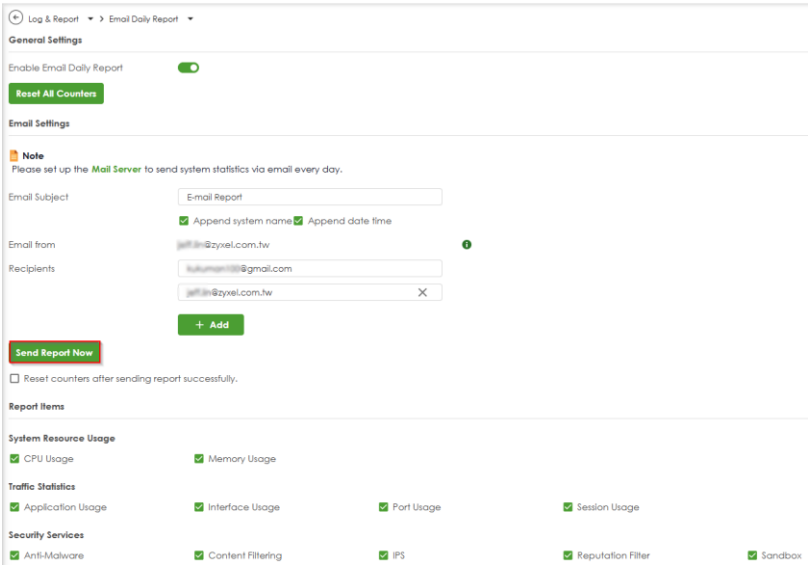


   Fill in the recipient email address and send a test email.

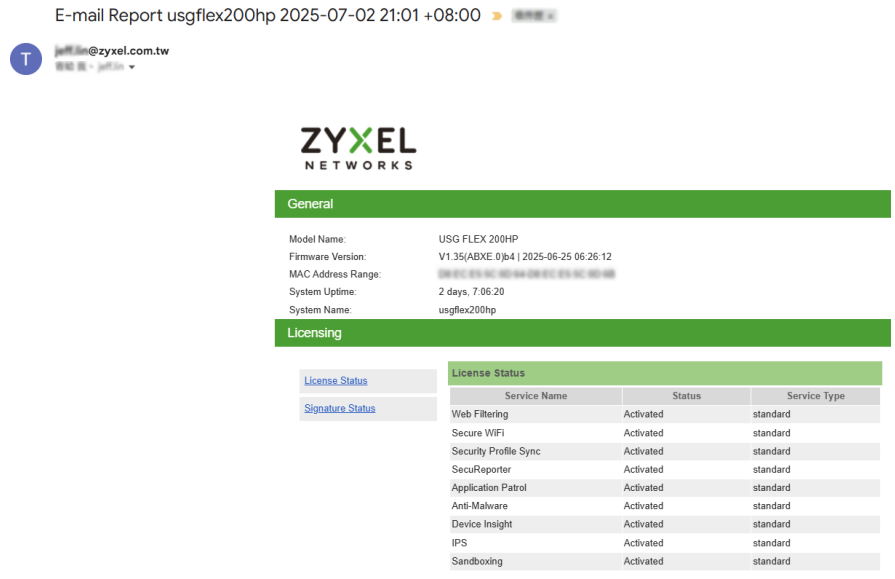
Navigate to **Log & Report > Log/Events > System** and check for the successful token-retrieval log message.



2. Navigate to **Log & Report > Email Daily Report > Send Report Now** to send an email through your firewall.



Ensure that the email is successfully received in the mailbox.



Troubleshooting

1. **Authentication Failed**:
   - Double-check credentials: Ensure that the Client ID, Tenant ID, and Client Secret are copied precisely without any extra spaces.
   - Ensure admin consent was granted for API permissions
   - Check that the sender email address exists in your Microsoft 365 tenant

2. **Permission Denied:**
   - Confirm API permission is granted (Step2-1).
   - Verify the application has admin consent
   - 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:**

   - Verify SMTP server settings (smtp.office365. com:587). Ensure port 587 is unblocked.
   - Ensure STARTTLS encryption is enabled
   - Check firewall/network connectivity

5. **Browser Issues:**

   - **Browser doesn't open**: Check if pop-up blockers are enabled and allow pop-ups for the gateway
   - **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).
   - **Token not acquired after sign-in**: Click "Refresh Token Status" button to check token status
   - **Multiple browser tabs open**: Close extra tabs and try again
   - **Browser doesn't close automatically**: Manually close the tab after successful sign-in

6. **Token Issues:**
    - **Token acquisition failed**: Verify internet connectivity and try clicking "Get New Token" again
    - **Token expires quickly**: This is normal - the gateway will automatically refresh tokens
    - **"Refresh Token Status" button shows no token**: Repeat the "Get New Token" process
    - **Token status not updating**: Wait 10-15 seconds then click "**Refresh Token Status**" again

Security Best Practices

1. **Secret Management:**
    - Store client secrets securely
    - Rotate secrets before expiration
    - Use different applications for different purposes
2. **Access Control:**
    - Grant minimum required permissions only
    - Regularly review application permissions
    - Monitor application usage through Azure logs
3. **Monitoring**
    - Enable audit logging in Microsoft Entra ID
    - Monitor for unusual authentication patterns
    - Set up alerts for failed authentication attempts

Additional Information

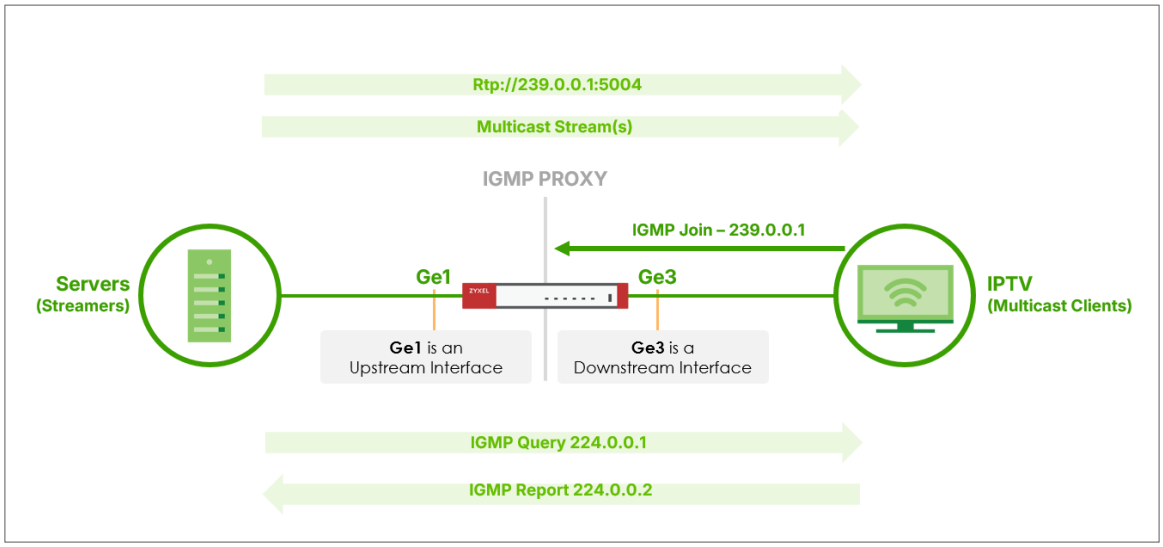
1. **Token Lifecycle:**
    - Access tokens expire after 1 hour
    - Your gateway automatically handles token refresh
    - Initial token must be acquired through browser sign-in
    - Subsequent token renewals happen automatically in the background
    - No user interaction required for token renewal after initial setup
2. **Supported Email Types:**
    - Plain text emails
    - HTML formatted emails
    - Emails with attachments
    - Bulk email sending (within Microsoft limits)
3. **Rate Limits** – Microsoft imposes sending limits
    - 30 messages per minute
    - 10,000 messages per day (default)
    - Higher limits available through Microsoft support
4. **Support** – If you encounter issues:
    - Verify all steps were completed correctly
    - Check Microsoft Entra ID audit logs for authentication errors
    - Contact your system administrator for Azure access issues
    - 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.

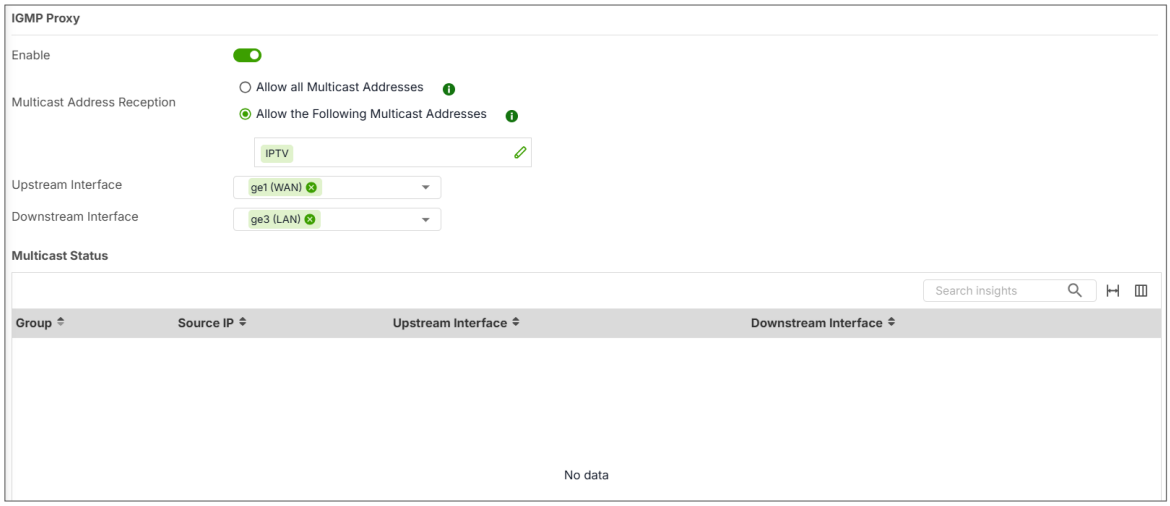
The Internet Group Management Protocol (IGMP) is a core mechanism of multicast technology, responsible for managing multicast group memberships between hosts and upstream routing devices. With IGMP, network devices can effectively determine which endpoints need to receive specific multicast streams, 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).

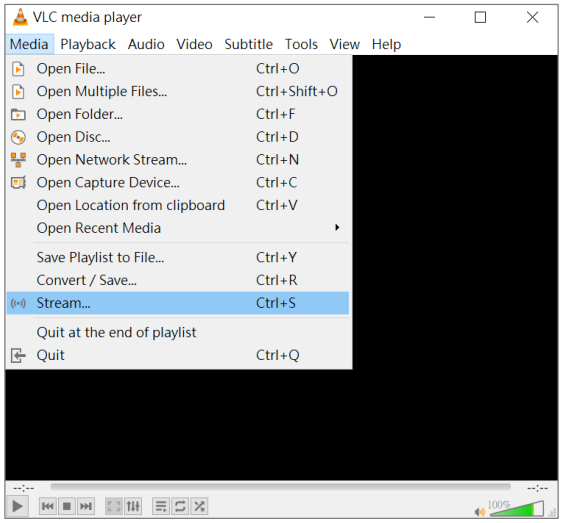
Enable the IGMP Proxy for Downstream and Upstream Interface

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.

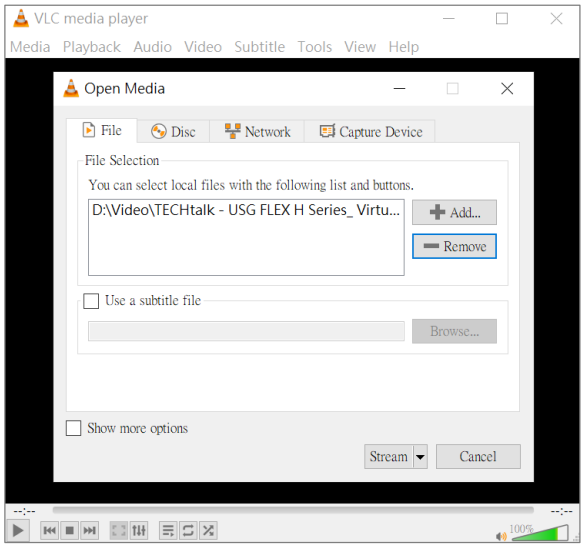


Set Up Streamer Server Using VLC software

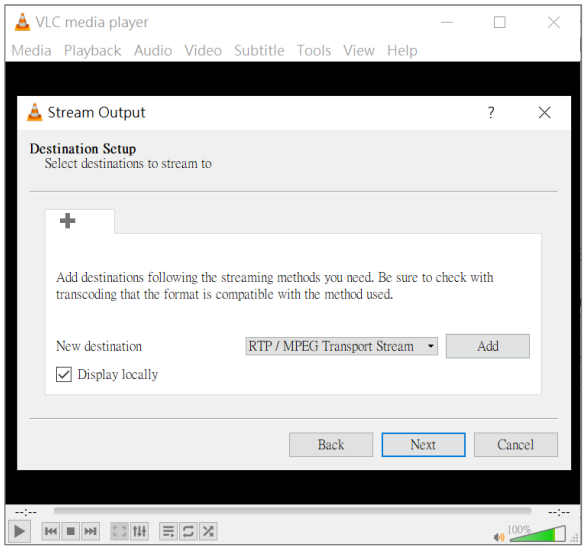
Open Medial Player, and Select “Stream”



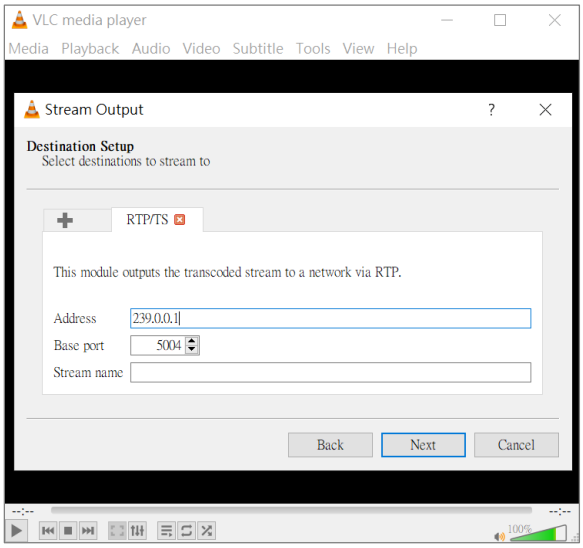
Add a video file and click on “Stream” button.



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

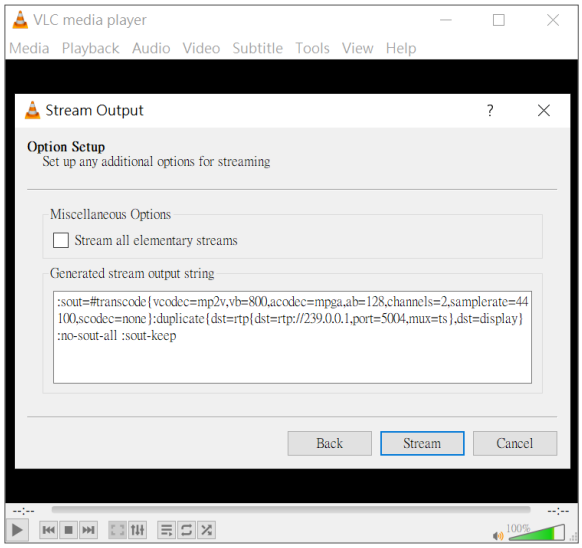


Configure IP address and port number of IGMP group.



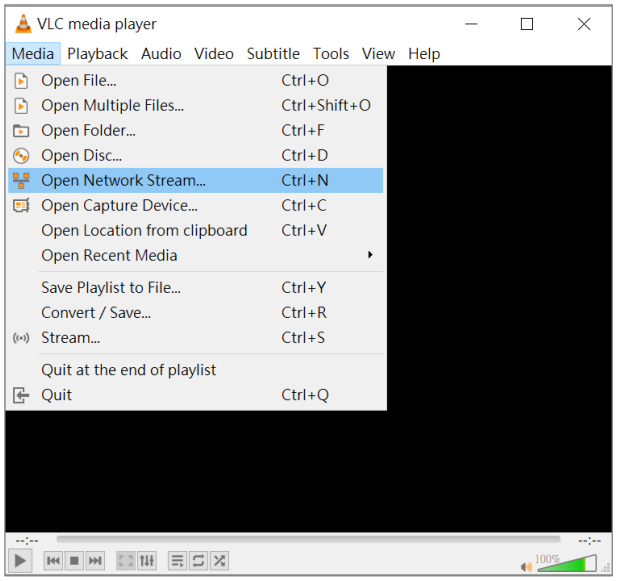
Click Next to complete the setup process

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

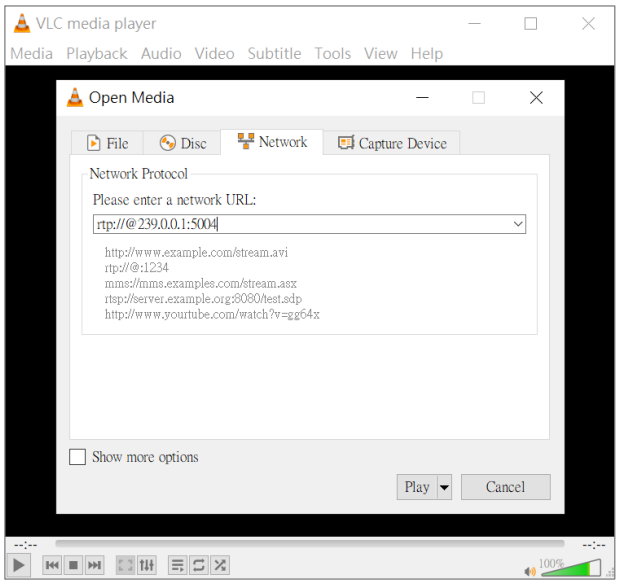


Set Up Player Client Using VLC software

Open Medial Player, and select “Open Network Stream”.



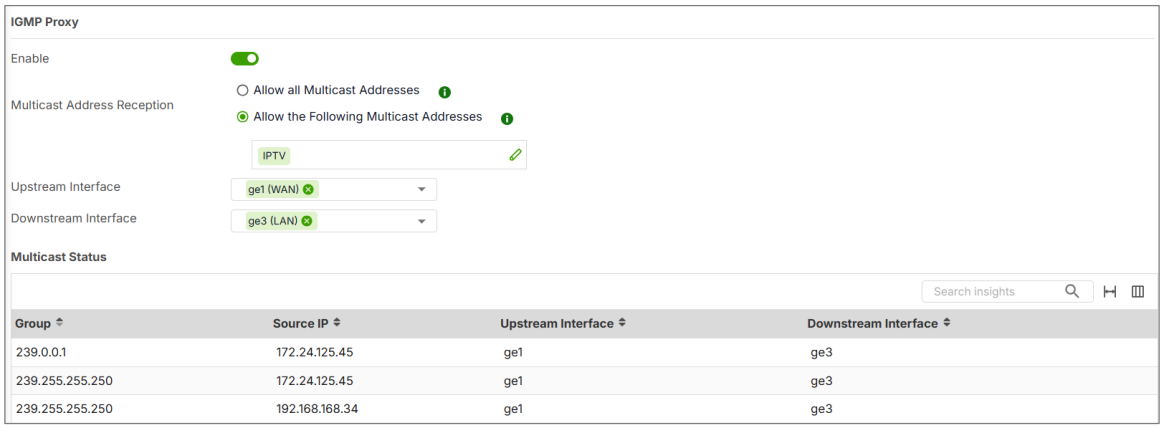
Fill in the IP address of IGMP group with port number, then press “Play.



We can now see the stream playing on the client.

Test the Result

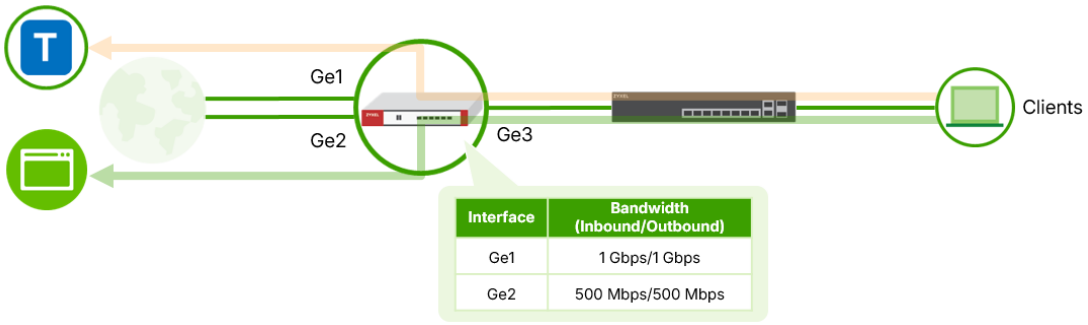
After IPTV client join the multicast group, we can monitor the status on Multicast table.



How to Configure Application-Based Policy Route

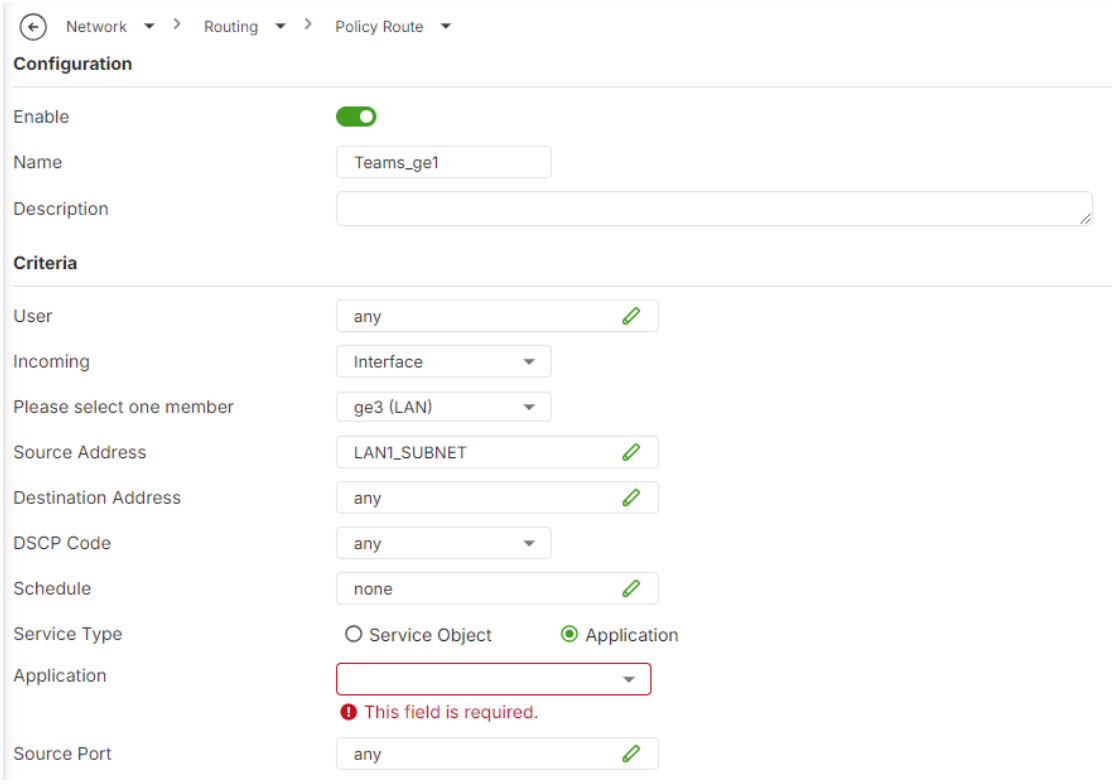
USG FLEX H series supports configuring Application-Based Policy Routing. You can use the application as the matching criterion in a policy route to control traffic forwarding behavior based on the detected application, allowing traffic to be routed through a specific WAN interface according to application 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.

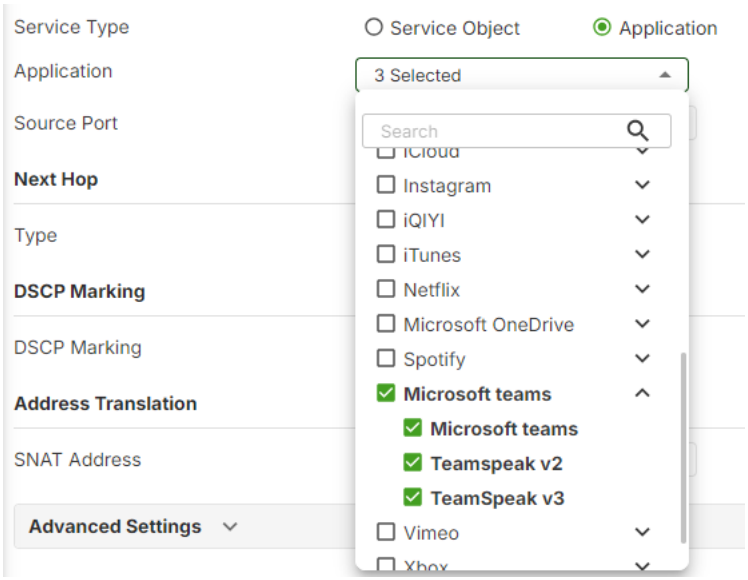


Interface	Bandwidth (Inbound/Outbound)
Ge1	1 Gbps/1 Gbps
Ge2	500 Mbps/500 Mbps

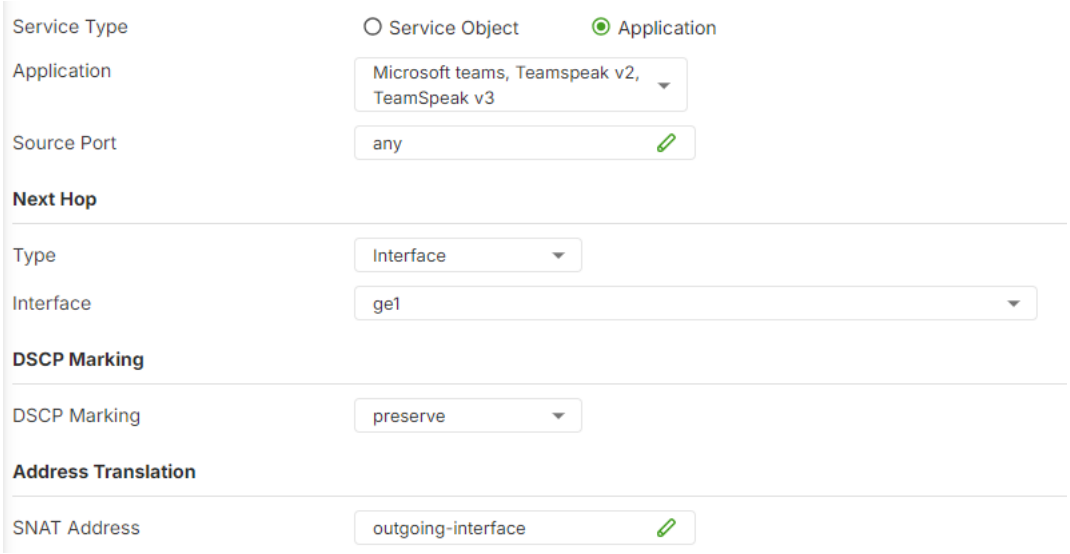
In the USG Flex H, go to Network > Routing > Policy Route > Add a Policy Route rule. Configure a Name for you to identify the Policy Router rule, such as "Teams_ge1". Set up the Criteria for the user, incoming interface, source/destination address, and select the Service Type as Application.



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

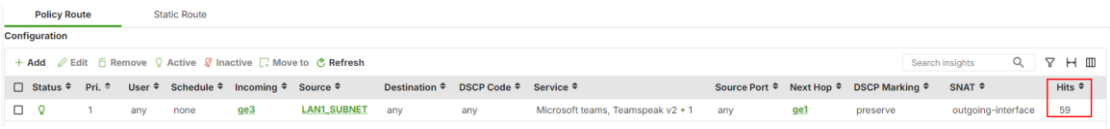


Configure the ge1 interface as the Next-Hop, and select the SNAT address.



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.



Chapter 6- Nebula

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

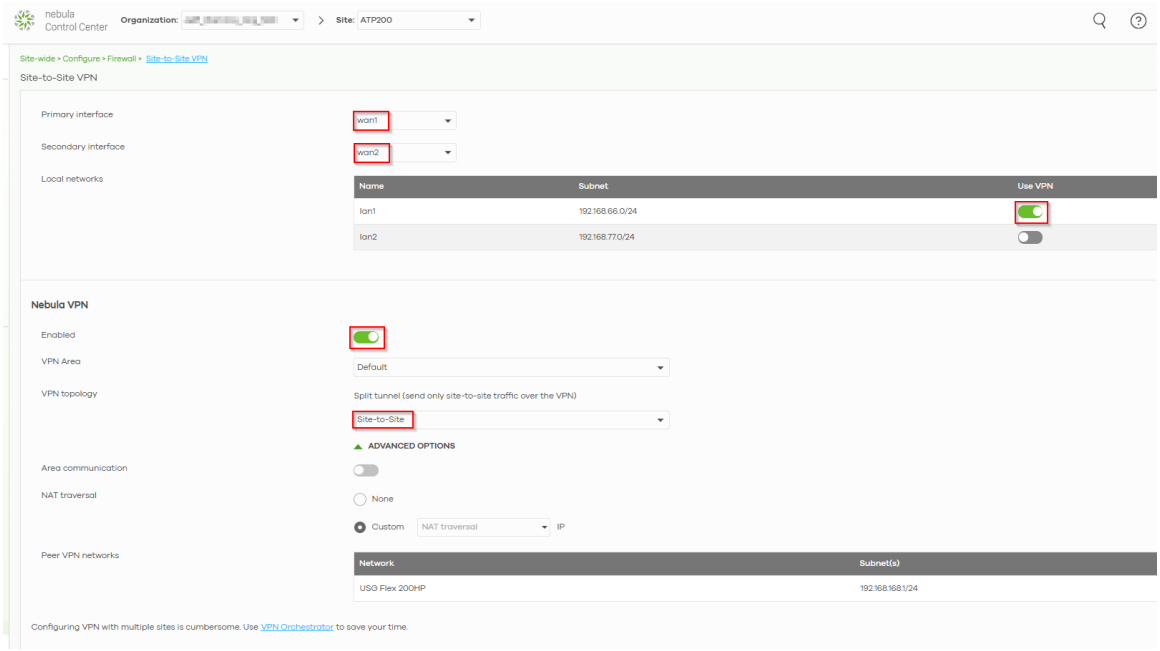
This example shows how to use Nebula VPN to establish Site to Site VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Site-to-Site VPN tunnel is established, LAN hosts can communicate with each other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

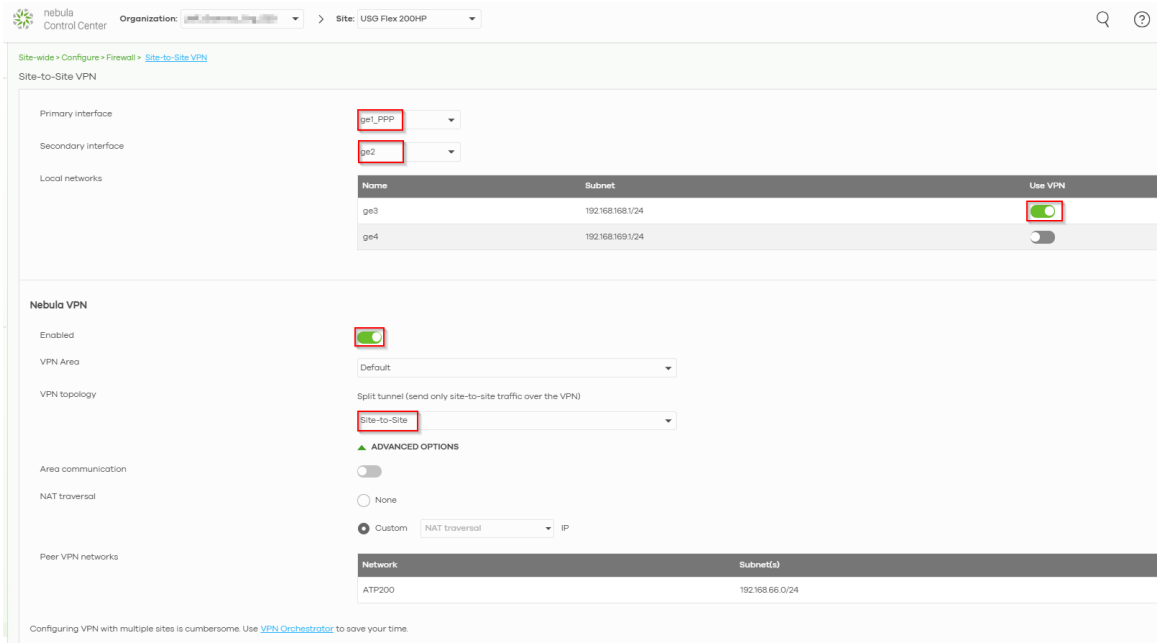
Set Up the Site-to-Site VPN settings on the Nebula Firewall

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

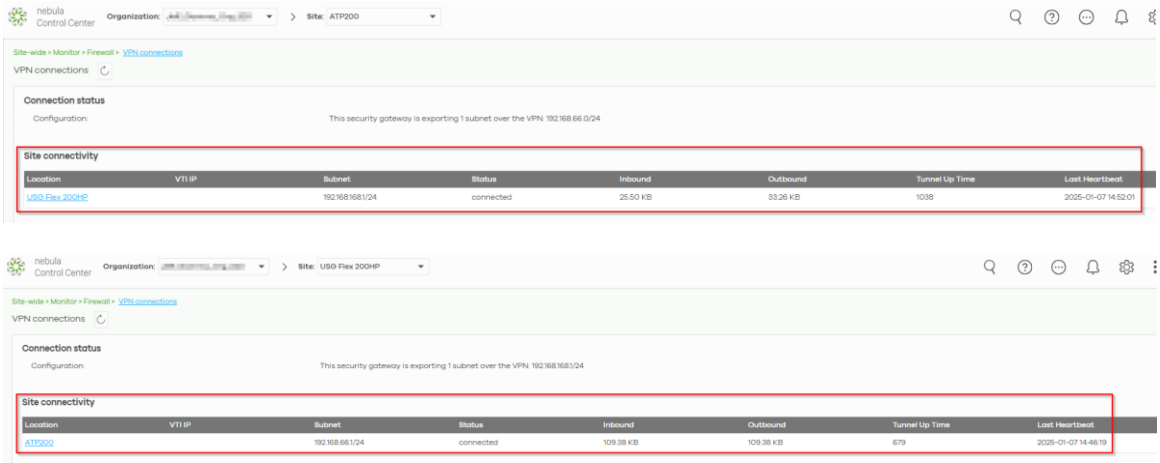


USG FLEX H site

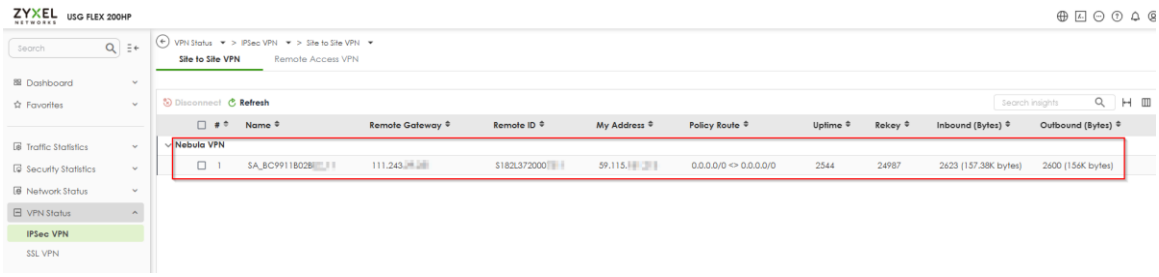


Verify the VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.



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.



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

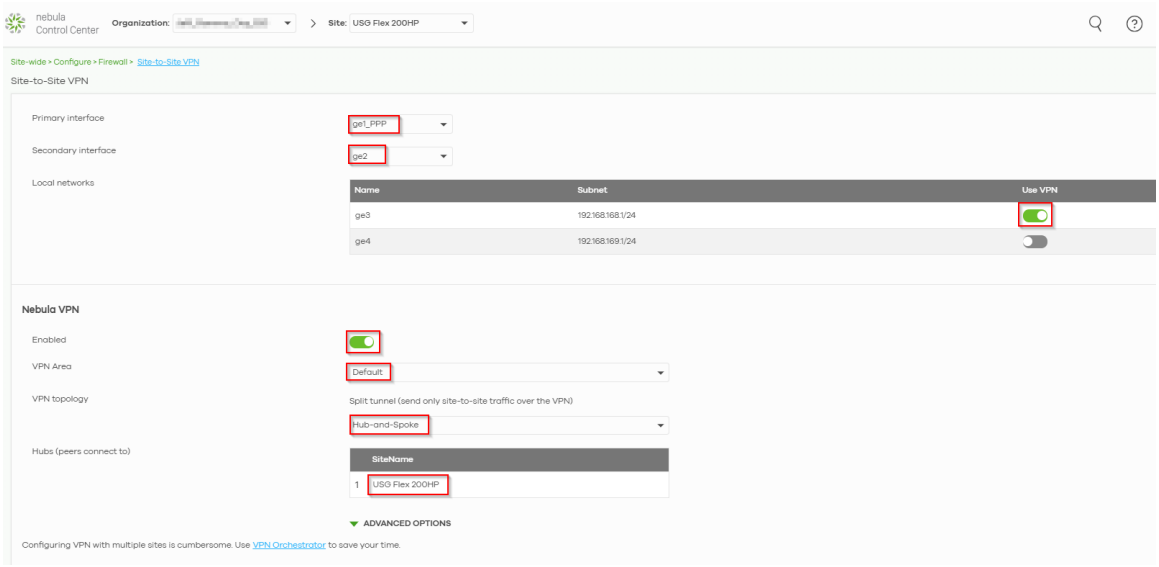
This example shows how to establish Hub-and-Spoke VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the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

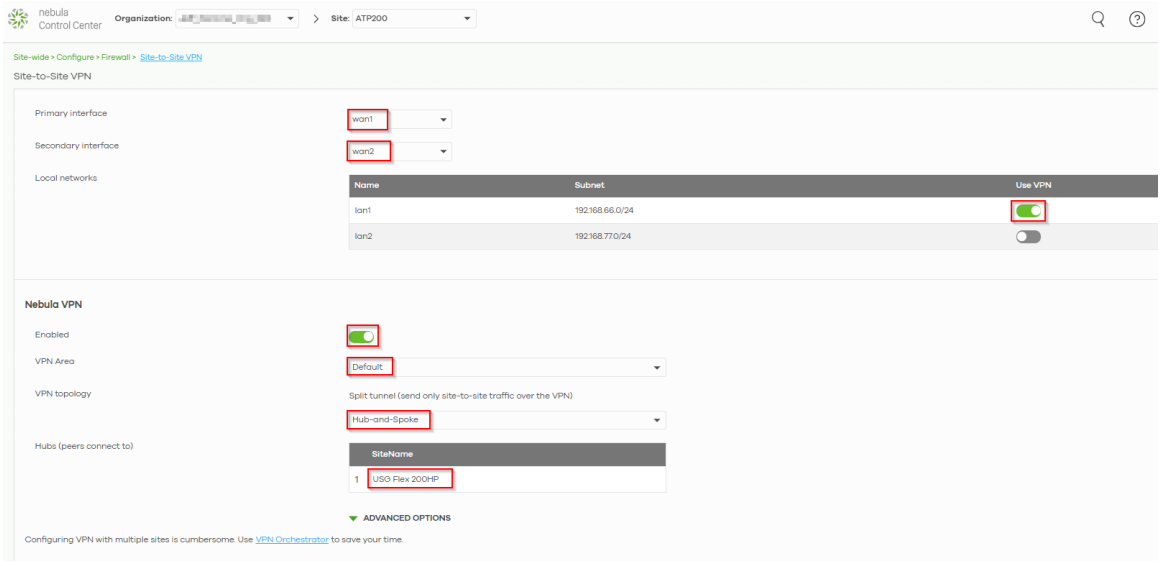
Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

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

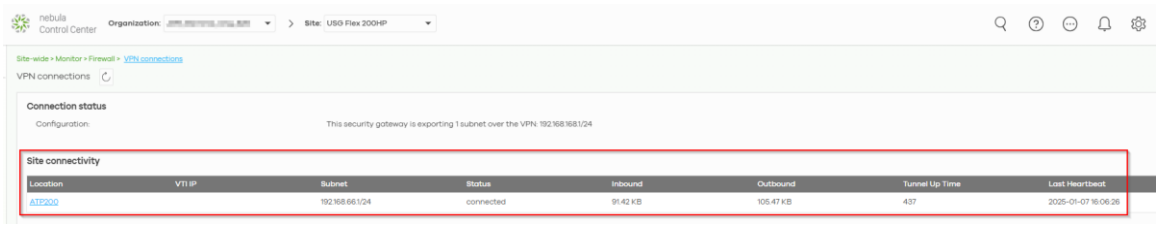


USG FLEX/ATP site

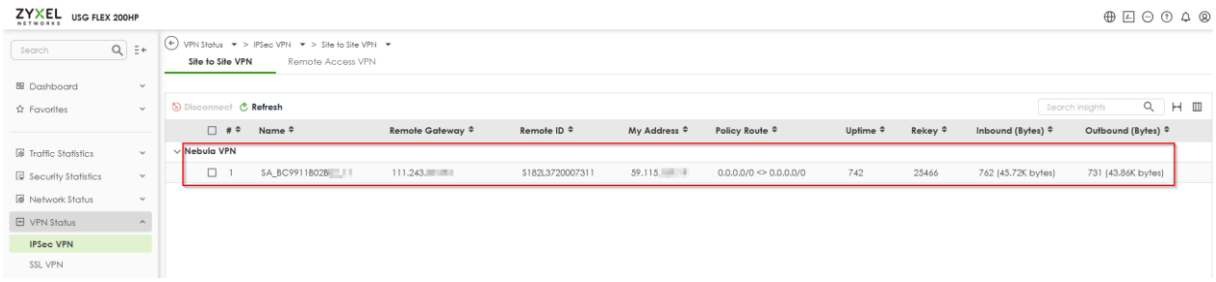


Verify The VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.



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.



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

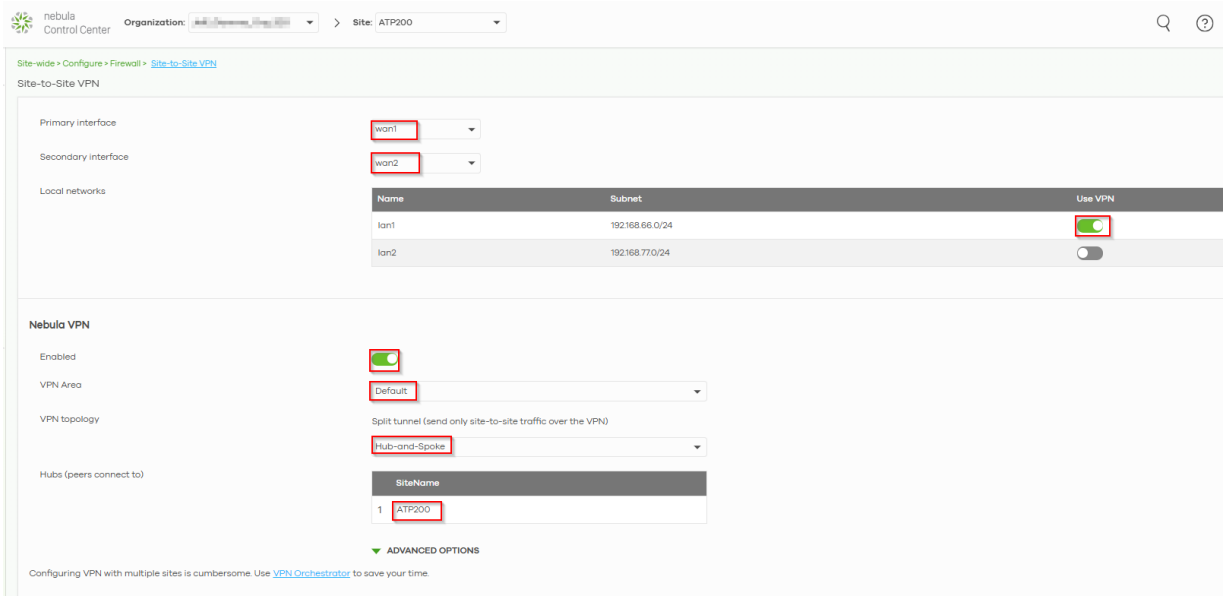
This example shows how to use Nebula VPN to establish Hub-and-Spoke VPN tunnel between USG FLEX/ATP and USG FLEX H. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each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

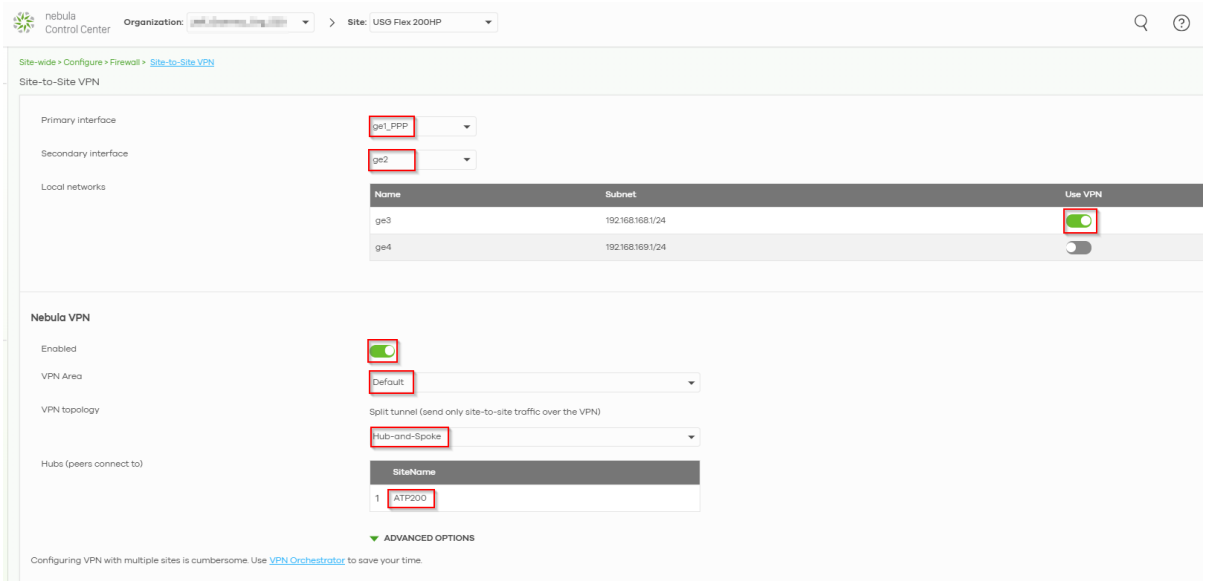
Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

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

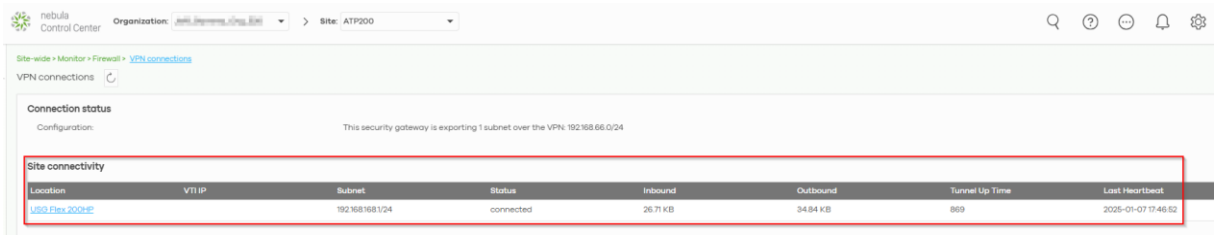


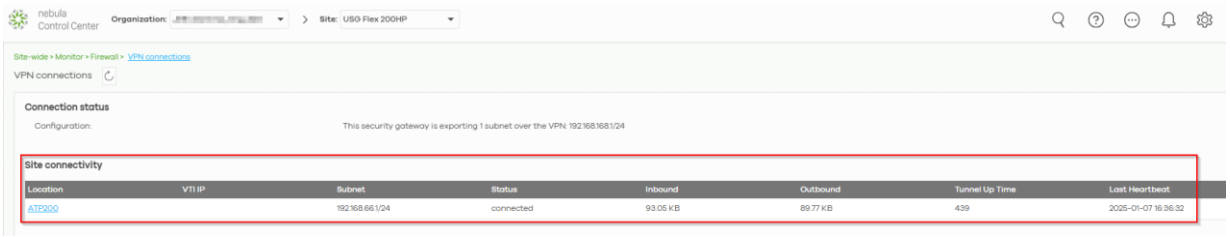
USG FLEX H site



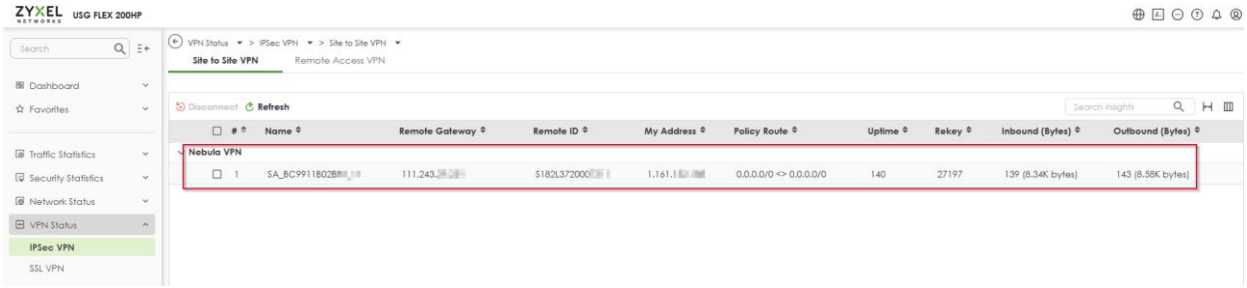
Verify The VPN connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.





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.

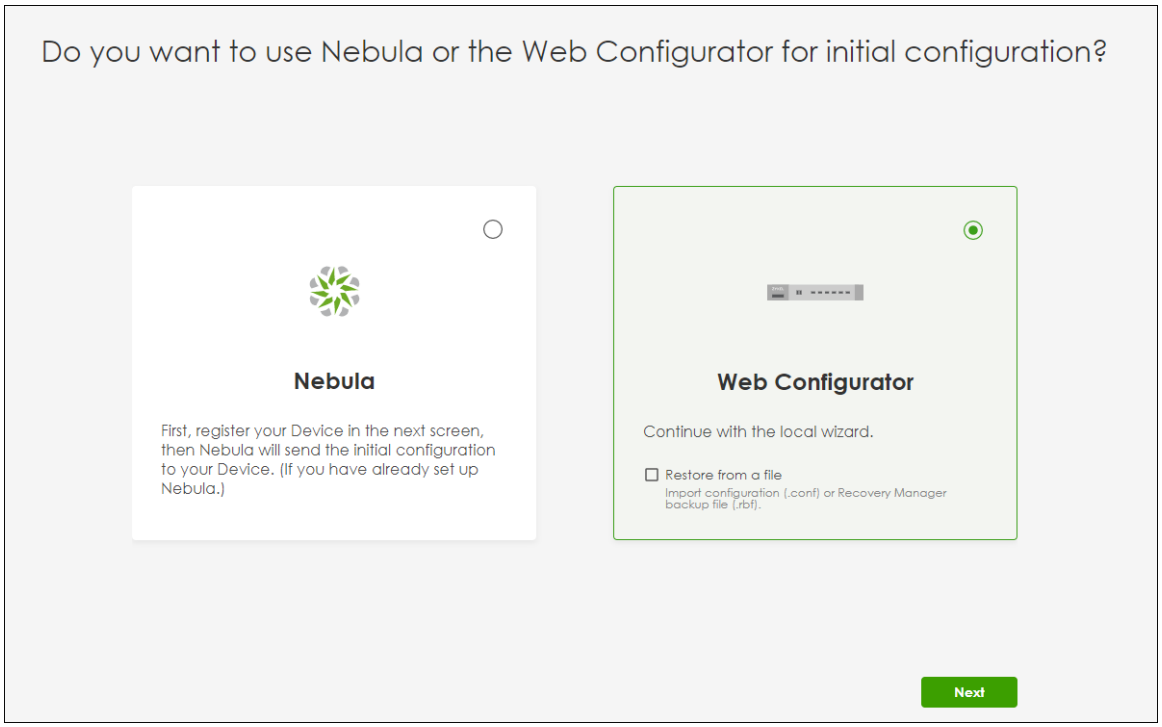


How to Onboard Firewall to Nebula within Initial Setup Wizard

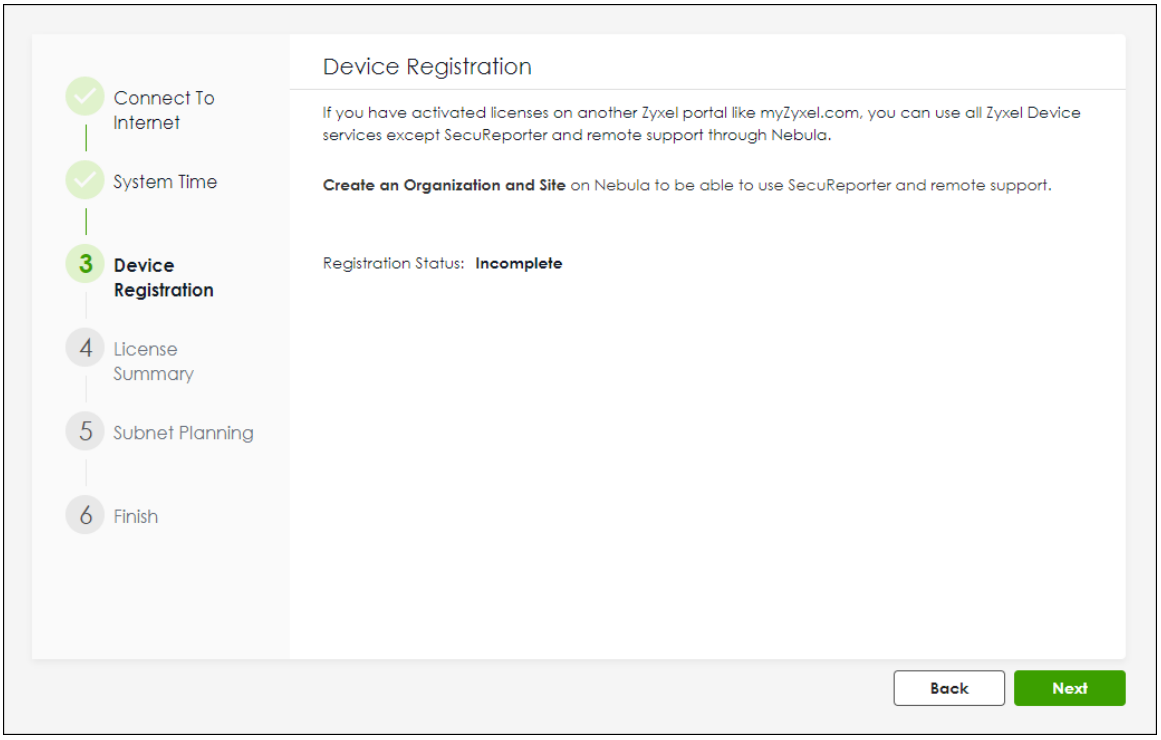
In the initial setup wizard, there are 2 ways to onboard your firewall to Nebula. One is started by Web Configurator (Local configure first), and the other one is started from Nebula CC (Cloud configure first). A brand new firewall with version 1.35 and default configuration will start with the Initial 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)

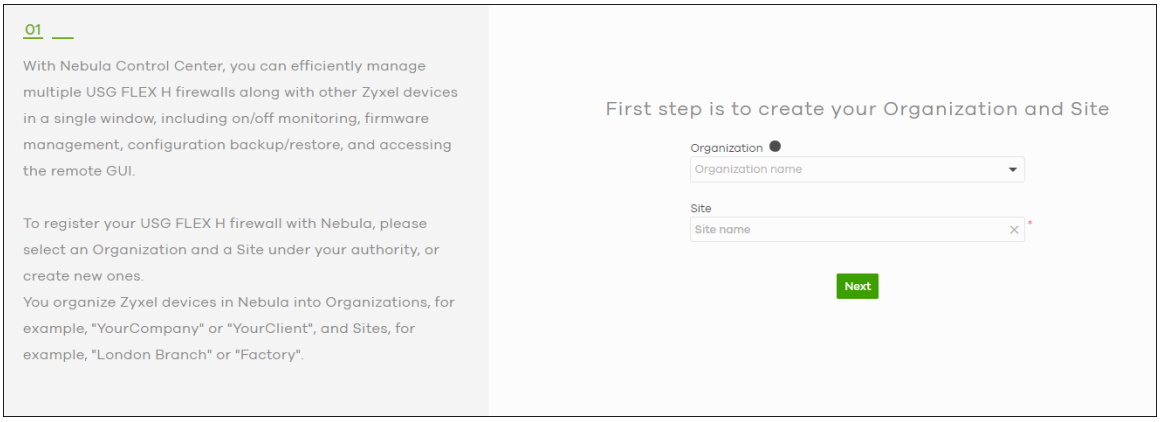
You can choose to onboard your firewall locally by selecting Web Configurator.



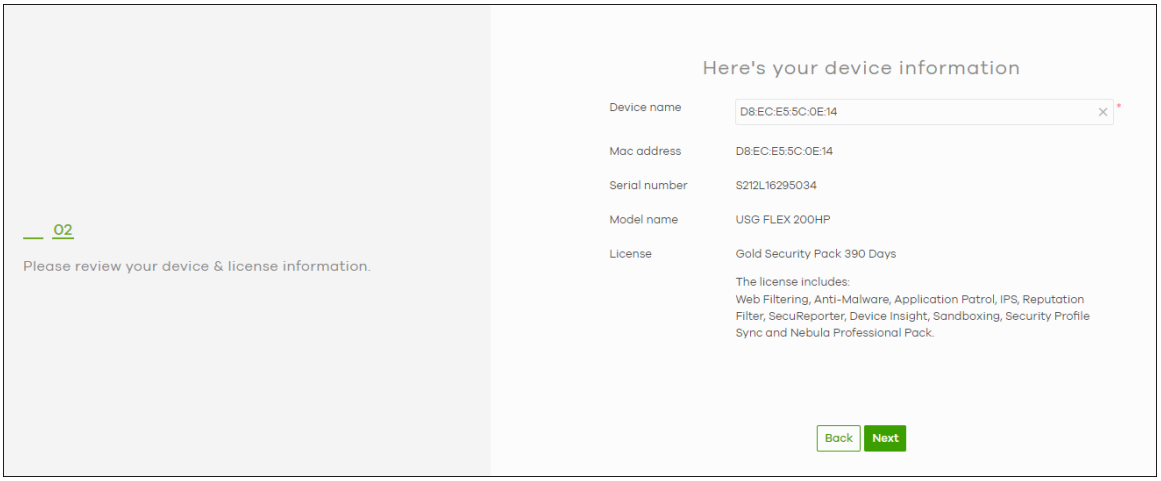
In Step 3, The Web GUI will prompt you to register your firewall.

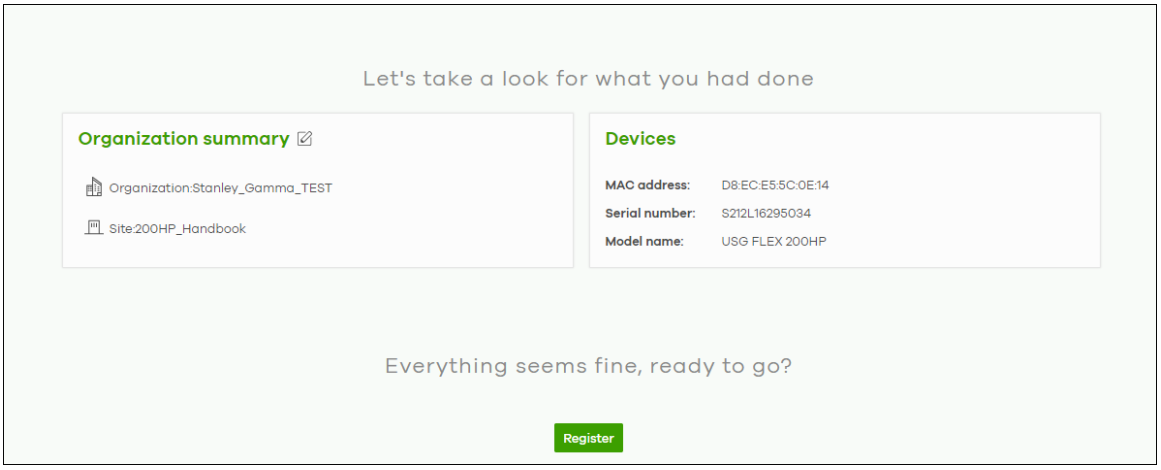


Click **Next** to proceed. The browser will redirect you to the Nebula Control Center (NCC), where you must assign the firewall to an existing Organization and Site or create a new one.

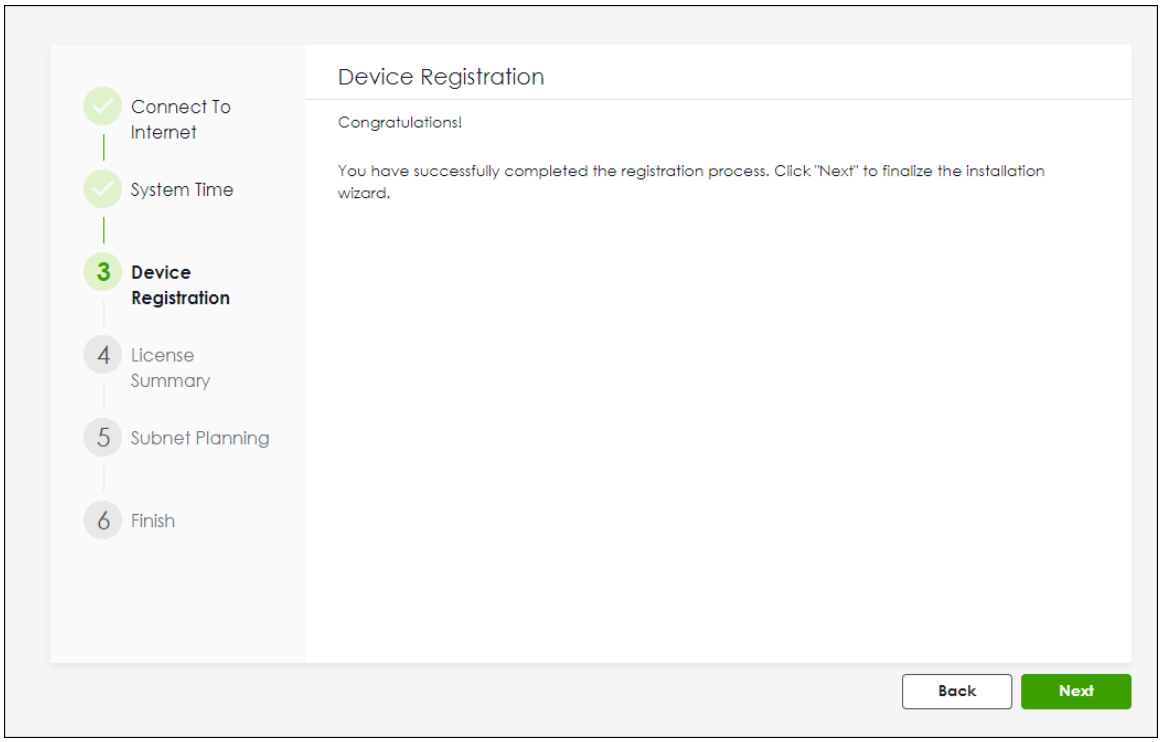


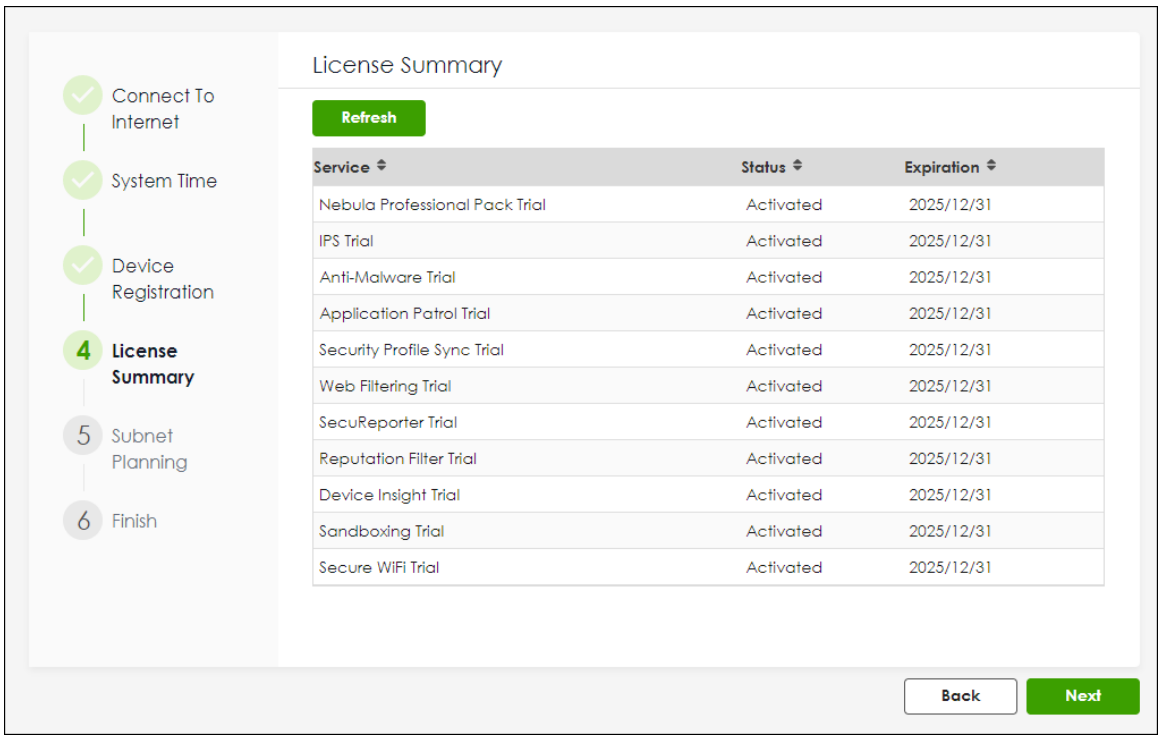
After clicking **Next**, your firewall will be registered to Nebula server.



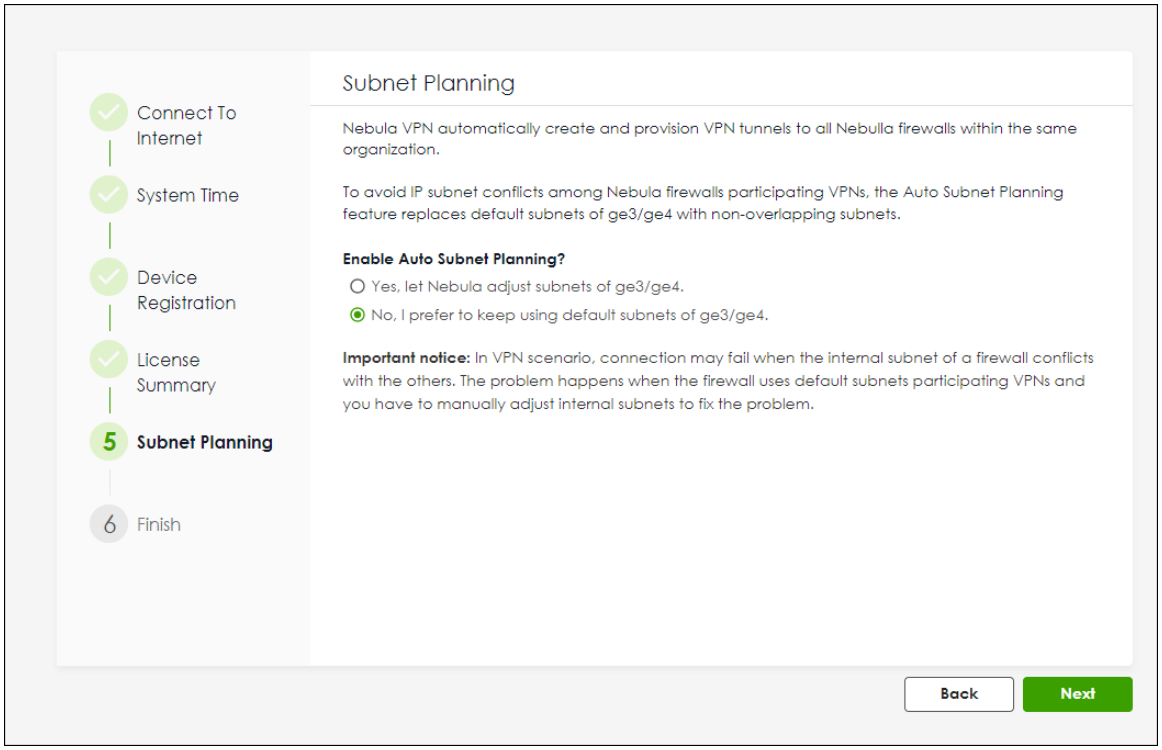


Once registration is complete, your browser will return to the Initial Setup Wizard, and showing the device registration status.

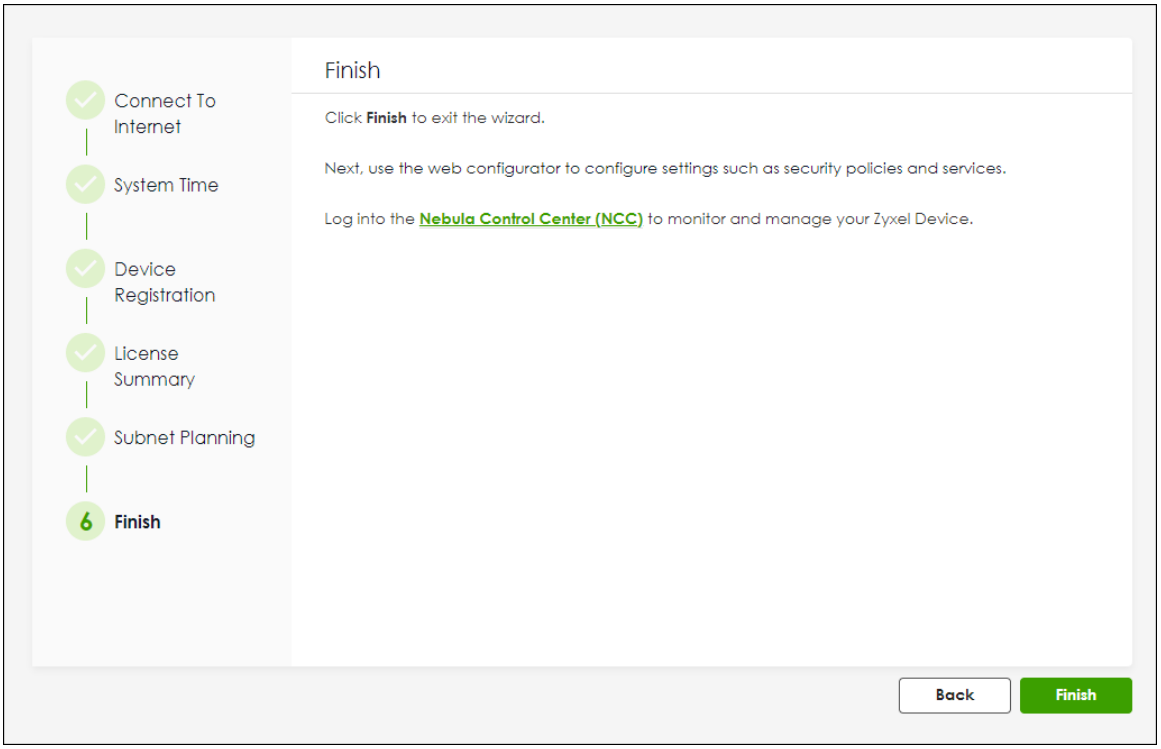




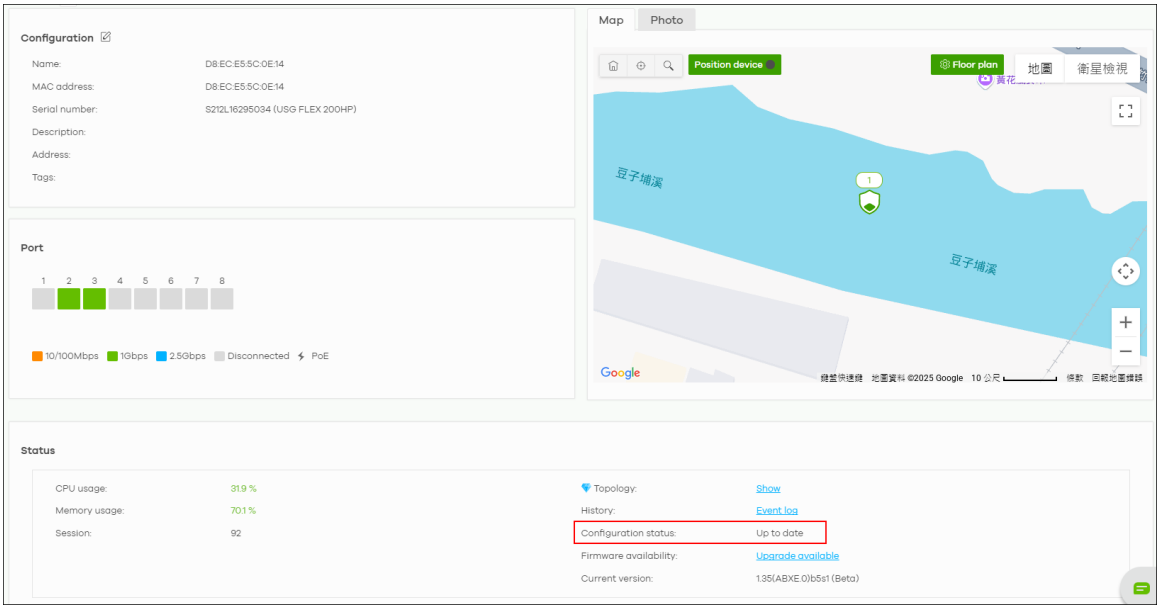
In step 5, you can choose whether to use the default interface IP address or apply the interface IP address already configured in Nebula server. If need using Nebula SD VPN suggestion to select “Yes” to apply Nebula site assige IP subnet to avoid subnet conflict.



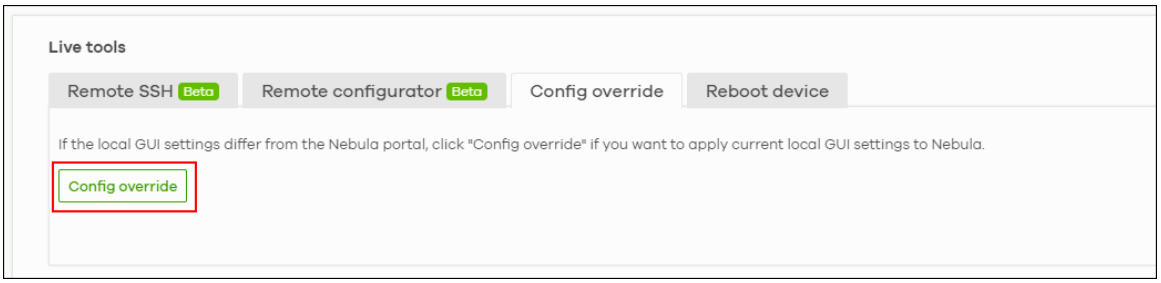
In Step 6, Click **Finish** to close the wizard from Web GUI.

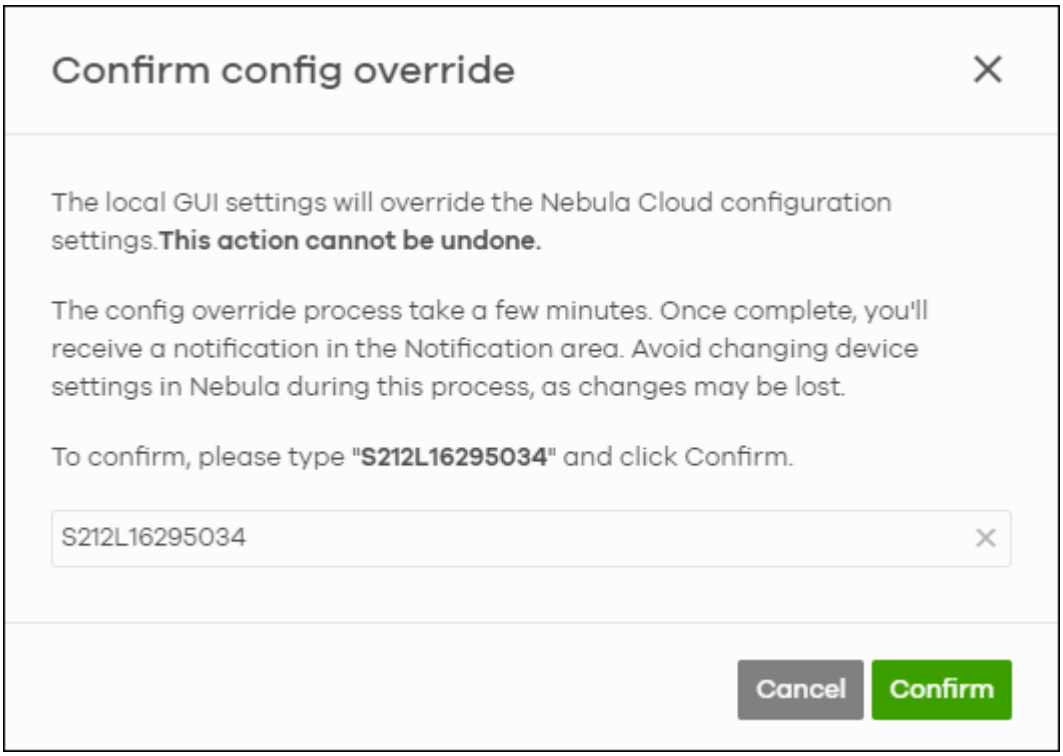


After completing the wizard, you can log in to Nebula Control Center (NCC) to check your firewall status. Ensure the **Configuration Status** shows **Up to date**, indicating the firewall has fully synchronized with the cloud.



If needed, you can click **Config Override** to force a configuration sync from the firewall to the Nebula server immediately.

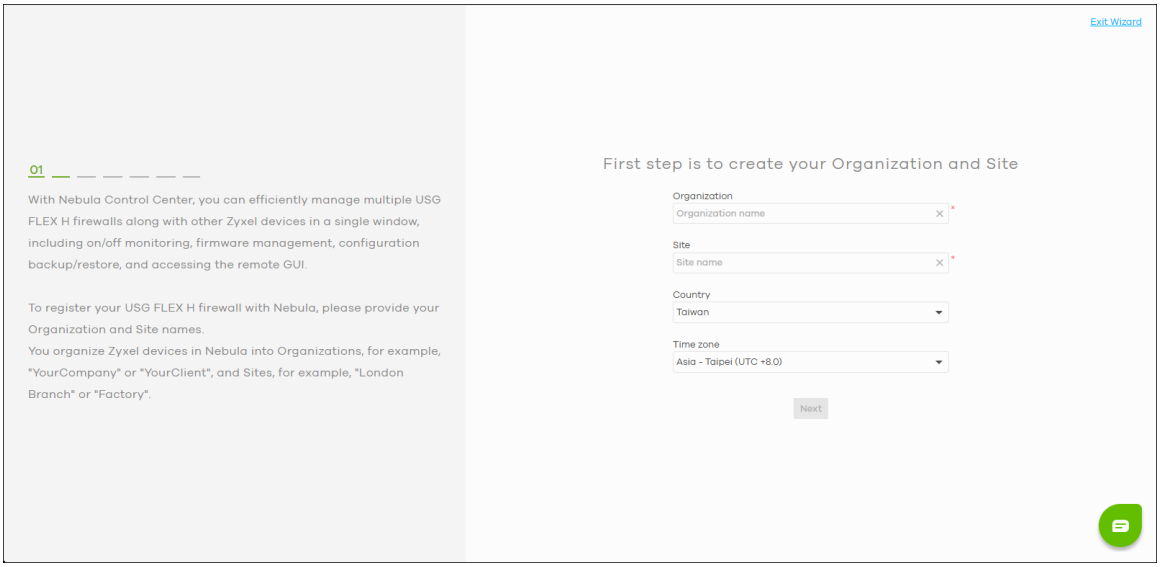




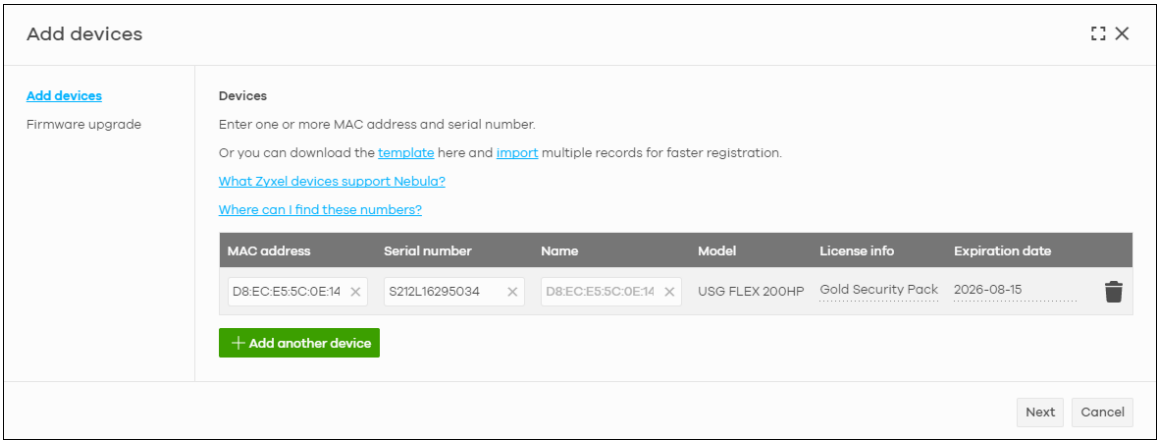
Onboarding via Nebula (Cloud Configuration First)

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.

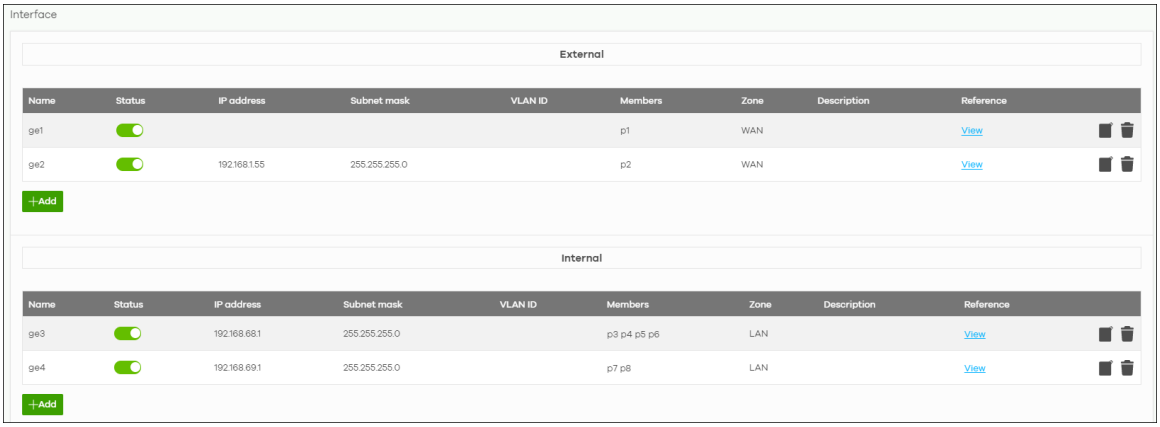
Go to https://nebula.zyxel.com/, log in with your Zyxel account, and create a new Organization and Site.



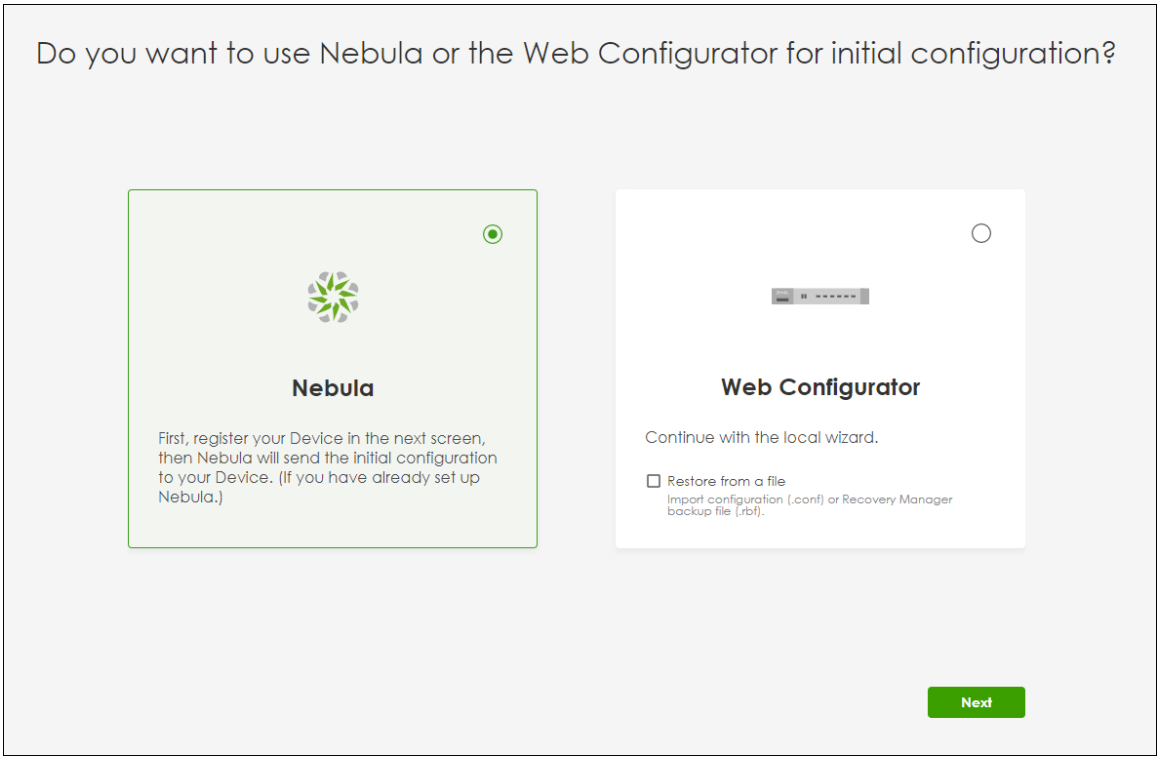
Click **Add** to register your firewall to the created site.



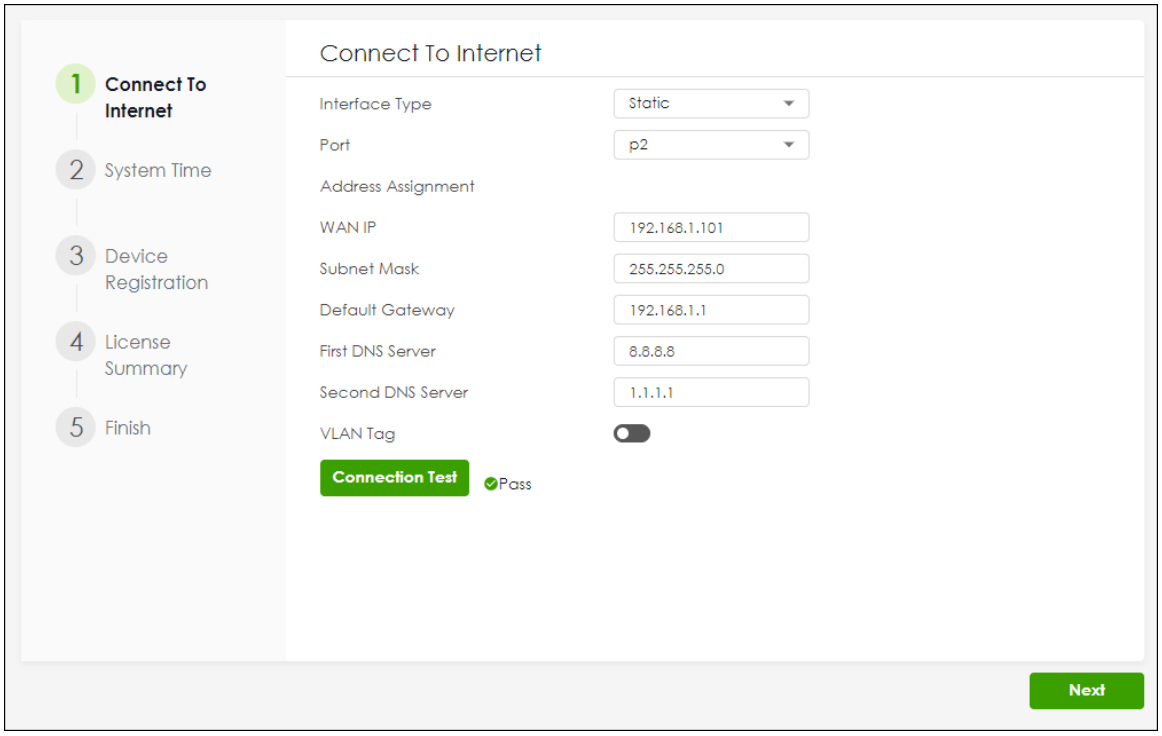
You can pre-configure interface settings in Nebula to match your network environment.



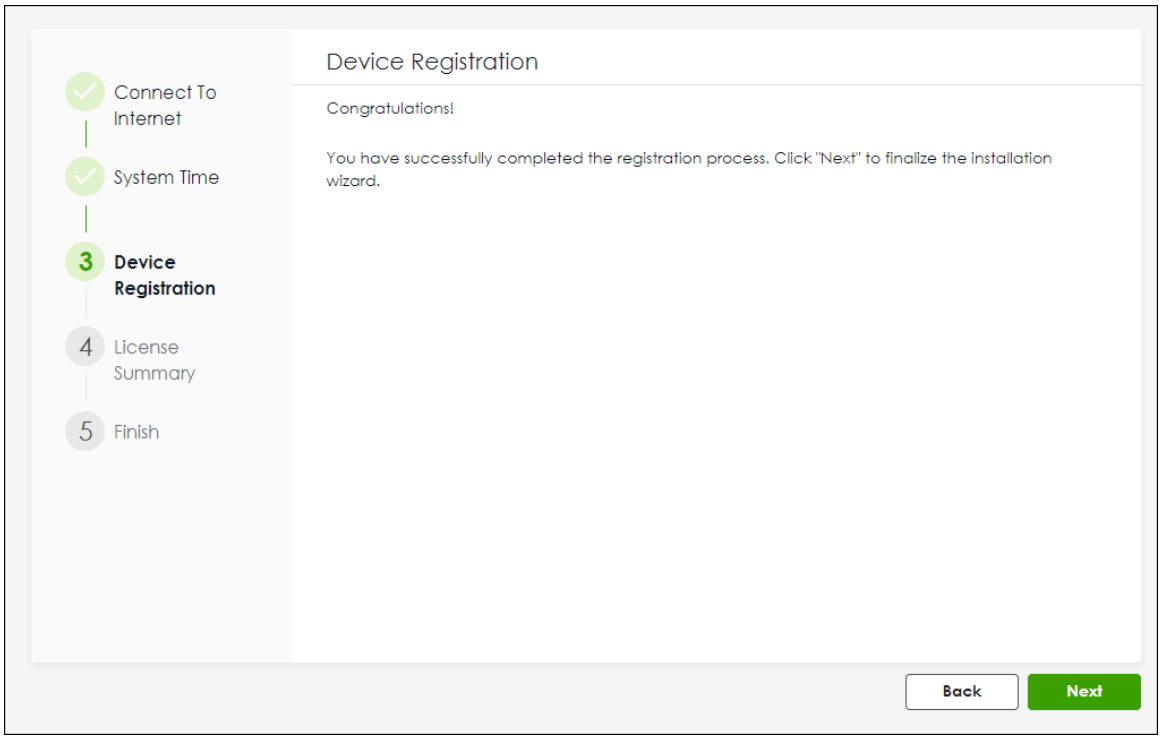
The default WAN setting on the firewall is DHCP. If your Internet connection also uses DHCP, you can simply connect the WAN cable to the firewall without needing to manually configure the device through the wizard.



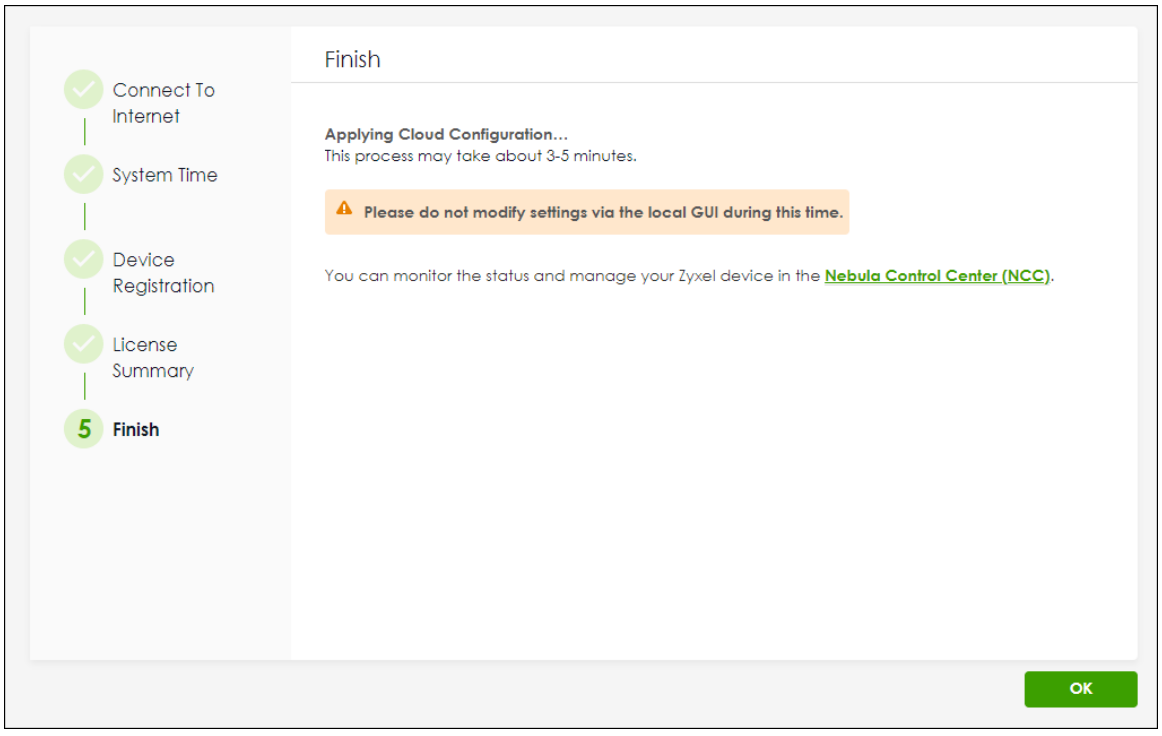
In Step 1, Configure the WAN IP address to ensure the firewall can connect to the Internet.



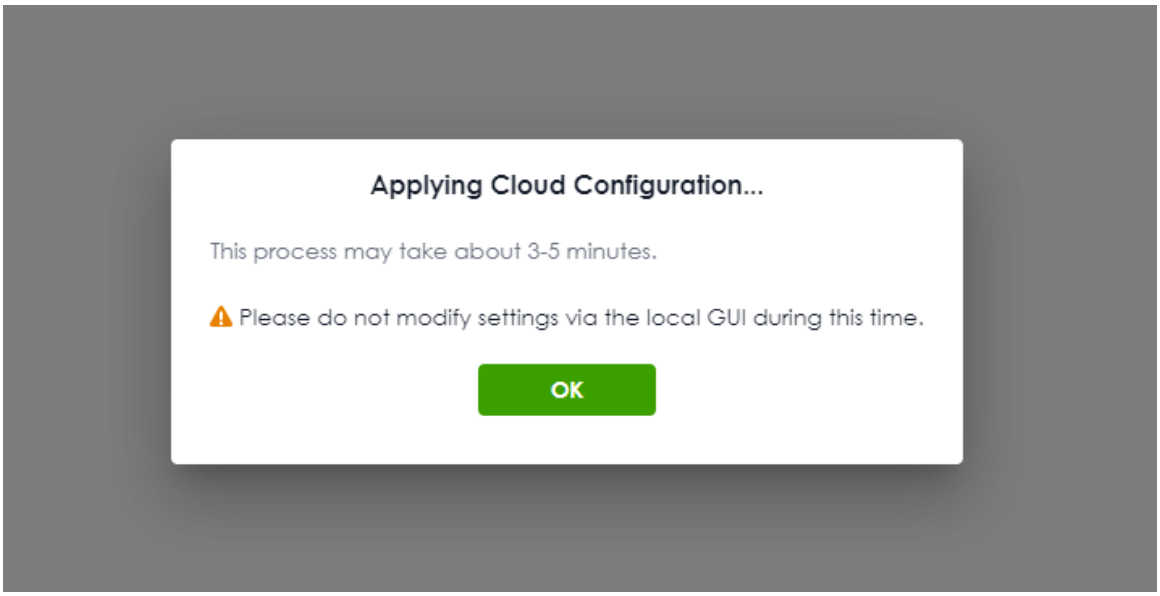
Once connected to the Internet and Nebula CC, the wizard will automatically verify the device's registration status.



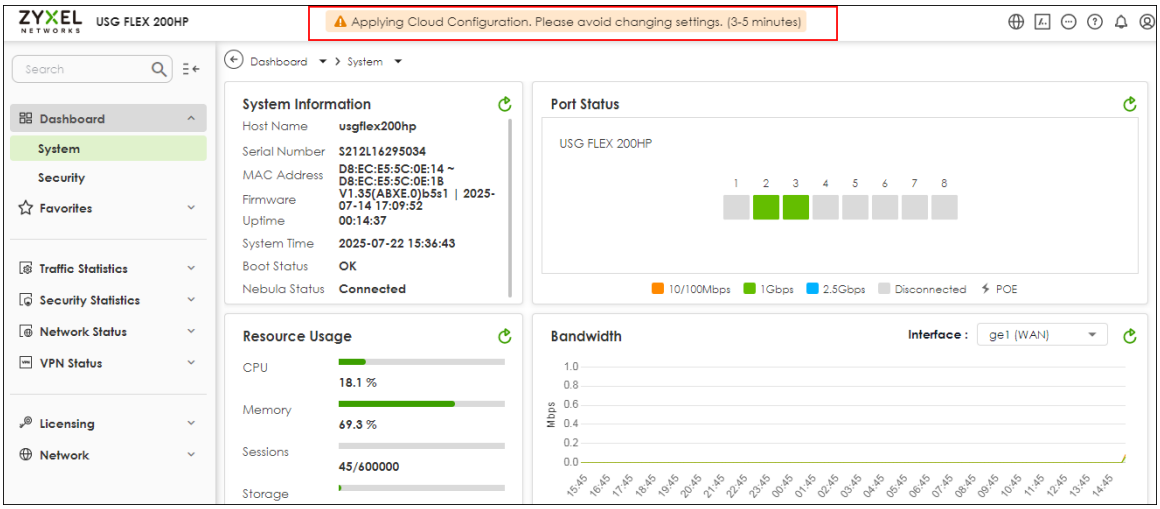
In step 5, Click **OK** to finish the wizard. Please wait 3–5 minutes for Nebula CC to provision the configuration to the firewall.



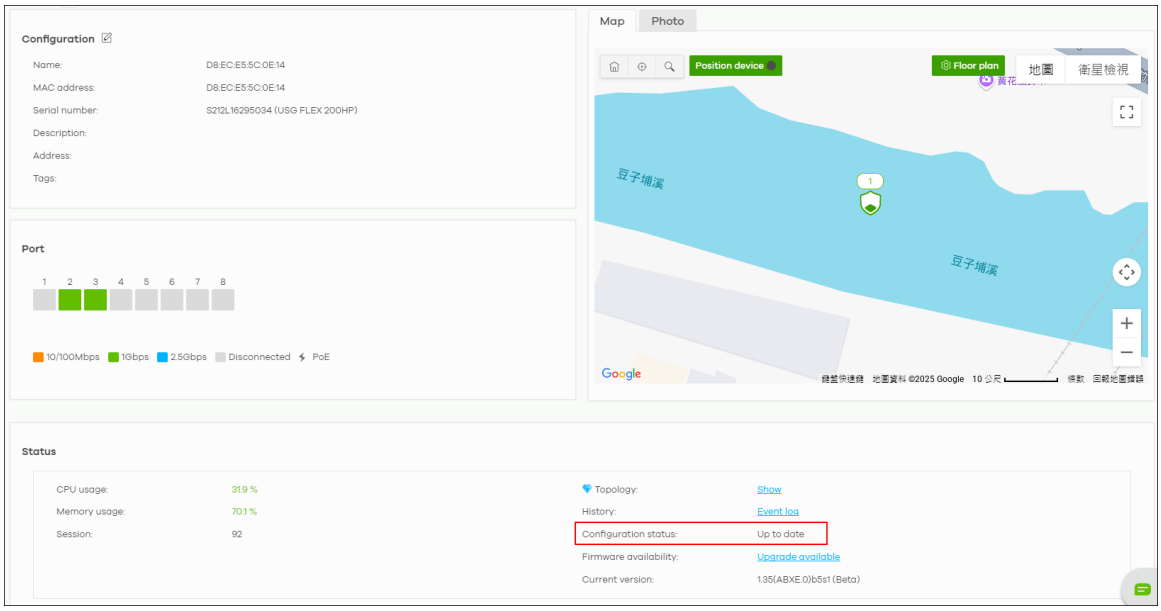
Before the configuration is fully applied, a notification message will appear. You will also see a banner at the top of the page.



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.

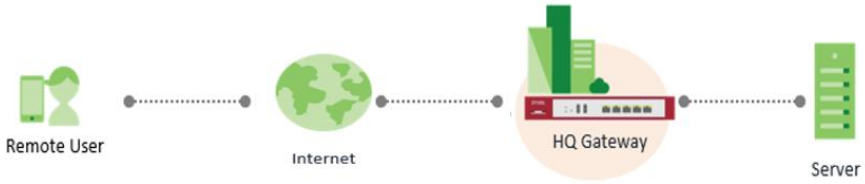


You can also monitor the firewall's status on the Nebula site and ensure the **Configuration Status** becomes **Up to date**.



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.

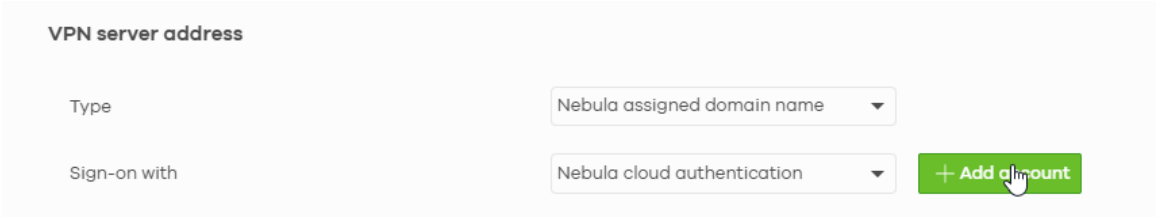


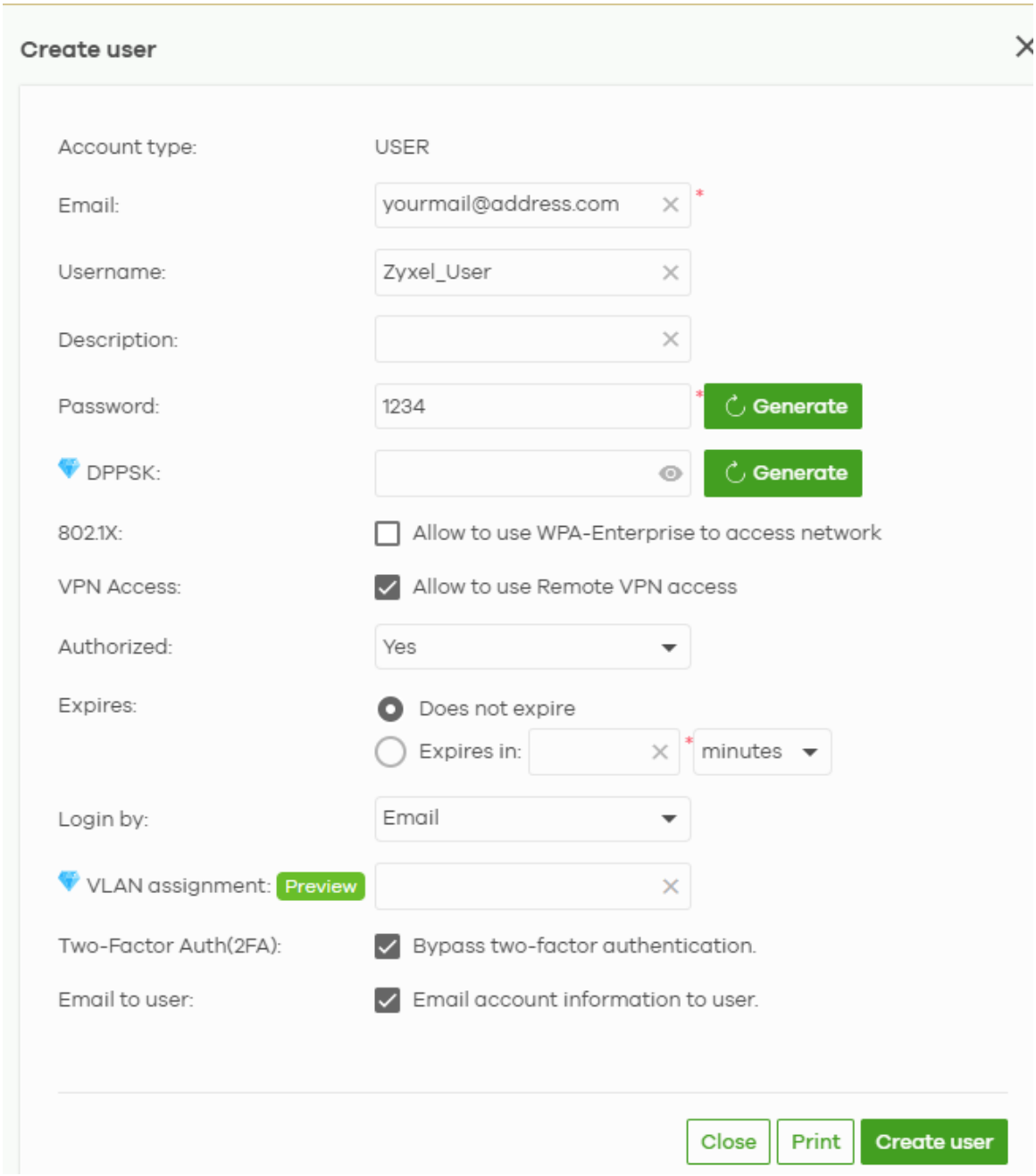
Before You Begin

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.





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.

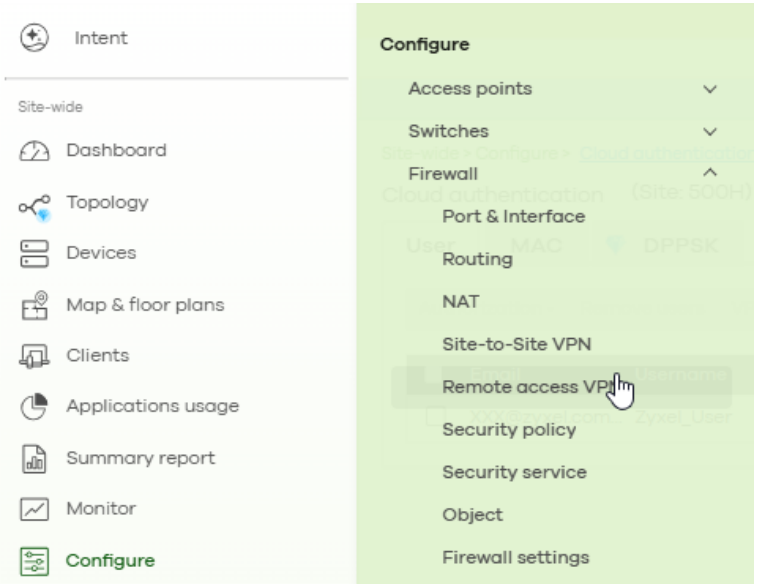
3. Select VPN server address type as ”Nebula assigned domain name”.

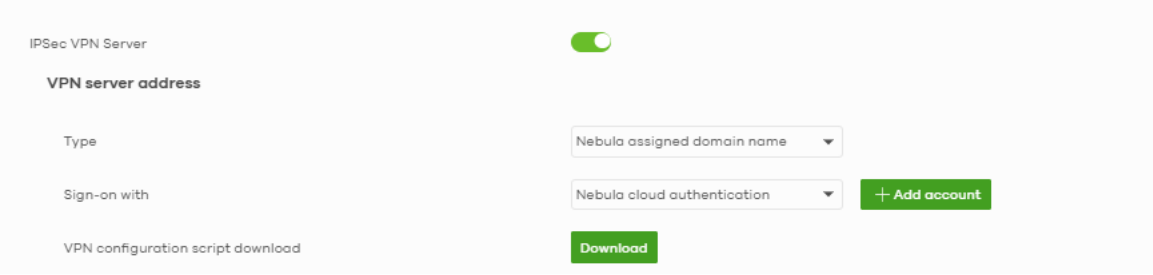
4. Sign-on with selected “Nebula cloud authentication” (The user authentication account can be also added on this page.

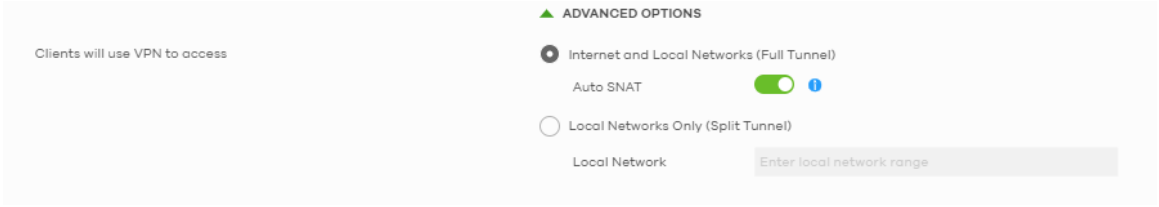
* Under The ADVANCED OPTIONS, you could base on the requirement to customized the settings.

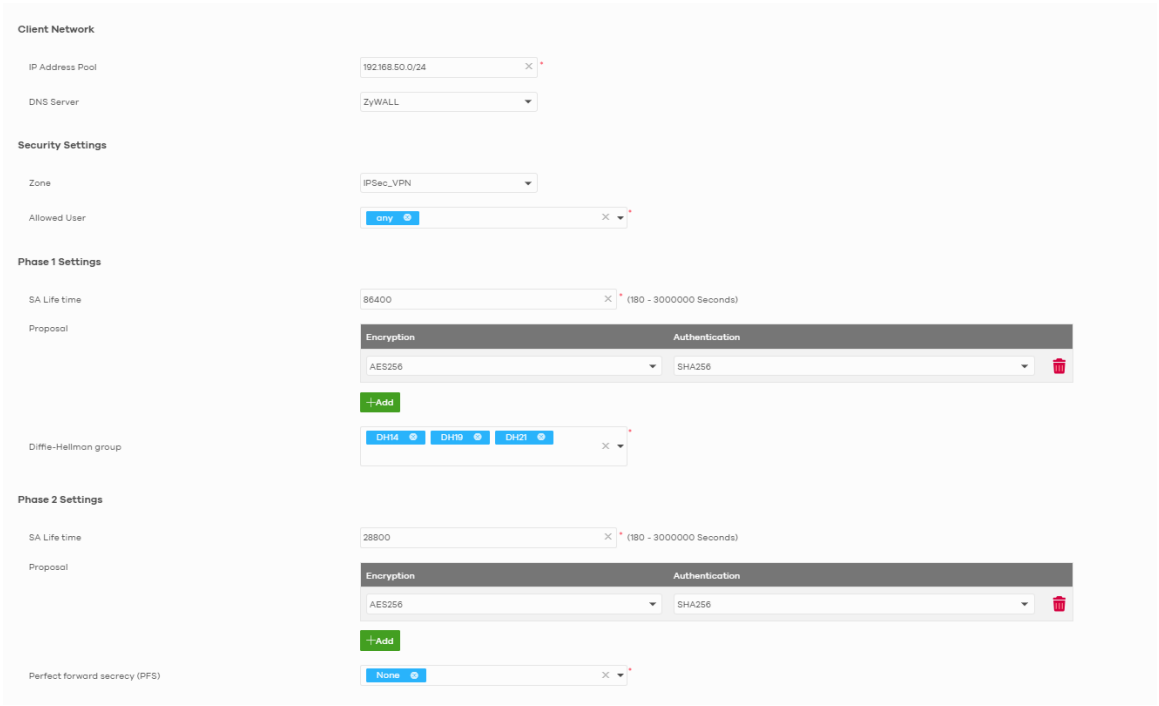
5. Choose the **tunnel type** based on your network policy:
   - **Internet and Local Networks (Full Tunnel)**: All traffic goes through VPN
   - **Local Networks Only (Split Tunnel)**: Only specified subnet(s) go through VPN
6. The default address pool for IKEv2 remote access VPN is **192.168.50.0/24**

Note: Cloud auth. account only support “any” users.

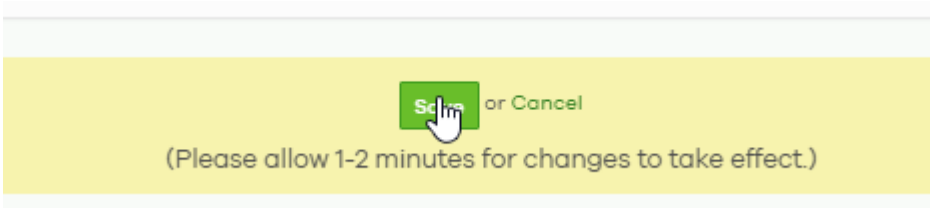








Don’t forget to click save before leaving the page.



Note: VPN configuration script download required to wait for synchronization

It may take 1-2 minutes to synchronize.

Enable SSL VPN on Nebula

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

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

   Under the ADVANCED OPTIONS, you could base on the requirement to customized the settings.
5. Choose the **tunnel type** based on your network policy:

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

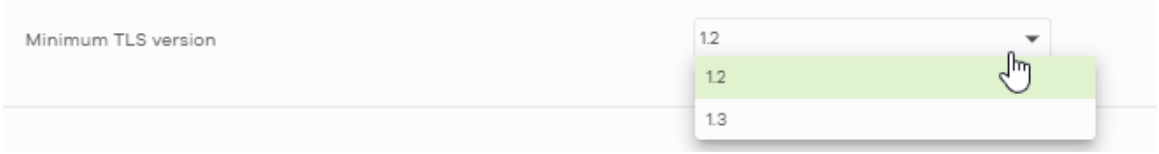
   Local Networks Only (Split Tunnel): Only specified subnet(s) go through VPN

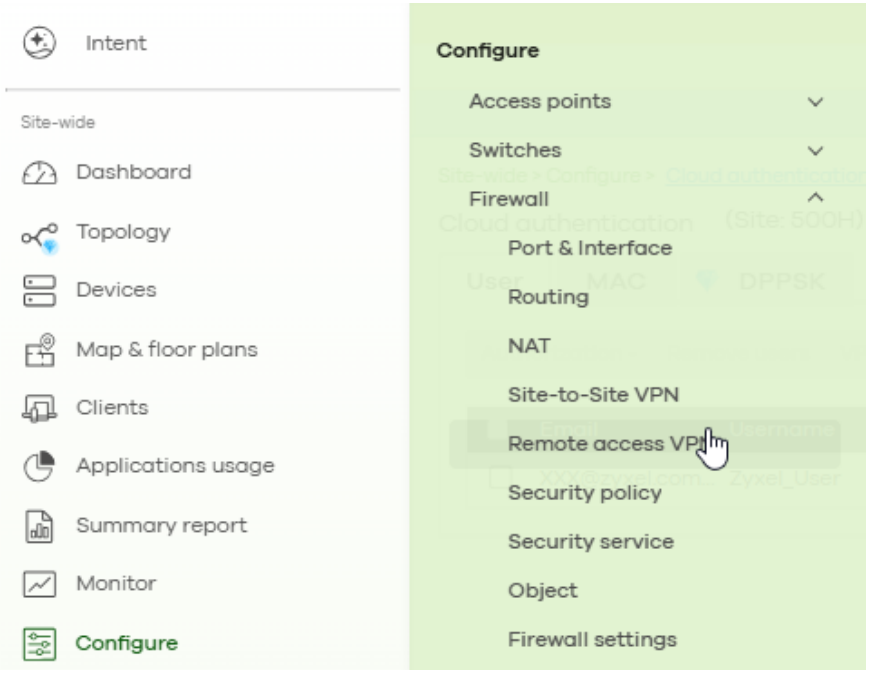
6. The default address pool for SSL VPN is **192.168.51.0/24**
7. Assign allowed users for SSL VPN access

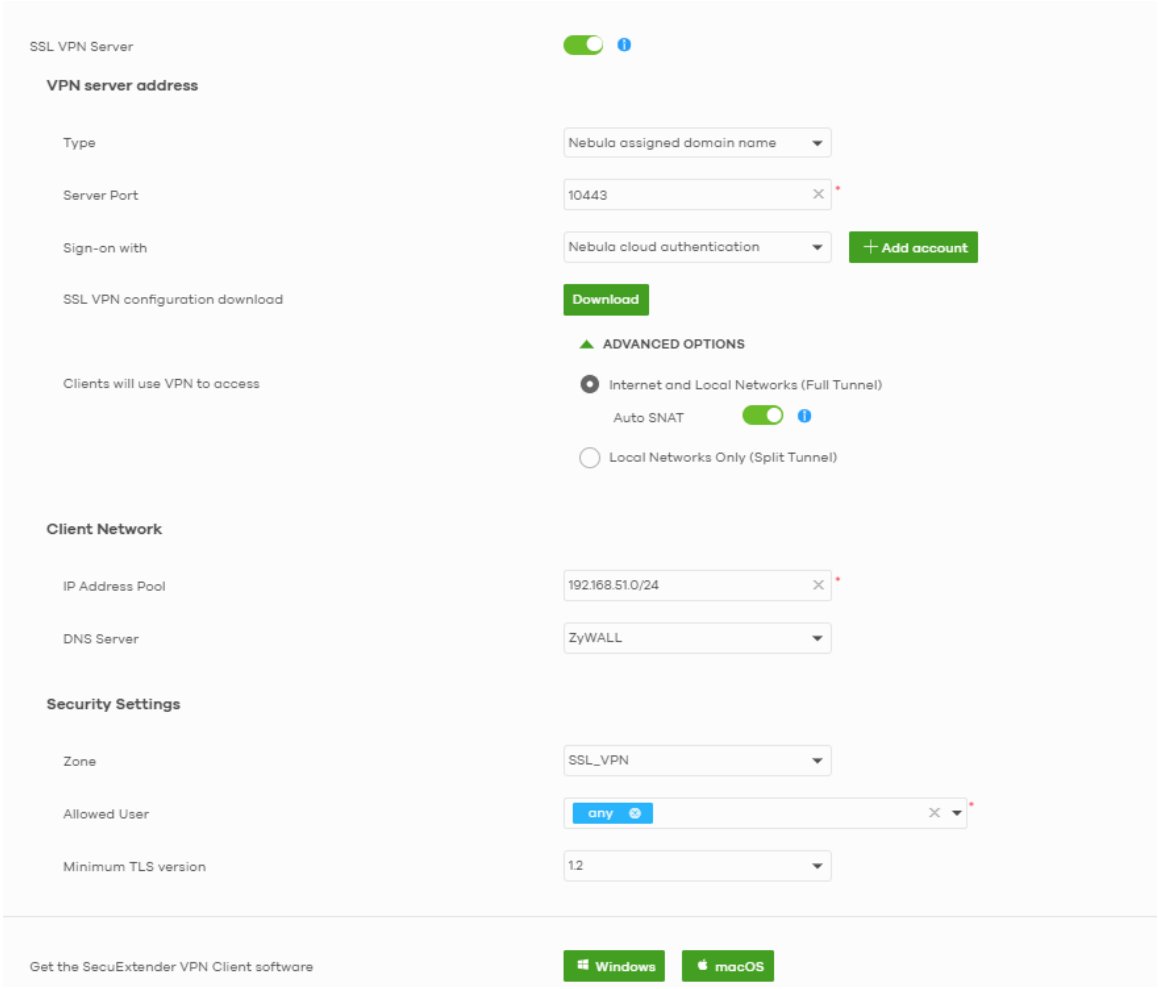
   Note: Cloud auth. only support "any" user

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

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

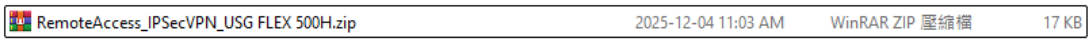




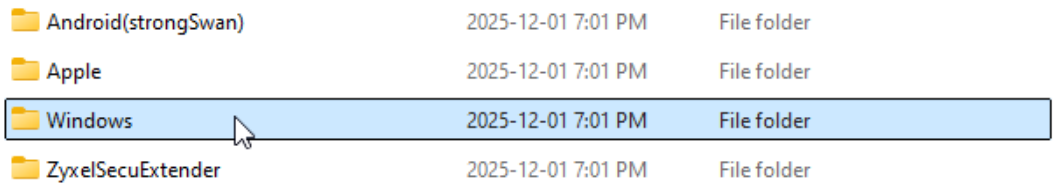


Configure IPSec VPN on the Laptop/Mobile

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

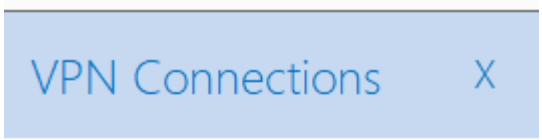


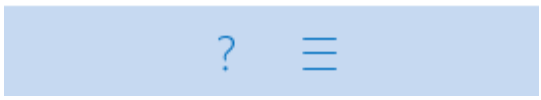
After download, will require to unzip the file



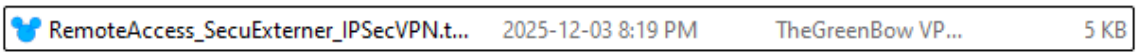
Set Up Remote Access on SecuExtender VPN Client (Windows)

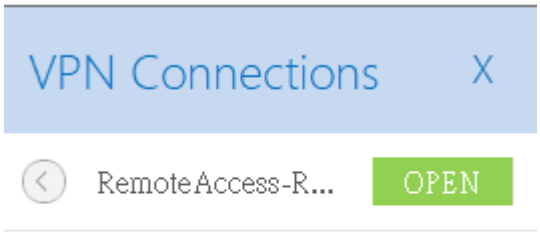
1. Launch the client



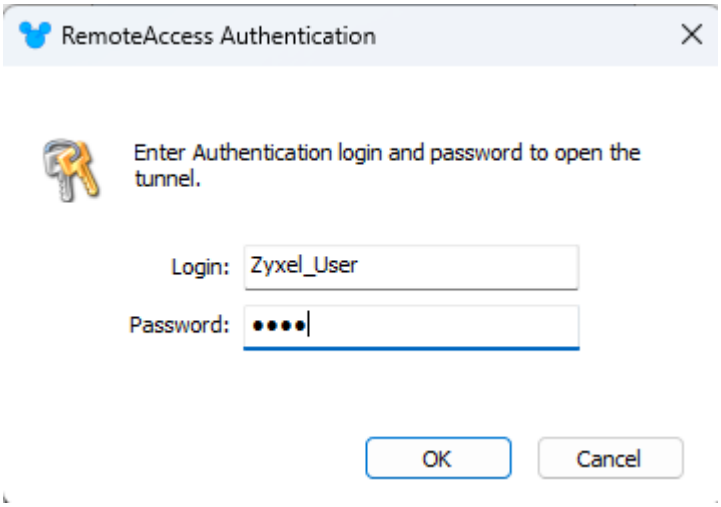


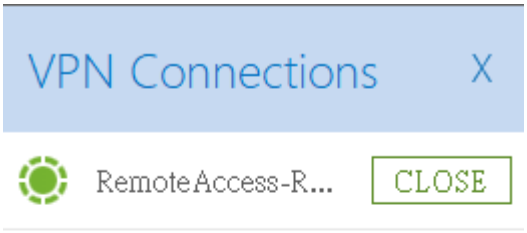
2. Double click the script file





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



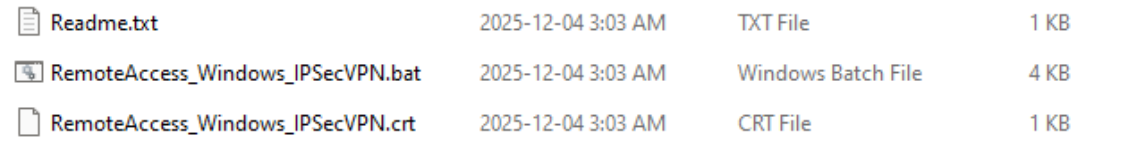


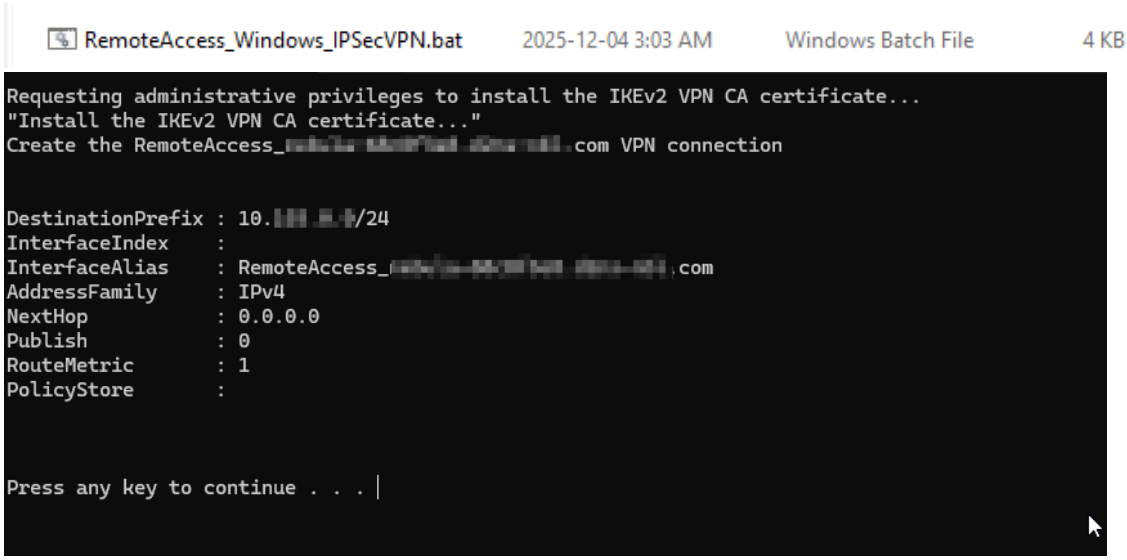

```
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::9b75:9035:5ef6:9150%23
IPv4 Address. . . . . . . . . . . : 192.168.50.1
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.50.2
```

```
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
```

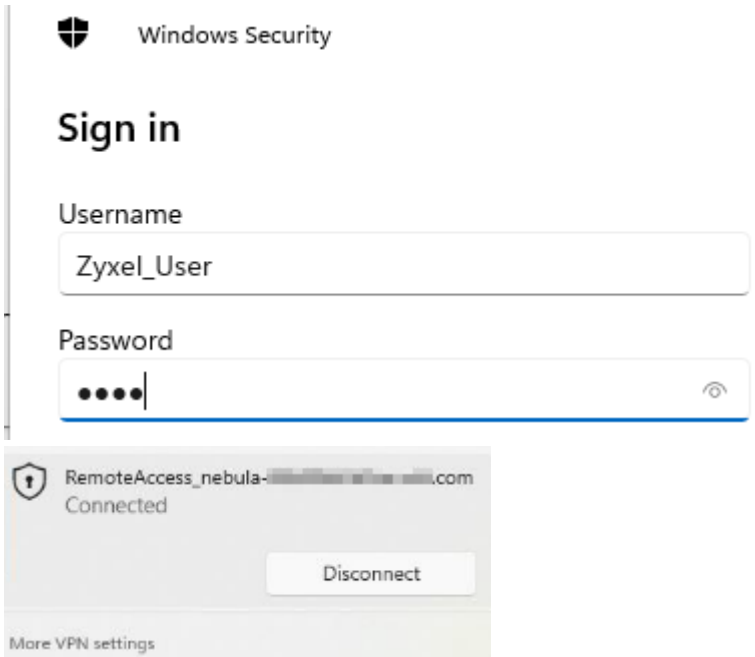

Set Up IKEv2 VPN On Windows (Native IKEv2 Client)

1. Installed the script
   Note: The certificate and bat file should be on same folder.





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



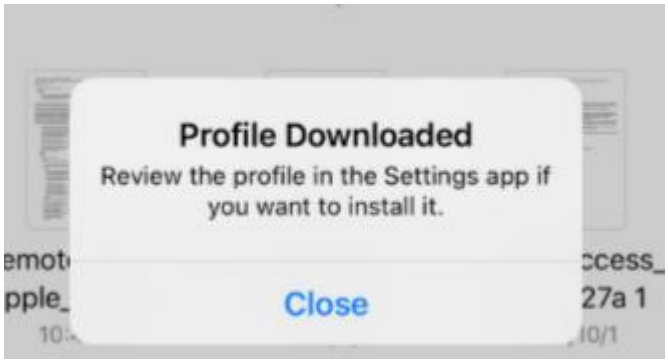

```
PPP adapter RemoteAccess_nebula [redacted] com:

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

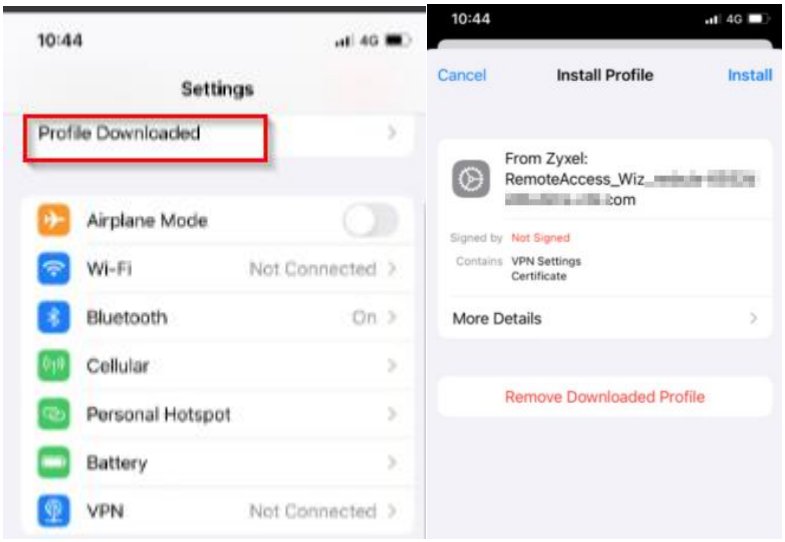
```
C:\Users\[redacted] ping 192.168.168.1

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

Set Up IKEv2 VPN on iOS

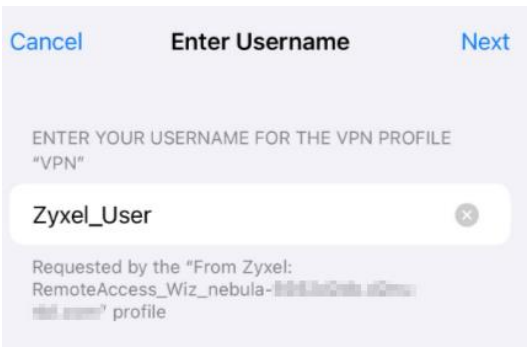
1. Send the scripts below to the iOS/macOS/iPadOS device. => macOS need manual change the auth type

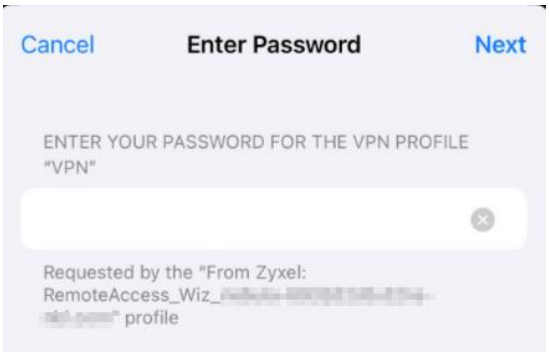
2. Go to **Settings** > **Profile Downloaded**, then **Install**
(Mac device: System Settings > Network / VPN)



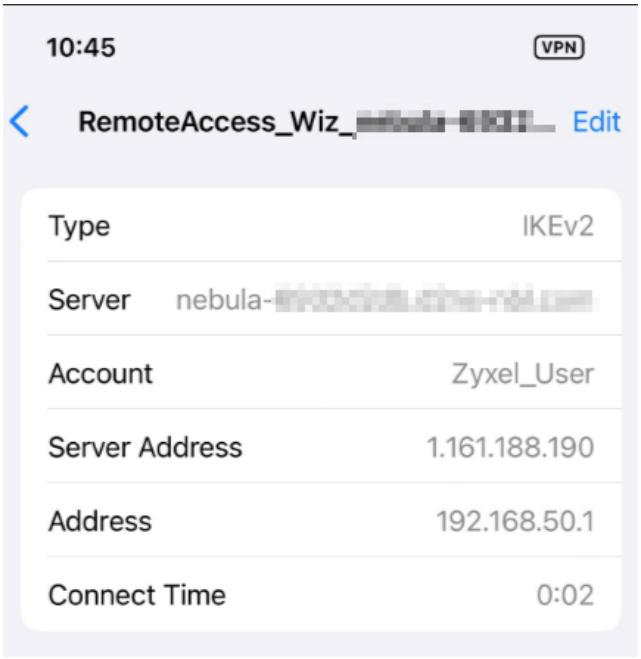


3. Enter your username and password.



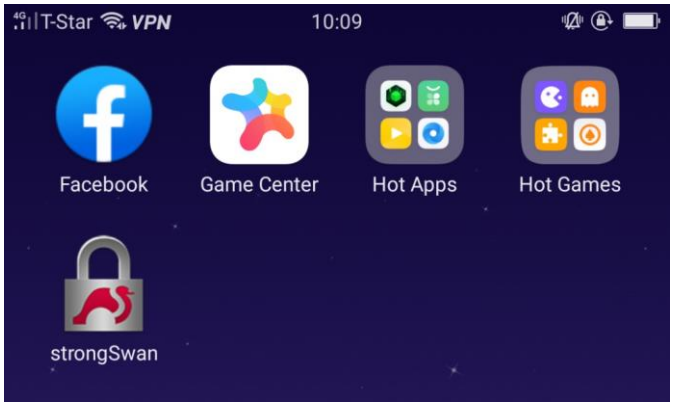


4. Connect to the VPN from the **Settings** > **VPN** menu.

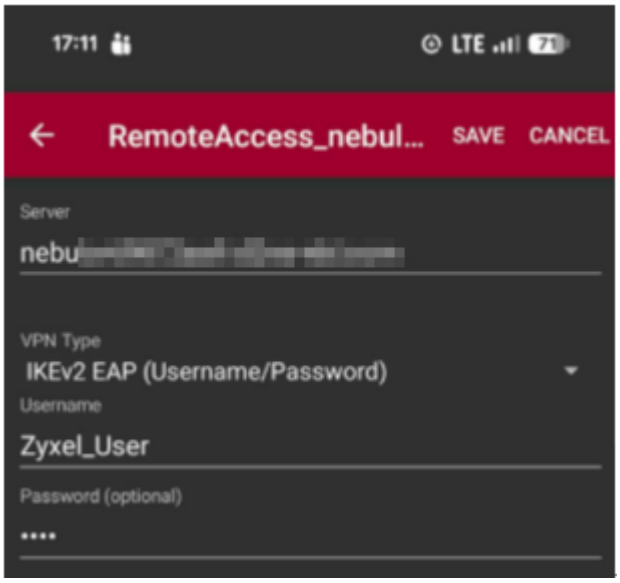


Set Up IKEv2 VPN on Android (strongSwan App)

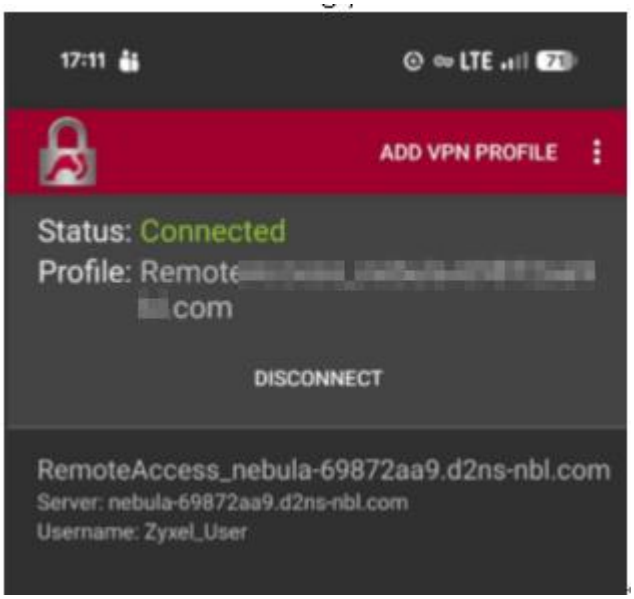
1. Install the **strongSwan VPN Client** from Google Play Store



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

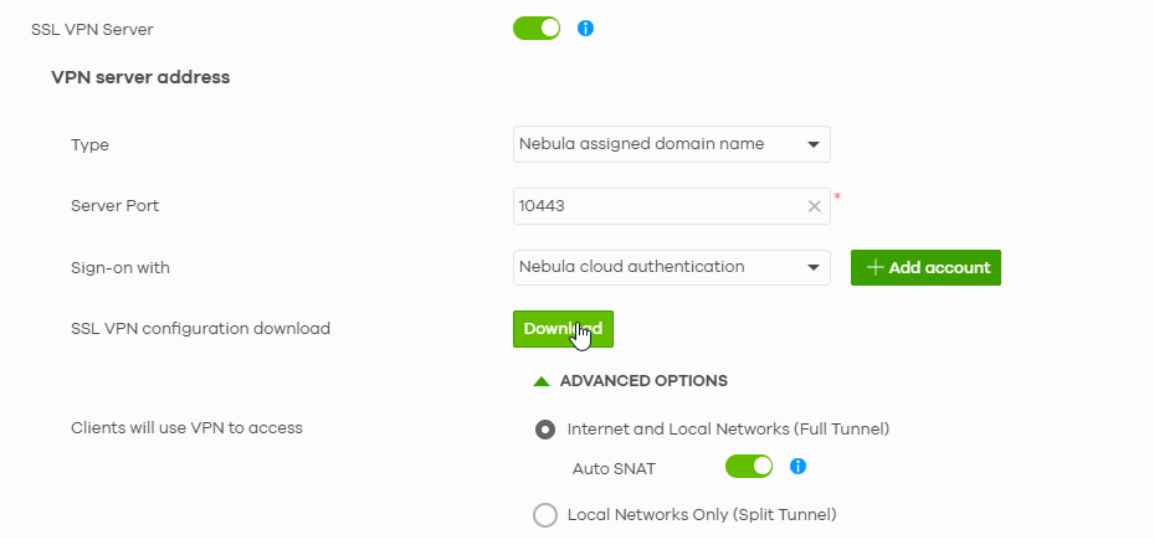


4. Connect to the VPN using your credentials

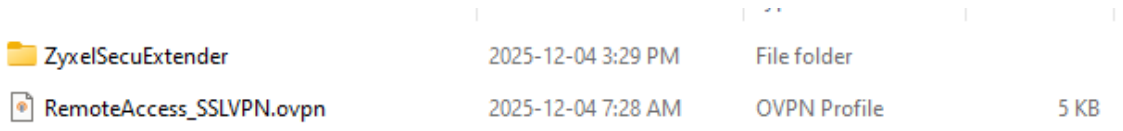


Configure SSL VPN on the Laptop/Mobile

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

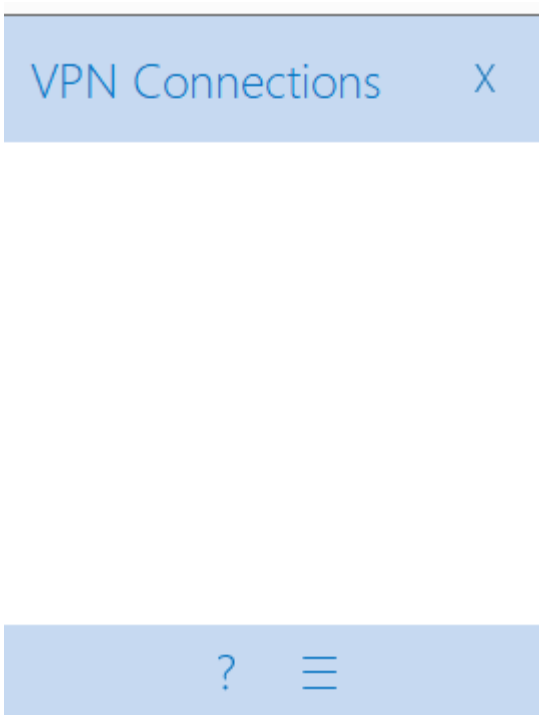


3. After download the file you will see two scripts file

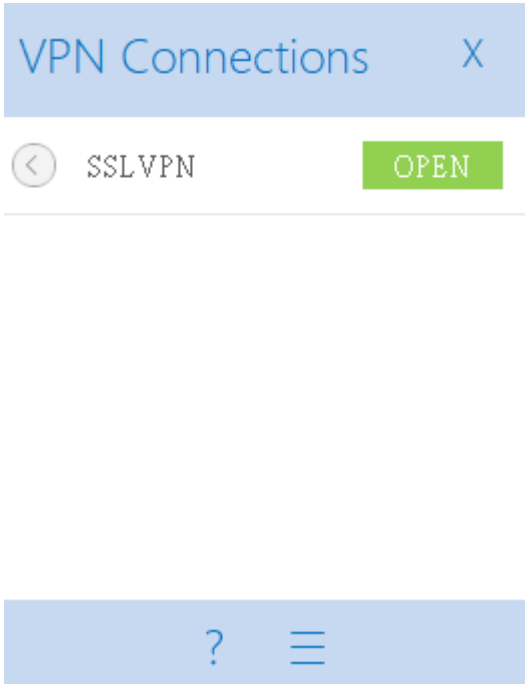


Set Up Remote Access on SecuExtender VPN Client(Windows)

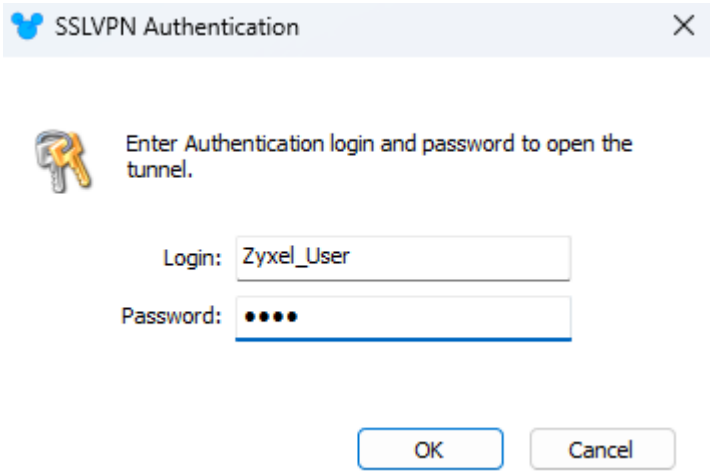
1. Launch the client

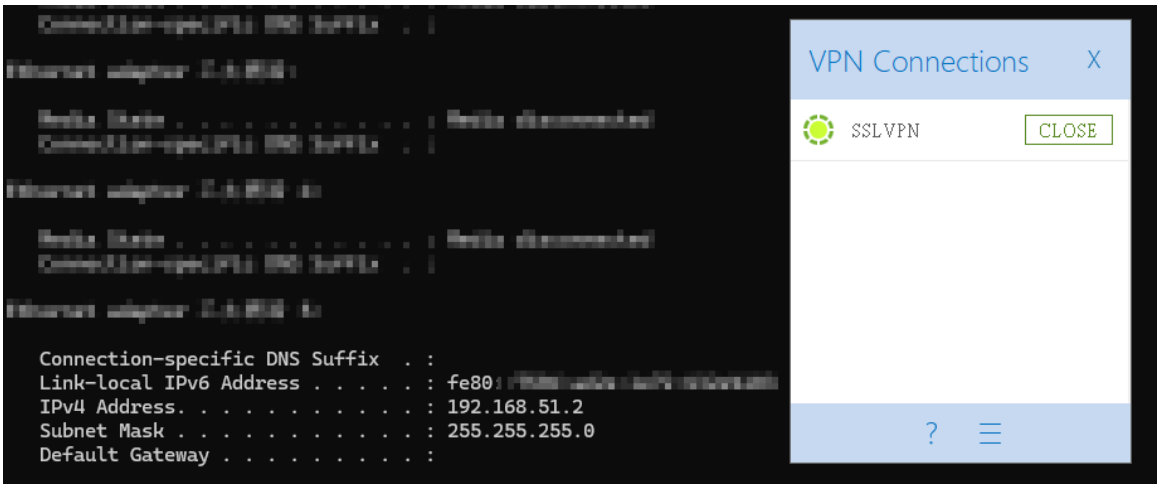


2. Double click the script file



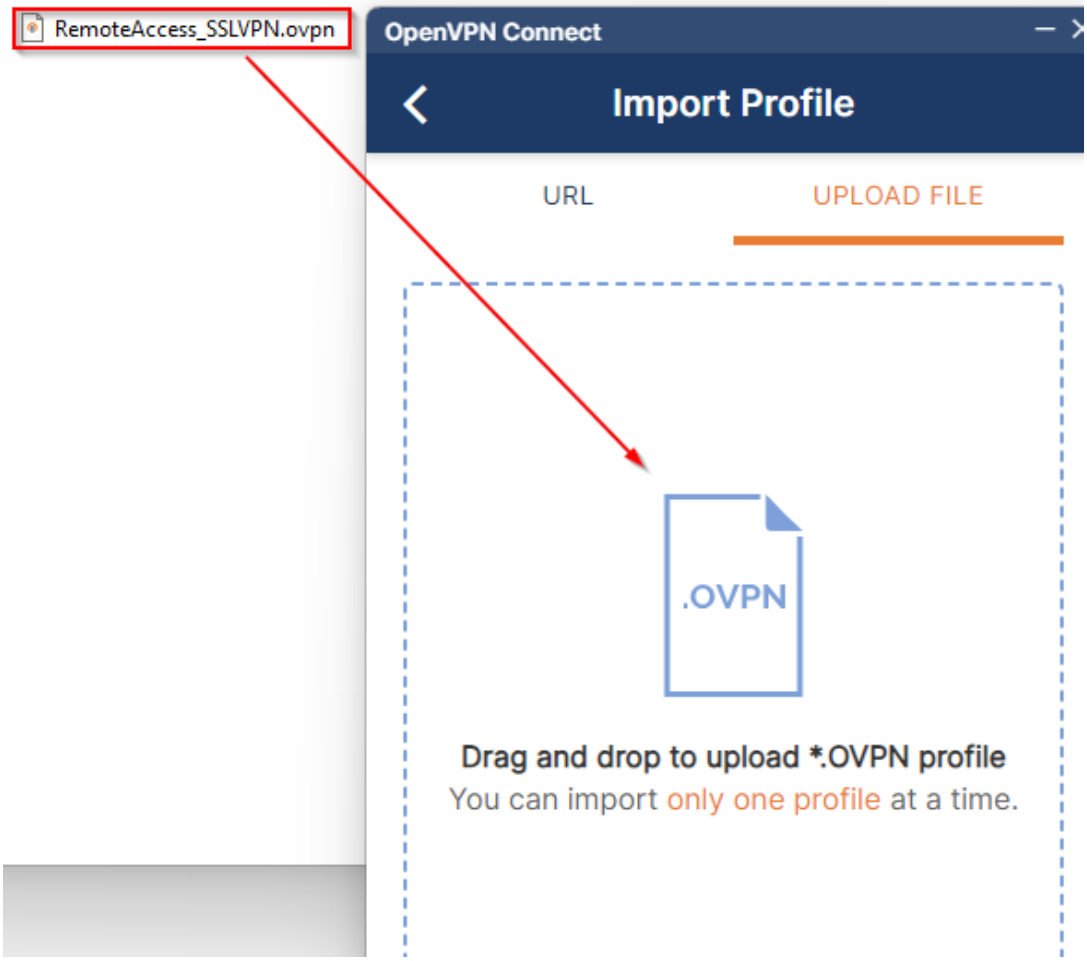
3. Click OPEN and type account and password set on Nebula authentication



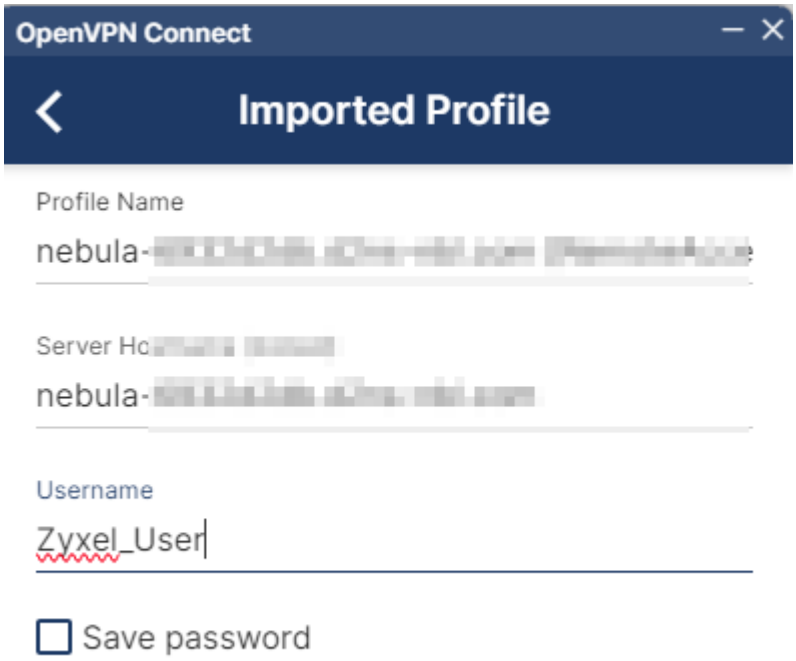


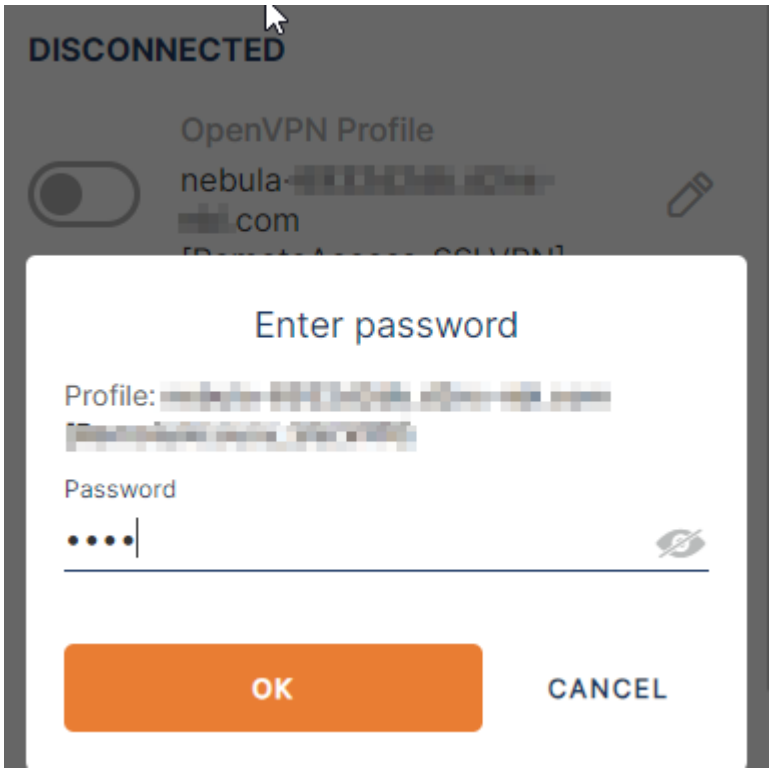
Set Up Remote Access on SecuExtender VPN Client(Windows)

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

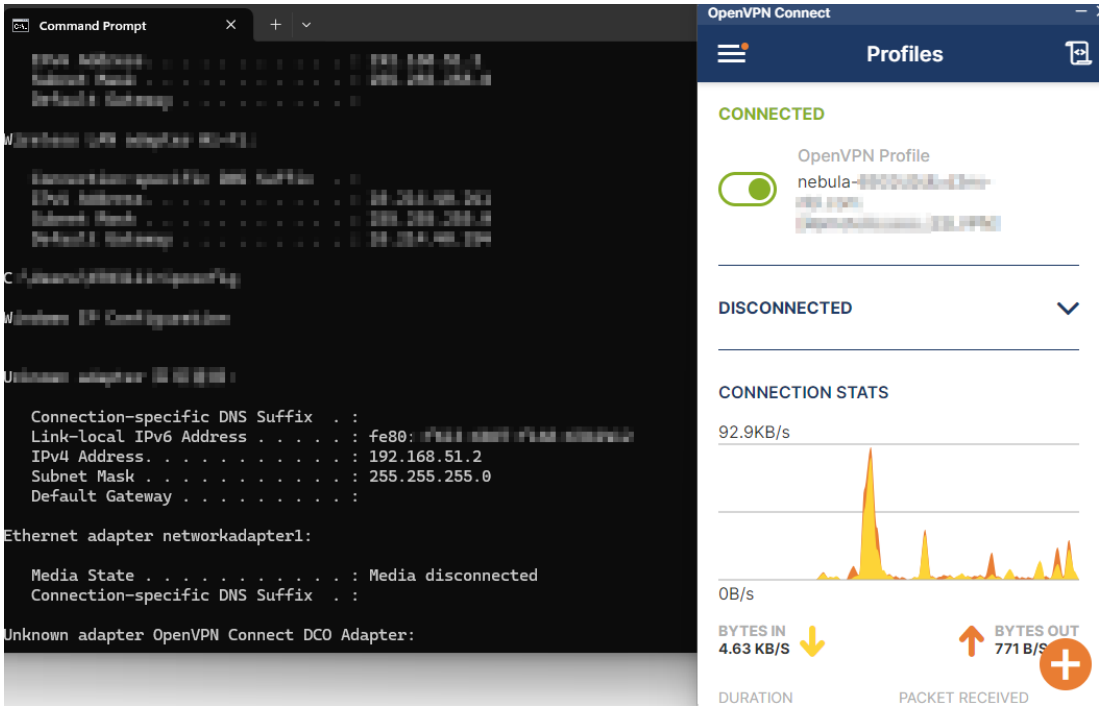


2. Enter Username and password



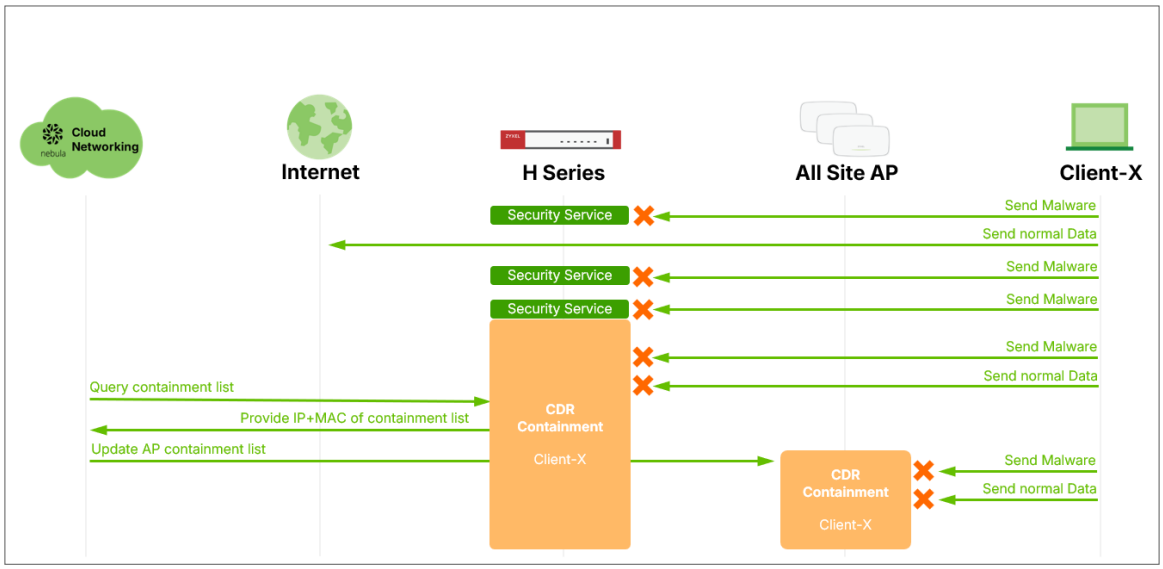


3. The connection should work



How to Configure CDR on Nebula

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



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 700H (Firmware Version: uOS V1.38).

Set Up the CDR on Nebula

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

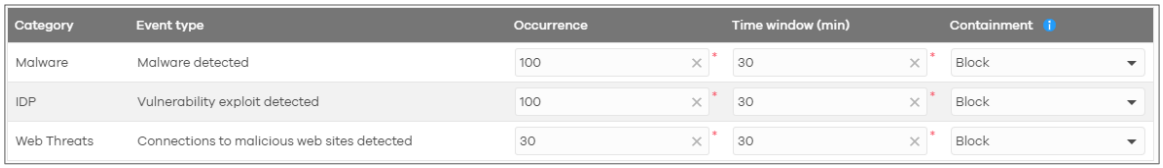
We have 3 actions for containment:

Alert: Send alert mail to recipient

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

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

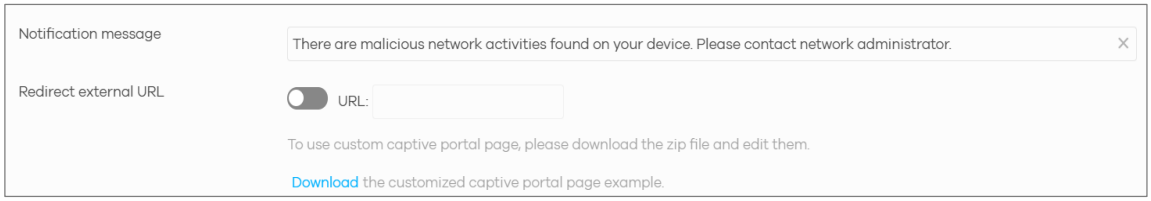
In this guide, we set the containment to block.



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.



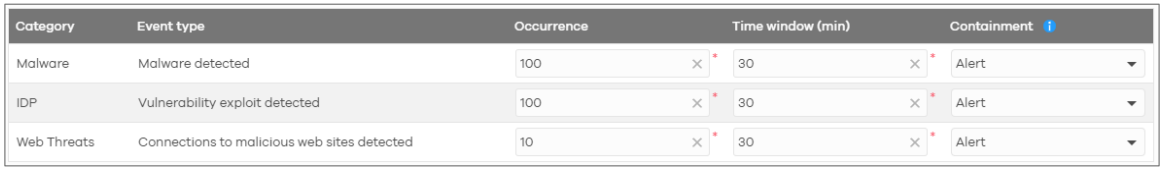
Set the Containment duration to 60 minutes. Once the client triggers CDR, the host will be blocked for 60 minutes.

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

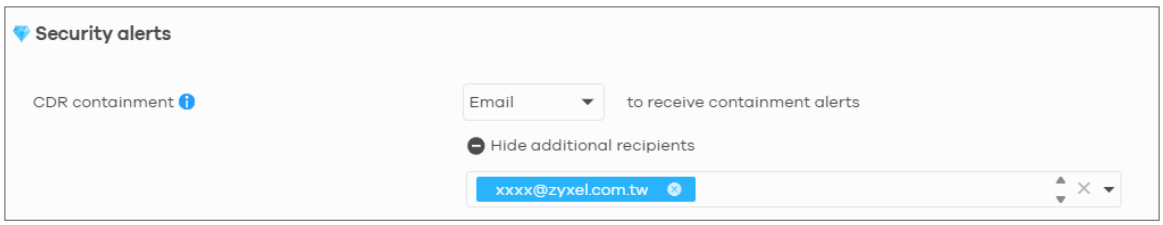
Set Up the containment to Alert

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

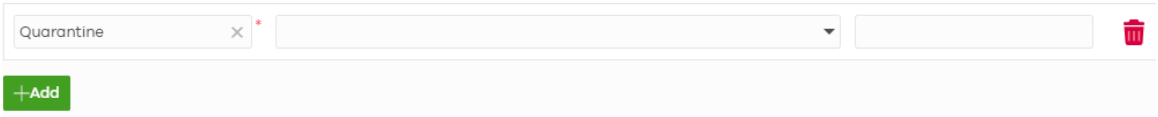


Set Up the containment to Quarantine

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.



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

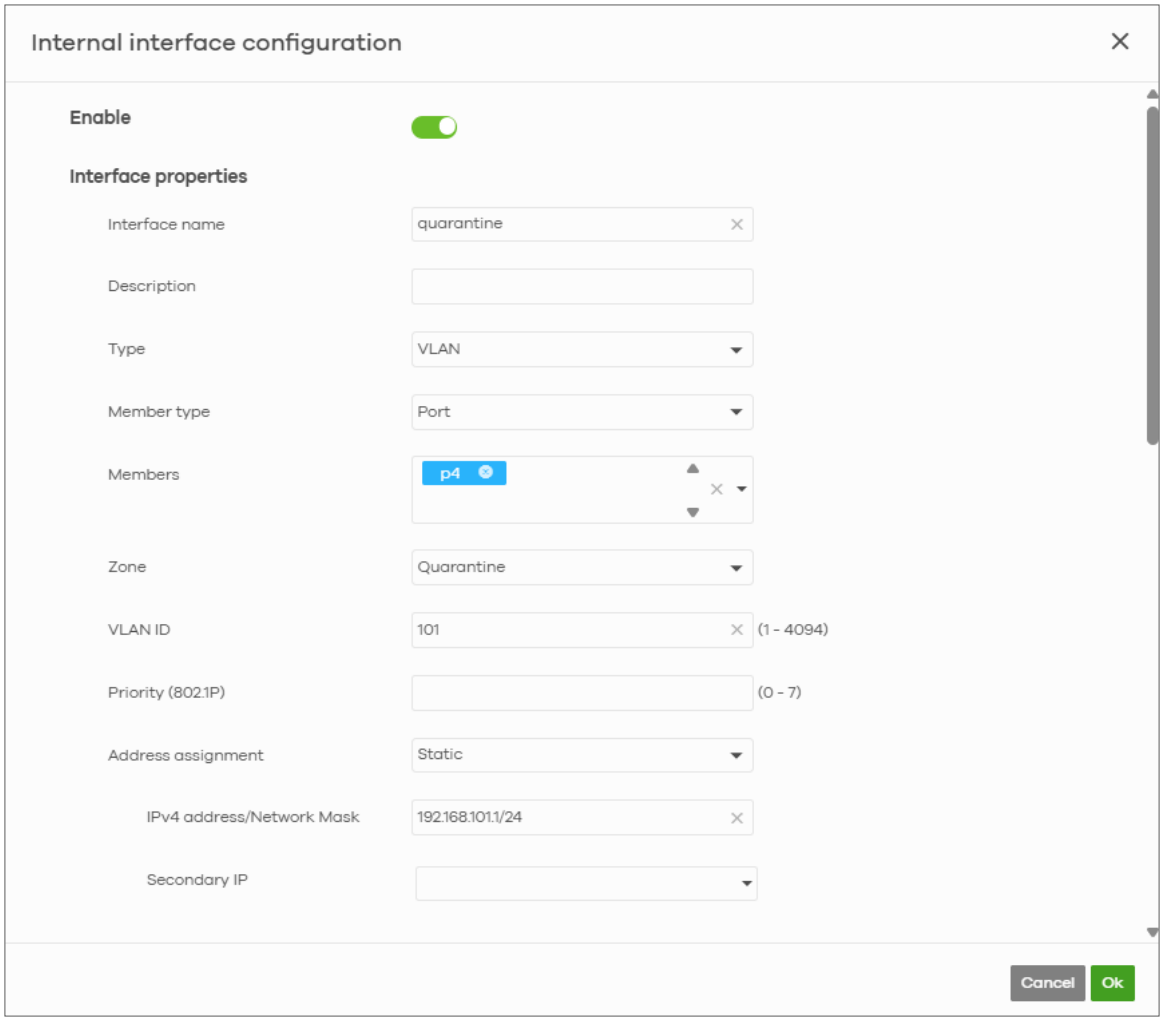
Member = p4

Zone = Quarantine

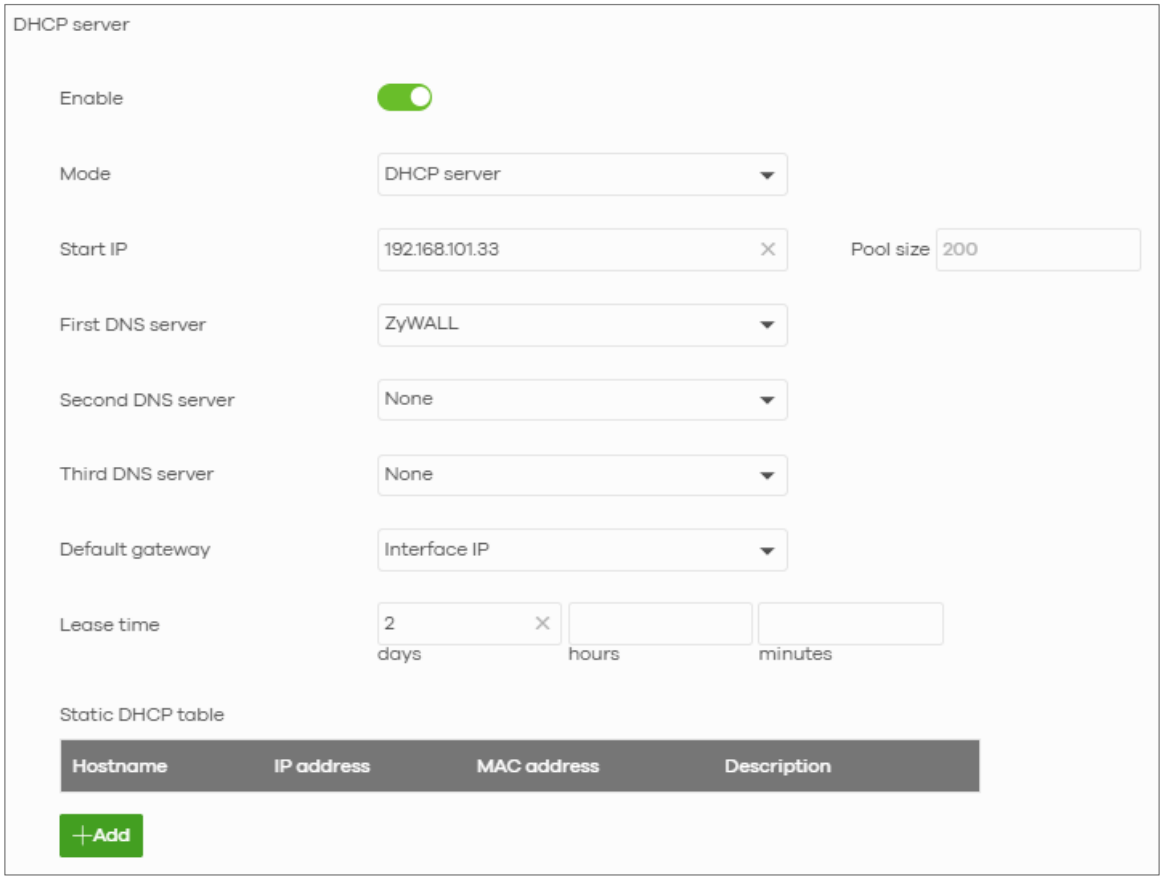
VLAN ID = 101

Address assignment = Static

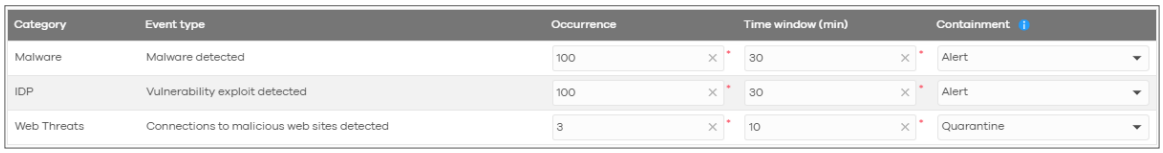
IPv4 address/Network Mask = 192.168.101.1/24



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



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



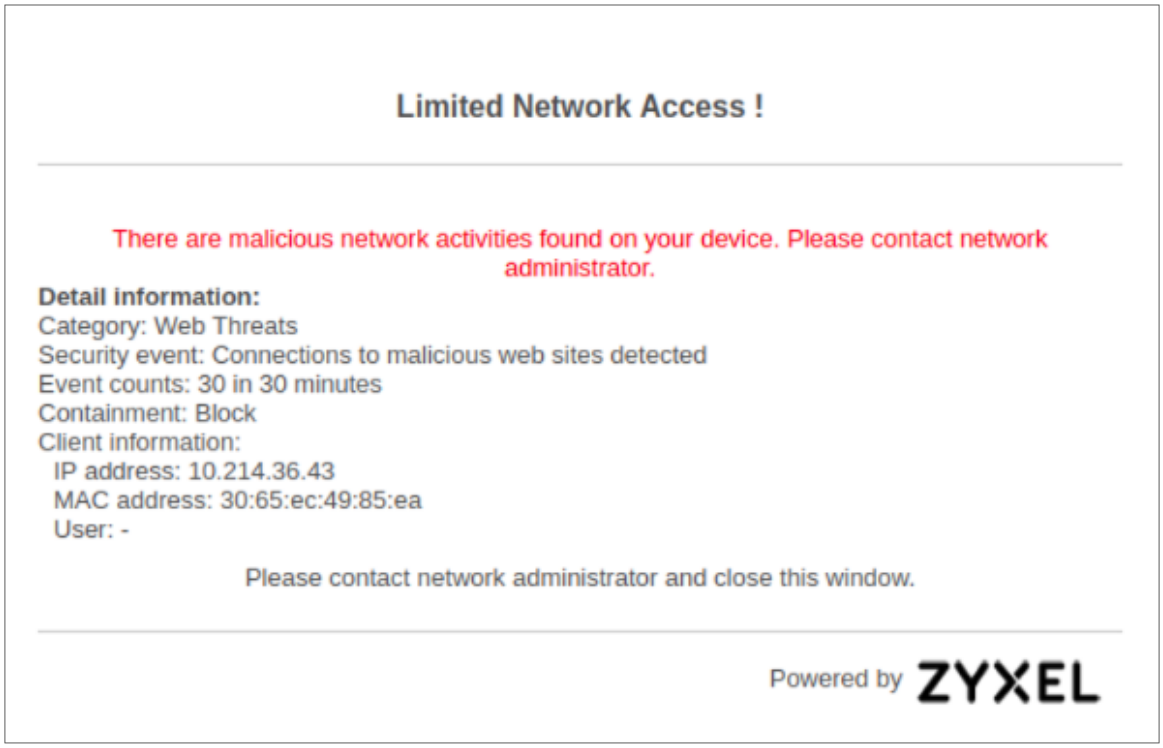
Fill in the VLAN ID to assign a quarantine VLAN.

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.

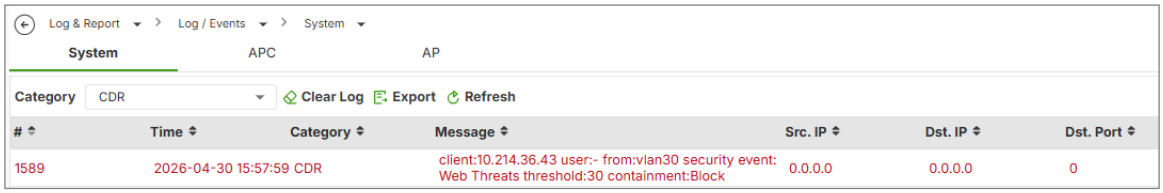
Note: This feature requires a license. Gold security pack is needed to enable this feature, and each Security service must be enabled because CDR relies on Security service (Anti-Malware, Intrusion Prevention System (IPS), Web Threats) to trigger CDR

Verification

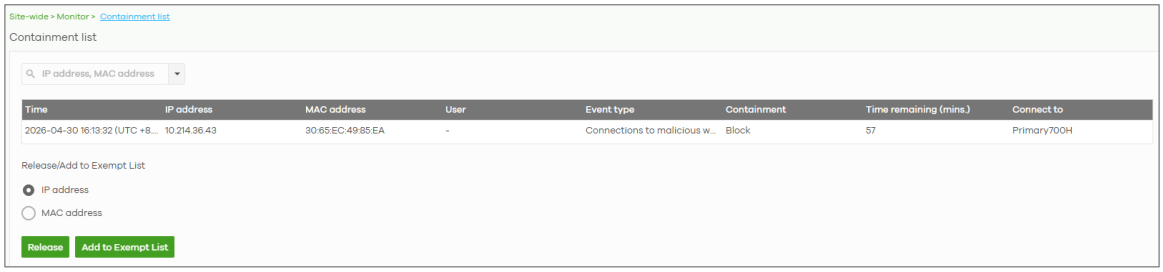
If clients access a malicious site, they will be redirected to a blocked page.



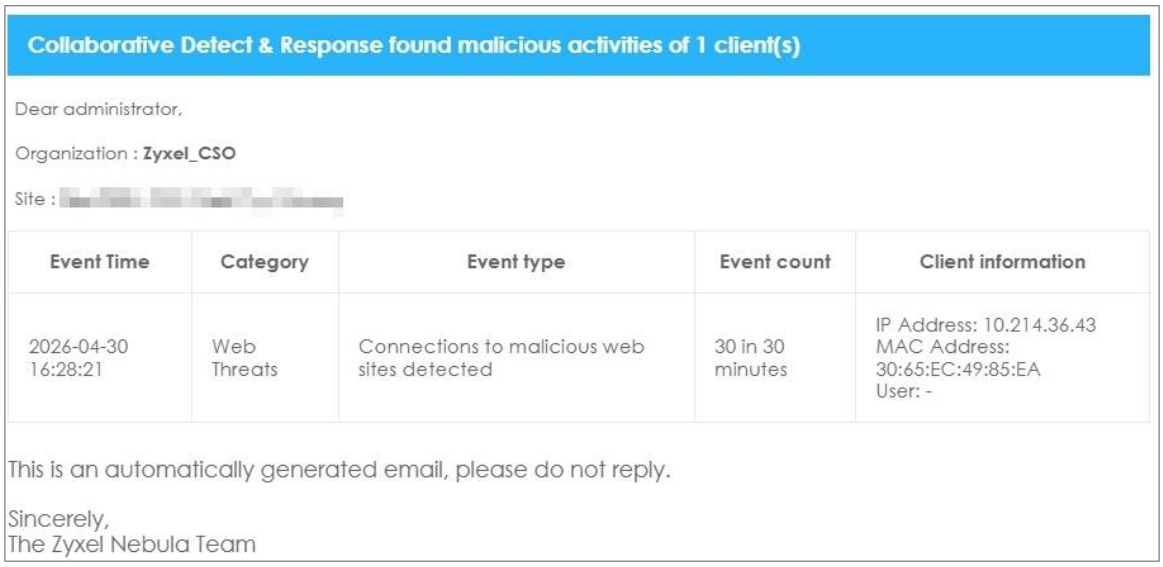
Navigate to Log & Report > Log/Events > System, and we can see the blocked log as shown below.



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.

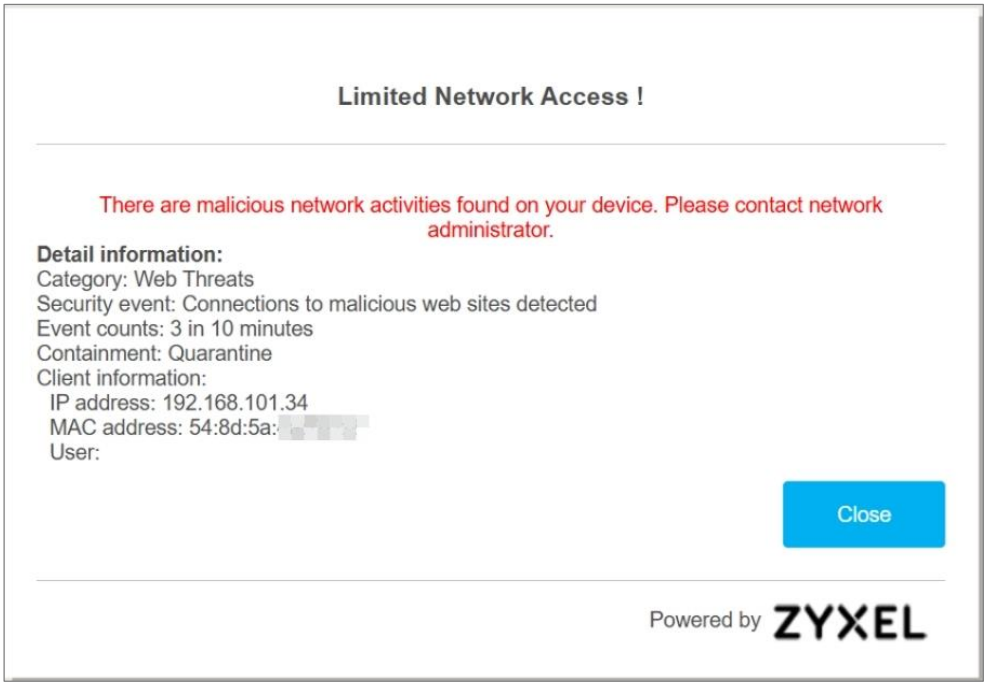


If you select the containment to alert, you will receive mail content as below.

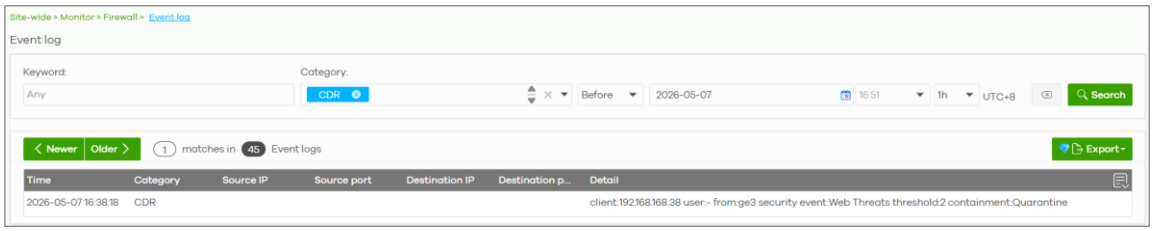


For the quarantine scenario, when a station triggers web threats, it will be redirected to a blocked page first.

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



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



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

