Configuration Guide
Omada VPN Client

Free VPN client for Omada routers.

- **Home**

  Check VPN connection details, quickly active connections.

- **Profiles**

  Create VPN profiles, import or export profile settings, establish VPN connections.

- **Settings**

  Configure the system display settings, check the logs.

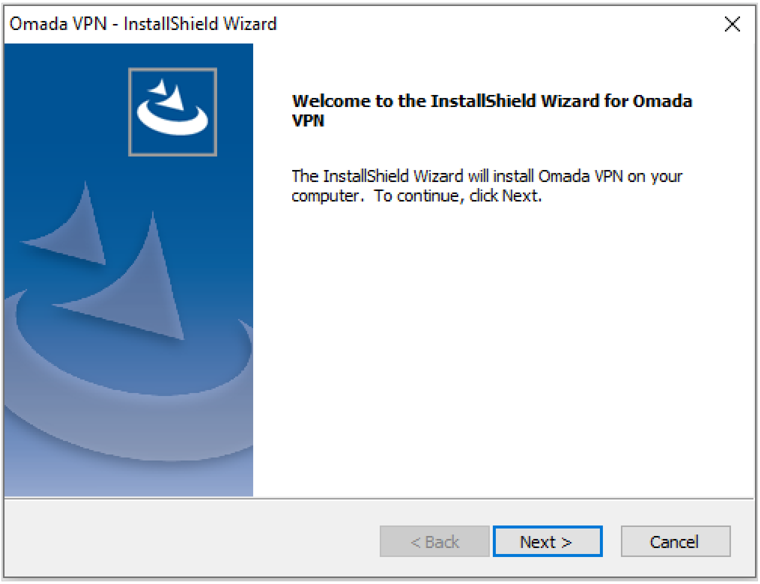
This guide will introduce how to install the Omada VPN Client and how to use the VPN client to connect to the VPN servers.

CONTENTS

Chapter 1 Install Omada VPN Client

Omada VPN client is provided only for Windows 10 and above. Make sure your PC's system meet the system requirements, then properly install the Omada VPN Client.

1. Download the installation file of Omada VPN Client from the website.
2. Follow the InstallShield Wizard to install the Omada VPN Client.

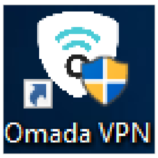


Omada VPN - InstallShield Wizard

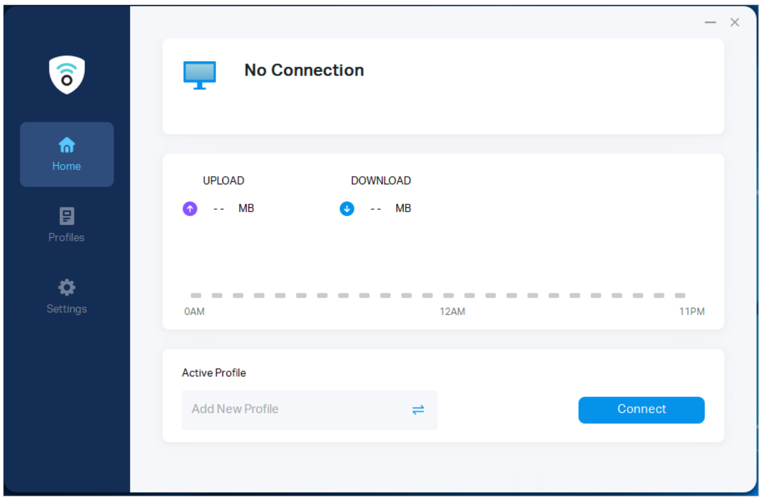
Welcome to the InstallShield Wizard for Omada VPN

The InstallShield Wizard will install Omada VPN on your computer. To continue, click Next.

3. After a successful installation, a shortcut icon of the Omada VPN Client will be created on your desktop.



4. Double-click the shortcut icon to launch Omada VPN Client to start configuring the connection to VPN servers.



Chapter 2 Set Up VPN Connections

This chapter introduces how to set up the router as a VPN server, set up VPN Client in different VPN mode, and how to start the VPN connection. IPsec VPN, SSL VPN, OpenVPN, and WireGuard VPN are supported.

2. 1 Set Up IPsec VPN Connection

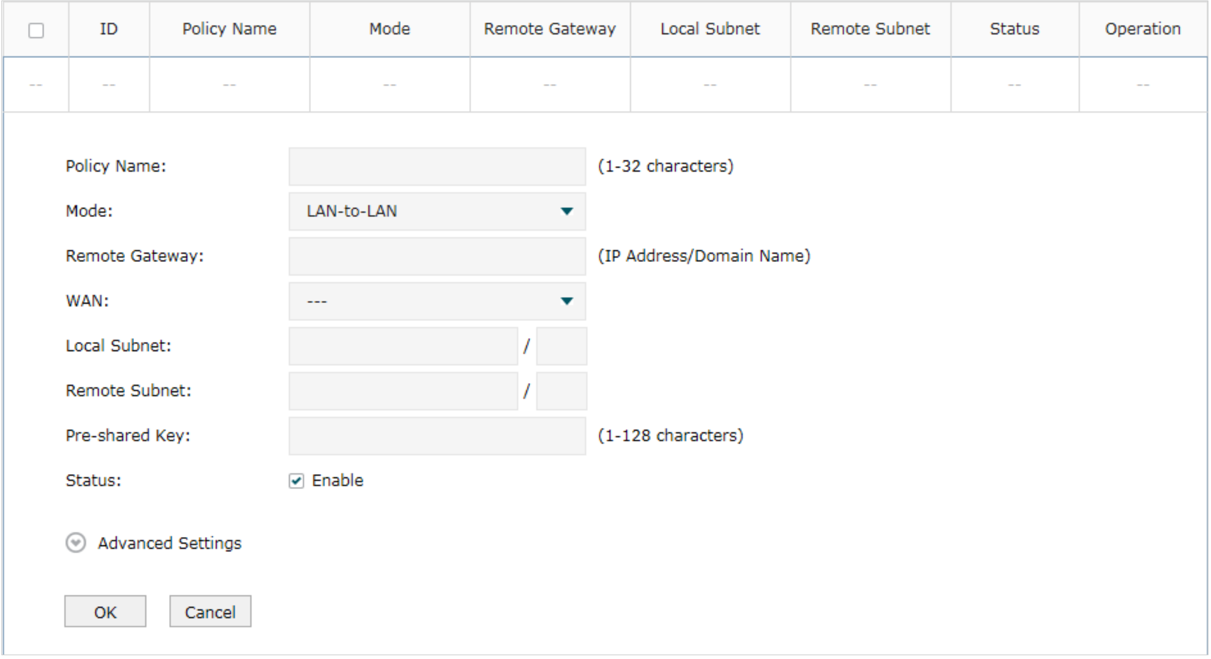
2.1.1 Set up the Omada router as an IPsec VPN server.

- **For Standalone Mode**

  - For both ends of the VPN tunnel, the Pre-shared key, Proposal, Exchange Mode, and Encapsulation Mode should be identical.
  - For both ends of the VPN tunnel, the Remote Gateway, Local/Remote Subnet, Local/Remote ID Type should be matched.

To complete the IPSec VPN configuration, follow these steps:

1) Choose the menu VPN > IPSec > IPSec Policy and click Add to load the following page.



□	ID	Policy Name	Mode	Remote Gateway	Local Subnet	Remote Subnet	Status	Operation
--	--	--	--	--	--	--	--	--

Policy Name: (1-32 characters)

Mode: LAN-to-LAN

Remote Gateway: (IP Address/Domain Name)

WAN: ---

Local Subnet: /

Remote Subnet: /

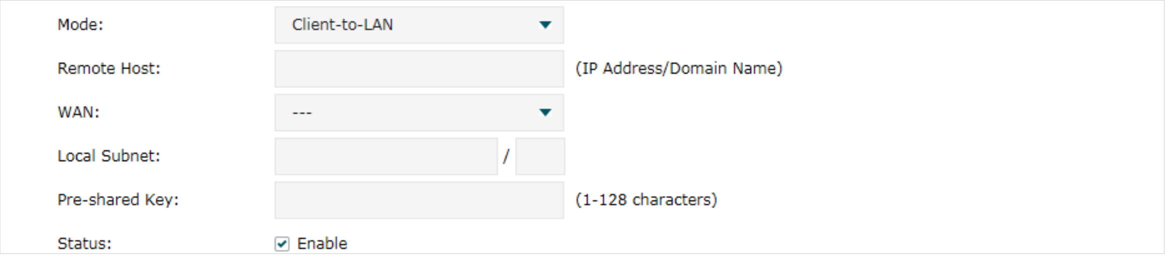
Pre-shared Key: (1-128 characters)

Status: ☑ Enable

Follow these steps to configure the basic parameters:

a. Specify the name of the IPSec Policy.

b. Configure the Network Mode. Select Client-to-LAN when a host is connected to the network.



Mode: Client-to-LAN

Remote Host: (IP Address/Domain Name)

WAN: ---

Local Subnet: /

Pre-shared Key: (1-128 characters)

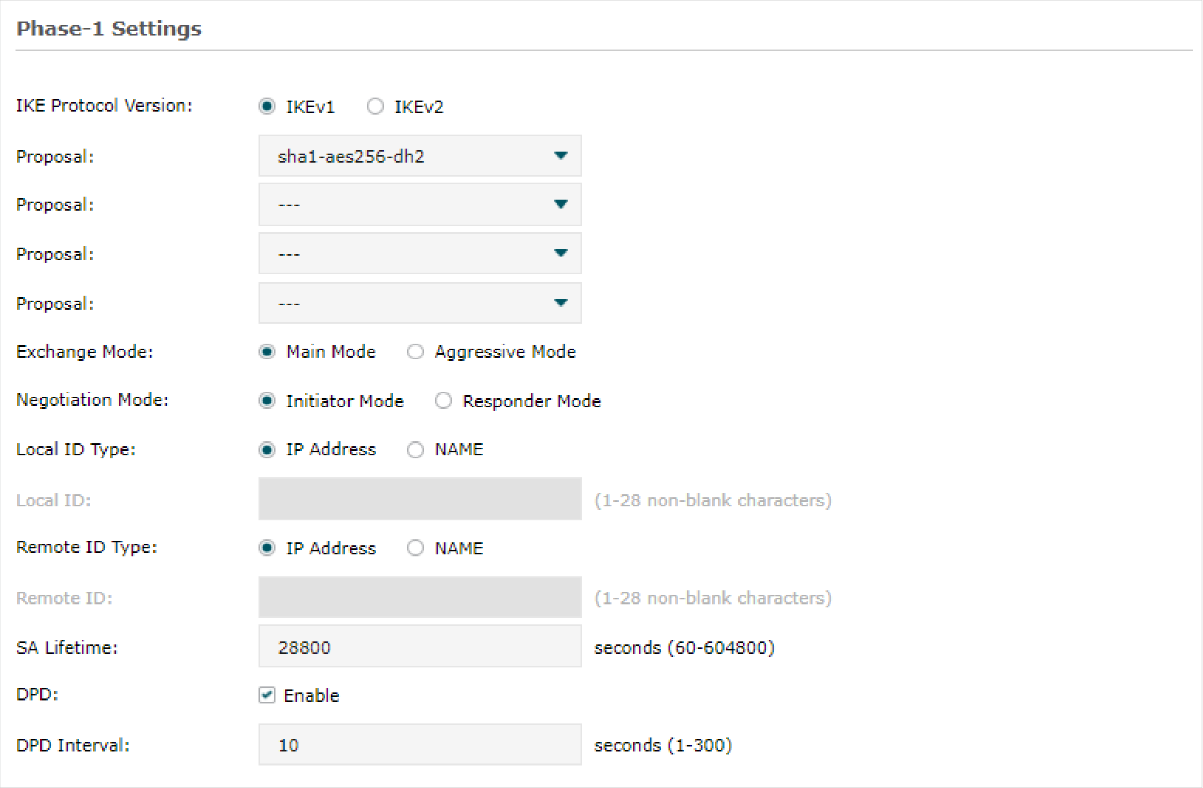
Status: ☑ Enable

Remote Host	Enter the IP address of the remote host. 0.0.0.0 represents any IP address.
WAN	Specify the WAN port on which the IPSec tunnel is established.
Local Subnet	Specify the local network. (This is the IP address range of the LAN on the local side of the VPN tunnel.) It's formed from the IP address and subnet mask.
Pre-shared Key	Specify the unique pre-shared key for both peers' authentication.
Status	Choose to enable the IPSec policy.

c. Click OK.

2) Configuring the Advanced Parameters

a. Choose the menu VPN > IPSec > IPSec Policy and click Advanced Settings to load the following page.



Phase-1 Settings

IKE Protocol Version: ● IKEv1 ○ IKEv2

Proposal: sha1-aes256-dh2

Proposal: ---

Proposal: ---

Proposal: ---

Exchange Mode: ● Main Mode ○ Aggressive Mode

Negotiation Mode: ● Initiator Mode ○ Responder Mode

Local ID Type: ● IP Address ○ NAME

Local ID: (1-28 non-blank characters)

Remote ID Type: ● IP Address ○ NAME

Remote ID: (1-28 non-blank characters)

SA Lifetime: 28800 seconds (60-604800)

DPD: ☑ Enable

DPD Interval: 10 seconds (1-300)

b. In the Phase-1 Settings section, configure the IKE phase-1 parameters and click OK.

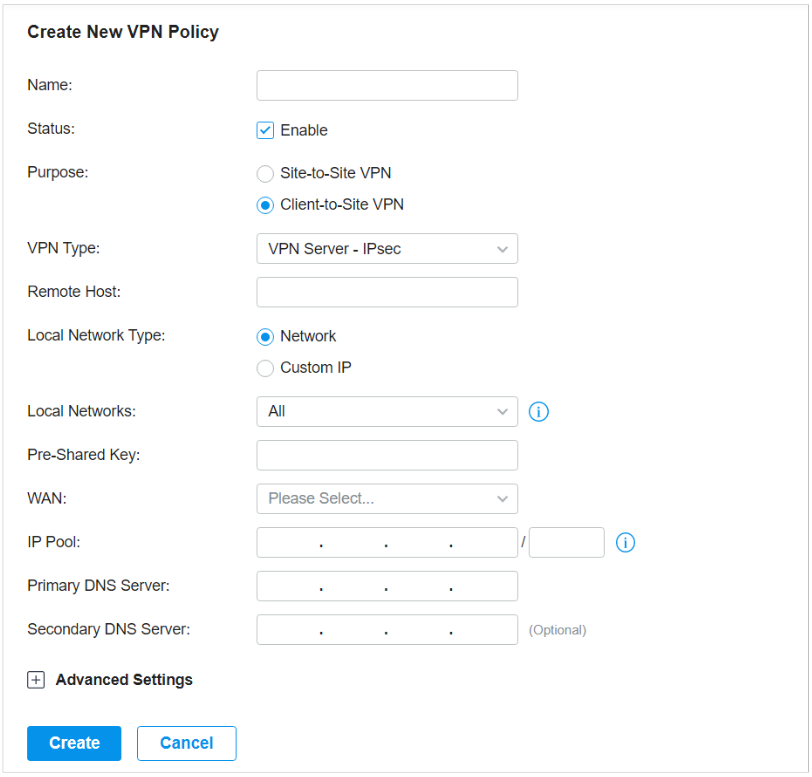
Proposal	Select the proposal for IKE negotiation phase 1 to specify the encryption algorithm, authentication algorithm and DH group. Up to four proposals can be selected.

Exchange Mode	Specify the IKE Exchange Mode as Main Mode or Aggressive Mode. By default, it is Main Mode. Main Mode: Main mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.
Local ID Type	Specify the local ID type for IKE negotiation. IP Address: Use an IP address as the ID in IKE negotiation. It is the default type. NAME: Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).
Local ID	When the Local ID Type is configured as NAME, enter a name for the local device as the ID in IKE negotiation.
Remote ID Type	Specify the remote ID type for IKE negotiation. IP Address: Use an IP address as the ID in IKE negotiation. It is the default type. NAME: Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).
Remote ID	When the Remote ID Type is configured as NAME, enter a name of the remote peer as the ID in IKE negotiation .
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable or disable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.

DPD Interval	If DPD is triggered, specify the interval between sending DPD requests. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

■ For Controller Mode

a. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:	
Status:	☑ Enable
Purpose:	○ Site-to-Site VPN ● Client-to-Site VPN
VPN Type:	VPN Server - IPsec
Remote Host:	
Local Network Type:	● Network ○ Custom IP
Local Networks:	All
Pre-Shared Key:	
WAN:	Please Select...
IP Pool:	. . . /
Primary DNS Server:	. . .
Secondary DNS Server:	. . . (Optional)

⊞ Advanced Settings

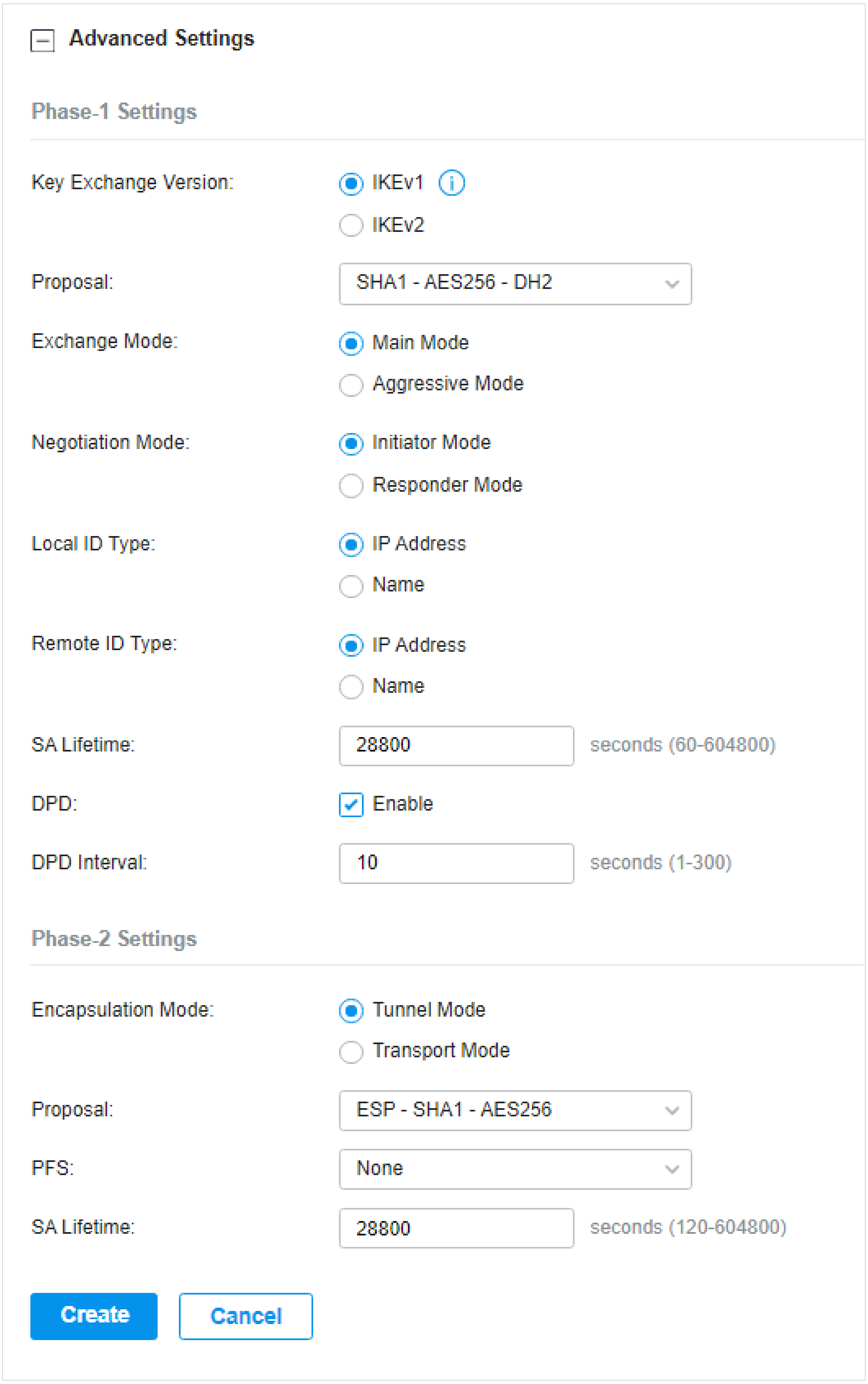
Create Cancel

b. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the basic parameters and click Create.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - IPsec.
Remote Host	Enter an IP address or a domain name of the host on the remote peer of the VPN tunnel. 0.0.0.0 represents any IP address.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.

Pre-Shared Key	Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both VPN peers create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.
WAN	Select the WAN port on which the IPsec VPN tunnel is established.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

c. Click Advanced Settings to load the following page.



⊟ **Advanced Settings**

Phase-1 Settings

Key Exchange Version: ● IKEv1 ⓘ ○ IKEv2

Proposal: SHA1 - AES256 - DH2

Exchange Mode: ● Main Mode ○ Aggressive Mode

Negotiation Mode: ● Initiator Mode ○ Responder Mode

Local ID Type: ● IP Address ○ Name

Remote ID Type: ● IP Address ○ Name

SA Lifetime: 28800 seconds (60-604800)

DPD: ☑ Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

Encapsulation Mode: ● Tunnel Mode ○ Transport Mode

Proposal: ESP - SHA1 - AES256

PFS: None

SA Lifetime: 28800 seconds (120-604800)

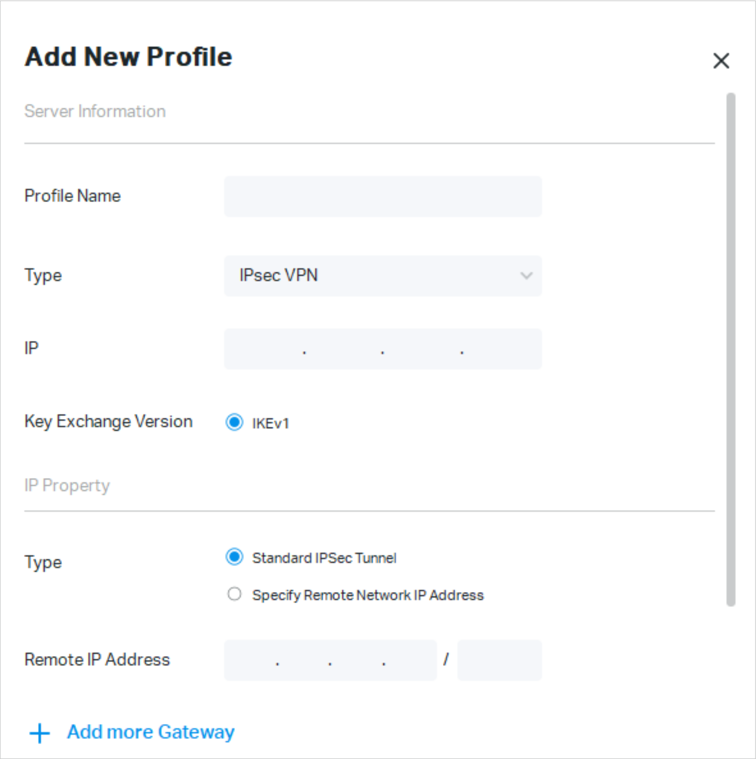
Refer to the following table to complete the Phase-1 settings according to your actual needs and click Create.

Phase-1 Settings	The IKE version you select determines the available Phase-1 settings and defines the negotiation process . Both VPN gateways must be configured to use the same IKE version and Phase-1 settings.
Internet Key Exchange Version	Select the version of Internet Key Exchange (IKE) protocol which is used to set up security associations for IPsec. Both IKEv1 and IKEv2 are supported with gateways, but IKEv1 is available only when the VPN policy is applied to a single Remote Subnet and a single Local Network. Note that both VPN peers must be configured to use the same IKE version.
Proposal	Specify the proposal for IKE negotiation phase-1. An IKE proposal lists the encryption algorithm, authentication algorithm and Diffie-Hellman (DH) groups to be negotiated with the remote IPsec peer. Authentication algorithms verify the data integrity and authenticity of a message. Encryption algorithms protect the data from being read by a third-party. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Note that both VPN peers must be configured to use the same Proposal.
Exchange Mode	Specify the IKE Exchange Mode when IKEv1 is selected. Main Mode: This mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: This mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.
Local ID Type	Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.
Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).

Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.
DPD Interval	Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

2.1.2 Set up IPsec VPN client.

1. Double-click the shortcut icon to launch Omada VPN Client. Go to Profiles, click Add, and select IPsec VPN type.



Add New Profile ×

Server Information

Profile Name

Type: IPsec VPN

IP: . . .

Key Exchange Version: ● IKEv1

IP Property

Type: ● Standard IPSec Tunnel ○ Specify Remote Network IP Address

Remote IP Address: . . . /

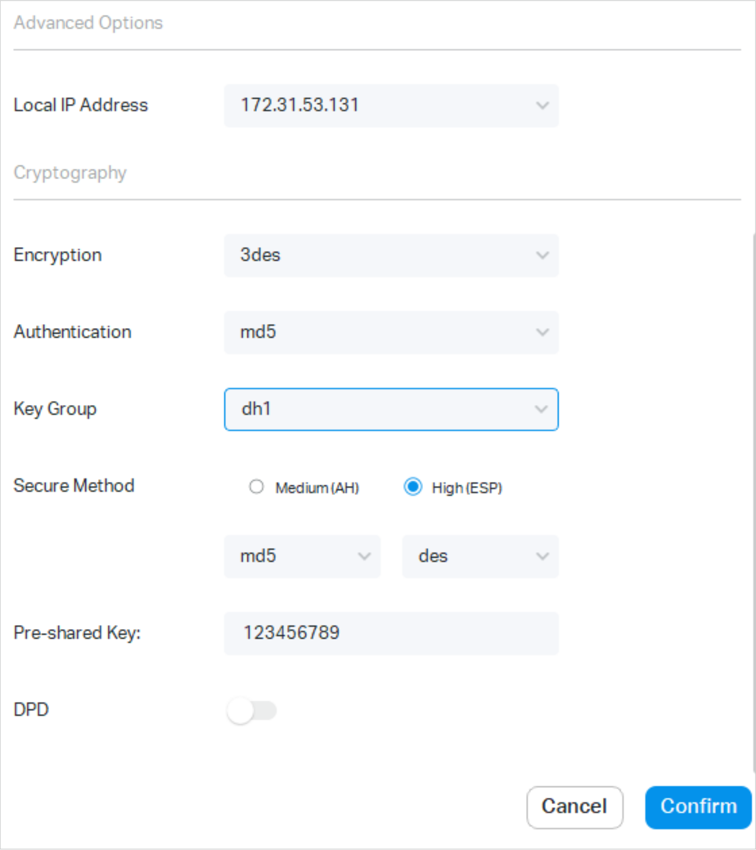
+ Add more Gateway

2. Specify the name of the profile.

3. Enter the WAN IP address of the IPsec VPN server.

4. Enter the LAN IP address of the IPsec VPN server.

5. In the Advanced Options section, enter the parameters specified in the IPsec VPN server.



Advanced Options

Local IP Address: 172.31.53.131

Cryptography

Encryption: 3des

Authentication: md5

Key Group: dh1

Secure Method: ○ Medium (AH) ● High (ESP)

md5 des

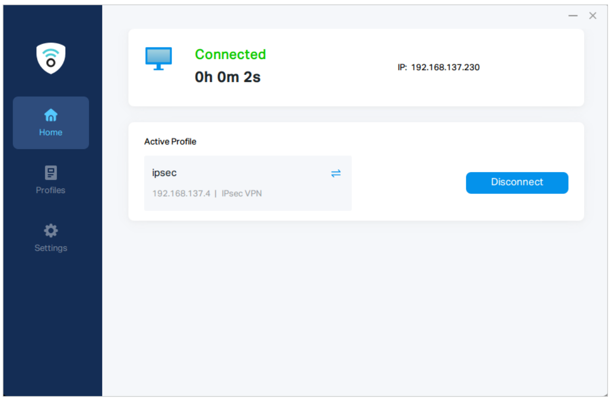
Pre-shared Key: 123456789

DPD

6. Click Confirm.

2.1.3 Active the IPsec VPN connection.

1. Select the profile we created on the Home or Profiles page. Click Connect to active the connection.



Connected

0h 0m 2s

IP: 192.168.137.230

Active Profile

ipsec

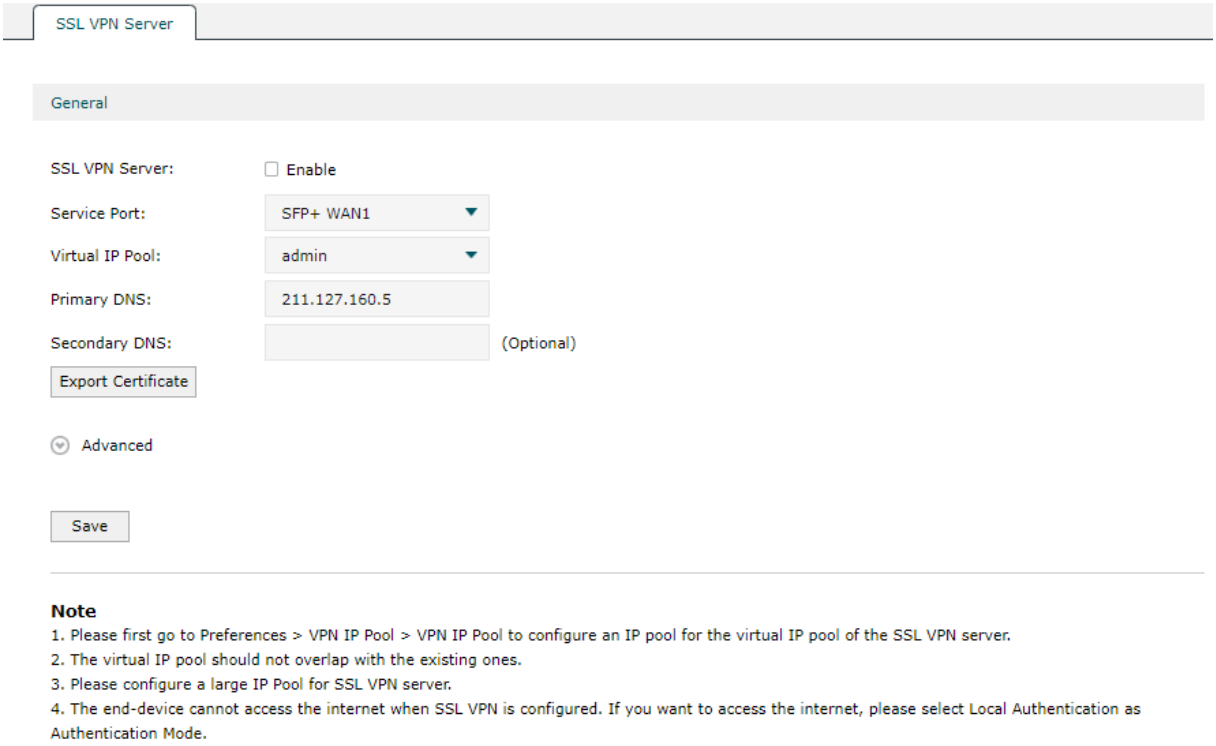
192.168.137.4 | IPsec VPN

2. 2 Set Up SSL VPN Connection

2.2.1 Set up the Omada router as an SSL VPN server.

- **For Standalone Mode**

1. Choose the menu SSL VPN > SSL VPN Server > SSL VPN Server to load the following page.



SSL VPN Server

General

SSL VPN Server: □ Enable

Service Port: SFP+ WAN1

Virtual IP Pool: admin

Primary DNS: 211.127.160.5

Secondary DNS: (Optional)

Note

1. Please first go to Preferences > VPN IP Pool > VPN IP Pool to configure an IP pool for the virtual IP pool of the SSL VPN server.
2. The virtual IP pool should not overlap with the existing ones.
3. Please configure a large IP Pool for SSL VPN server.
4. The end-device cannot access the internet when SSL VPN is configured. If you want to access the internet, please select Local Authentication as Authentication Mode.

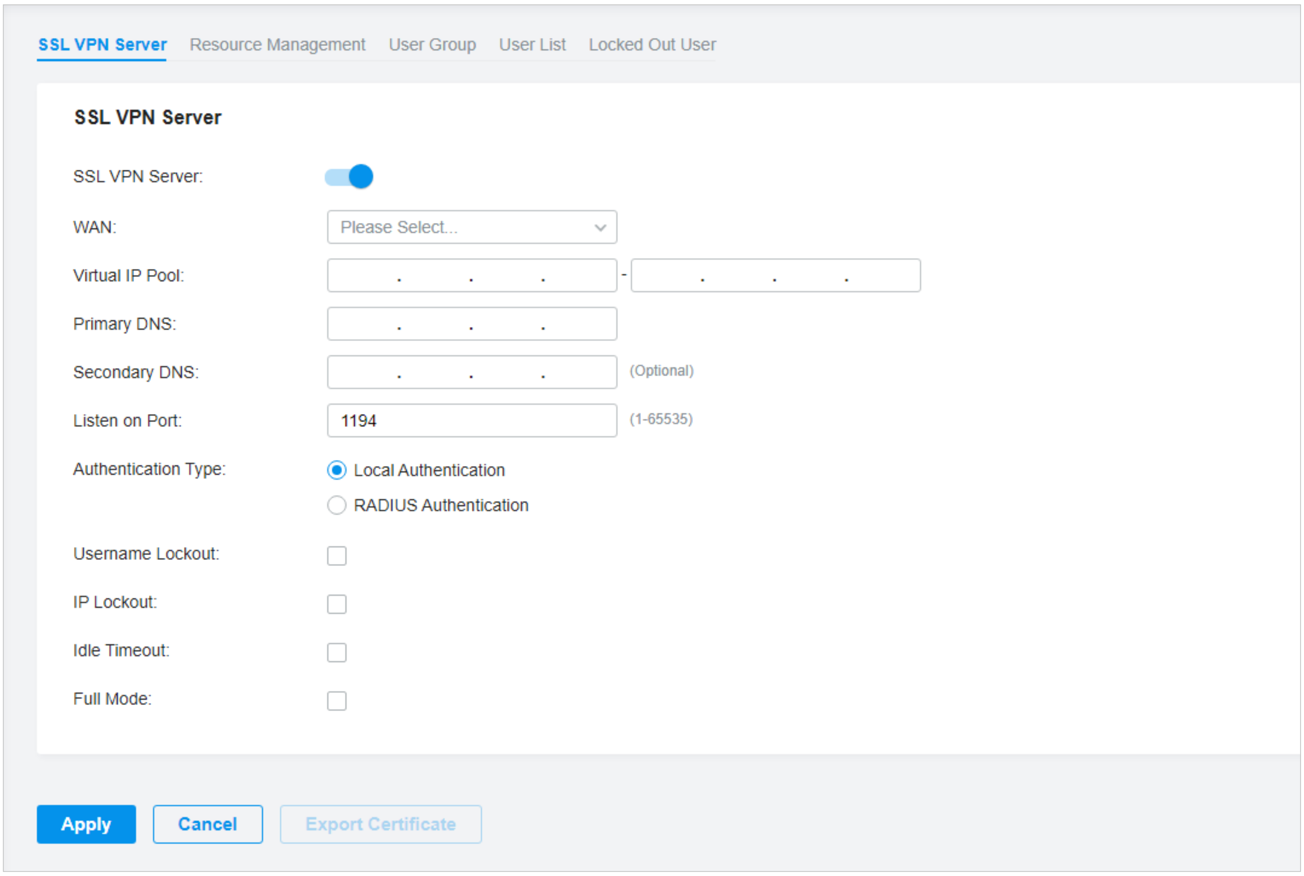
Check the box to enable the feature, then configure the corrresponding parameters

Service Port	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Virtual IP Pool	Select a virtual IP Pool, and the SSL VPN server will assign an IP address to a connected client within the pool. To create an IP Pool, go to Preferences > VPN IP Pool > VPN IP Pool. The number of IP addresses in the IP pool should not be less than 4.
Primary DNS	Specify the IP address of the DNS server. Please assign the LAN IP to the SSLVPN DNS server.
Secondary DNS	Specify the IP address of the DNS server. Please assign the LAN IP to the SSLVPN DNS server.
Listen on Port	Specify the port for the SSL VPN server to listen on. By default, it is 1194.
Authentication Type	Select the authentication for the clients. For RADIUS Authentication, go to SSL VPN > Authentication to configure.

Username Lockout	Block a client with the specific login username. Max. Login Attempts: Specify the maximum failed login attempts for a username. After the maximum attempt is reached, the username will be locked out. Lock Duration: Specify how long the username will be locked out.
IP Lockout	Block a client of the specific login IP. Max. Login Attempts: Specify the maximum failed login attempts for a username. After the maximum attempt is reached, the username will be locked out. Lock Duration: Specify how long the username will be locked out.
Idle Timeout	Enable the feature and the VPN tunnel will close automatically if there is no traffic for the specified amount of time.
Full Mode	Enable the feature and all traffic will go through the SSL VPN tunnel. When the feature is disabled, only the resource-related traffic will go through the tunnel.

- **For Controller Mode**

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > SSL VPN Server. Enable SSL VPN Server.



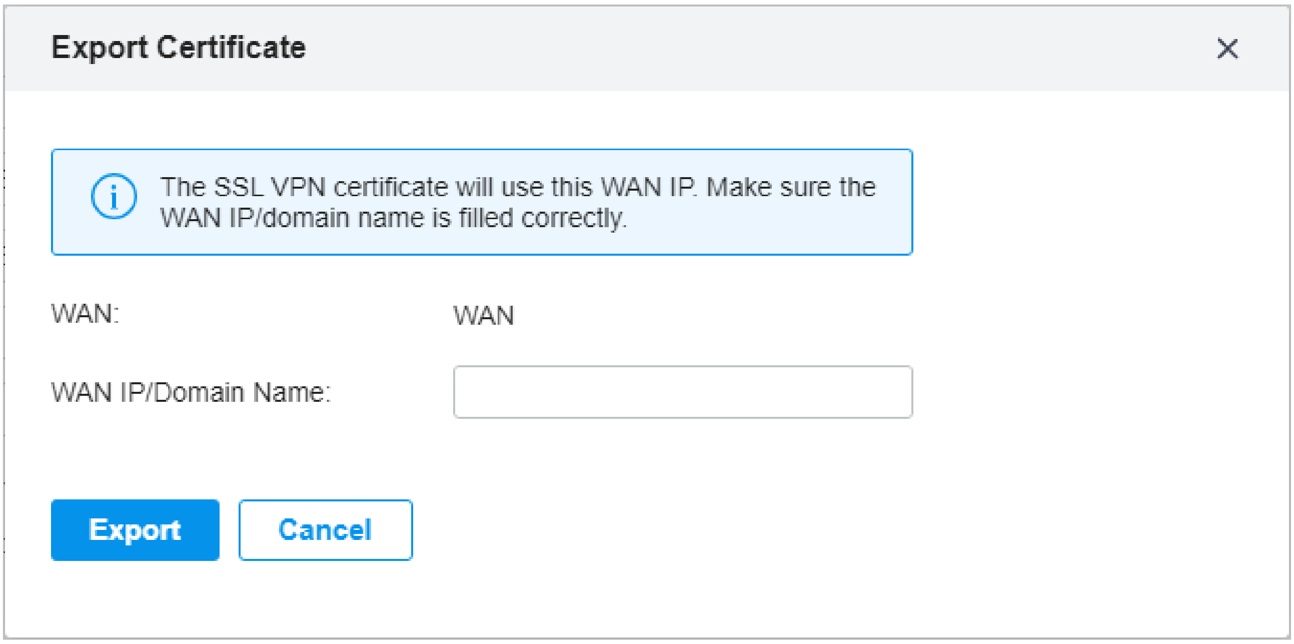
SSL VPN Server

SSL VPN Server:	● (on)
WAN:	Please Select...
Virtual IP Pool:	. . . - . . .
Primary DNS:	. . .
Secondary DNS:	. . . (Optional)
Listen on Port:	1194 (1-65535)
Authentication Type:	● Local Authentication ○ RADIUS Authentication
Username Lockout:	□
IP Lockout:	□
Idle Timeout:	□
Full Mode:	□

2. Configure the parameters according to your needs. Click Apply.

WAN	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Virtual IP Pool	Set a virtual IP Pool, and the SSL VPN server will assign an IP address to a connected client within the pool.
Primary/Secondary DNS	Specify the IP address of the DNS server. The clients will be informed of the DNS server, and it can help the clients resolve the domain name.
Listen on Port	Specify the port for the SSL VPN server to listen on. By default, it is 1194.
Authentication Type	Select the authentication for the clients: Local Authentication or RADIUS Authentication. If you selected RADIUS Authentication, configure the following parameters: RADIUS Server: Select a RADIUS server profile. Authentication Type: Select the authentication protocol for the RADIUS server. Max Requests: Specify the maximum number of requests sent when no response is received. Request Timeout: Specify the maximum interval for request timeout. After timeout, the request will be sent again. NAS IP: Specify the IP address for the router to communicate with the RADIUS server.
Username Lockout	When enabled, you can lock out a username in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a username. If the number of attempts reaches this amount, the username will be locked out. Lockout Duration: Specify how long the username will be locked out.
IP Lockout	When enabled, you can lock out an IP address in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a login IP. If the number of attempts reaches this amount, the login IP will be locked out. Lockout Duration: Specify how long the login IP will be locked out.
Idle Timeout	When enabled, the VPN tunnel will close automatically if there is no traffic for the specified amount of time.
Full Mode	When enable, all traffic will go through the SSL VPN tunnel. When disabled, only the resource-related traffic will go through the tunnel.

3. Click Export Certificate, enter the WAN IP/Domain Name to access the VPN, then click Export. The VPN configuration file will be exported for clients to access the VPN.



Export Certificate

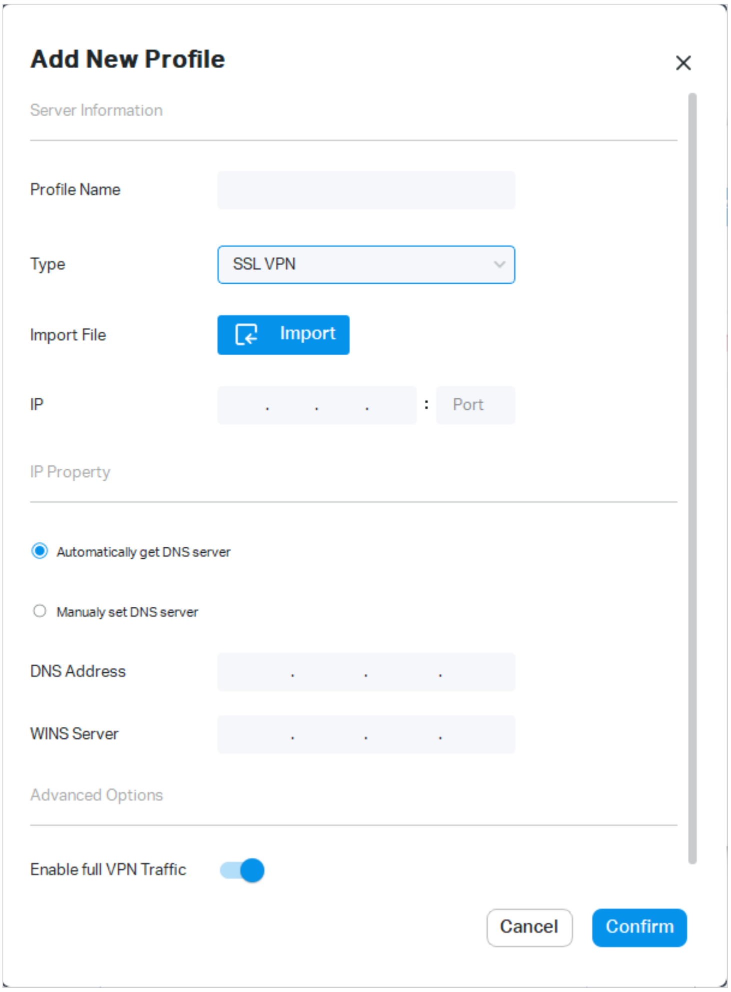
The SSL VPN certificate will use this WAN IP. Make sure the WAN IP/domain name is filled correctly.

WAN: WAN

WAN IP/Domain Name:

2.2.2 Set up SSL VPN client.

1. Double-click the shortcut icon to launch Omada VPN Client. Go to Profiles, click Add, and select SSL VPN type.



Add New Profile

Server Information

Profile Name

Type: SSL VPN

Import File: Import

IP . . . : Port

IP Property

● Automatically get DNS server

○ Manualy set DNS server

DNS Address . . .

WINS Server . . .

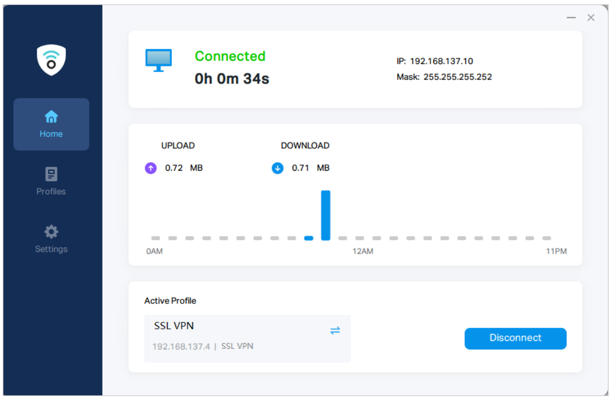
Advanced Options

Enable full VPN Traffic: On

2. Specify the name of the profile.
3. Enter the WAN IP address of the SSL VPN server or click Import to import the configuration file of the SSL VPN server exported when establishing the SSL VPN server.
4. Click Confirm.

2.2.3 Active the SSL VPN connection.

1. Select the profile we created on the Home or Profiles page. Click Connect to active the connection.



Connected

0h 0m 34s

IP: 192.168.137.10

Mask: 255.255.255.252

UPLOAD 0.72 MB

DOWNLOAD 0.71 MB

Active Profile

SSL VPN

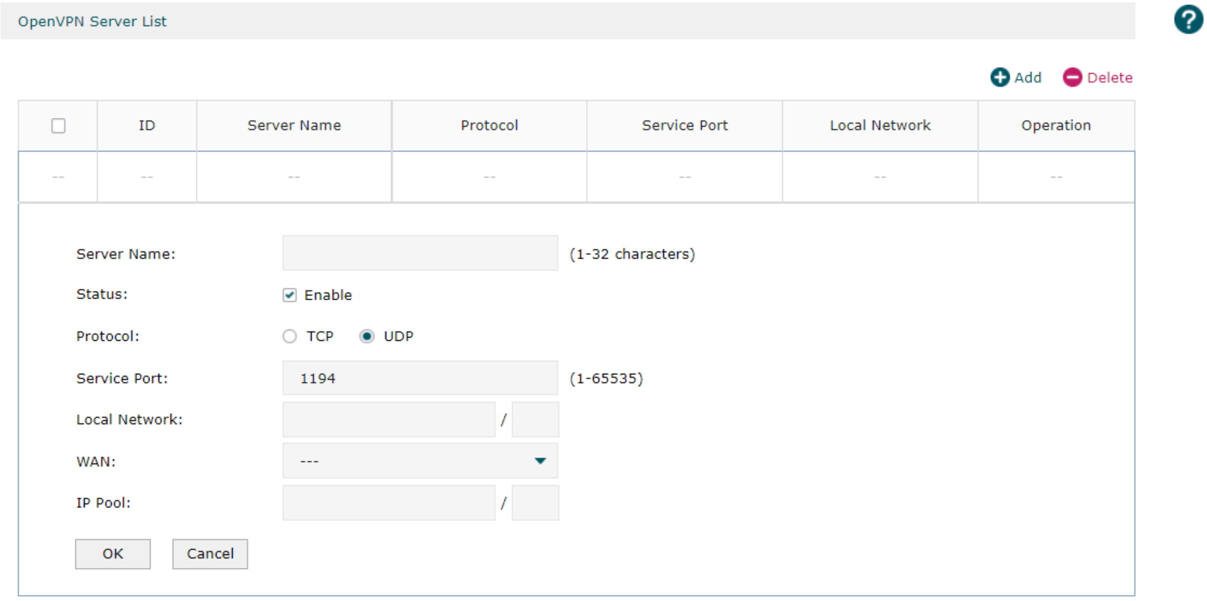
192.168.137.4 | SSL VPN

2. 3 Set Up OpenVPN Connection

2.3.1 Set up the Omada router as an OpenVPN server.

- **For Standalone Mode**

1. Choose the menu VPN > OpenVPN > OpenVPN Server and click Add to load the following page.


OpenVPN Server List

□	ID	Server Name	Protocol	Service Port	Local Network	Operation
--	--	--	--	--	--	--

Server Name: (1-32 characters)

Status: ☑ Enable

Protocol: ○ TCP ● UDP

Service Port: 1194 (1-65535)

Local Network: /

WAN: ---

IP Pool: /

2. Specify the name of the OpenVPN server, configure other relevant parameters according to your actual network environment, and click OK.

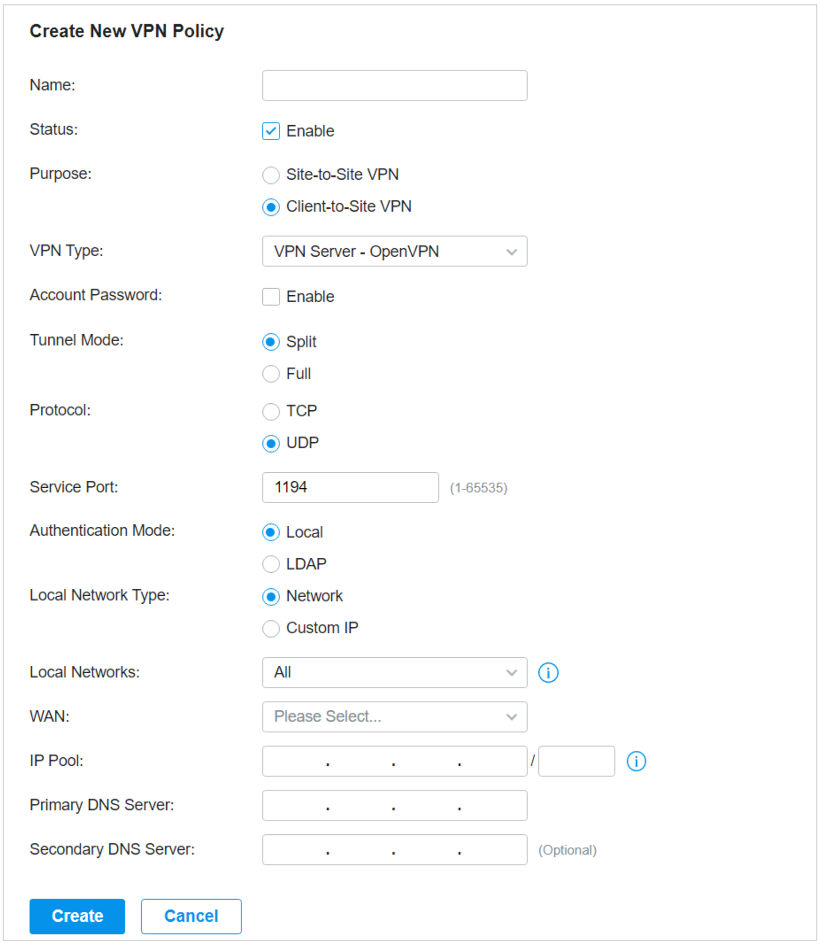
Server Name	Enter a name to identify the VPN server.
Status	Check the box to enable the OpenVPN server.

Protocol	Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP.
Service Port	Enter a VPN service port to which a VPN device connects. The default port is 1194.
Local Network	Select the network on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local network.
WAN	Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.

Note: After saving the settings, export the OpenVPN file that ends in .ovpn which is to be used by the remote client. The exported OpenVPN file contains the certificate and configuration information. It may take about 2 minutes to export the certificate.

- **For Controller Mode**

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



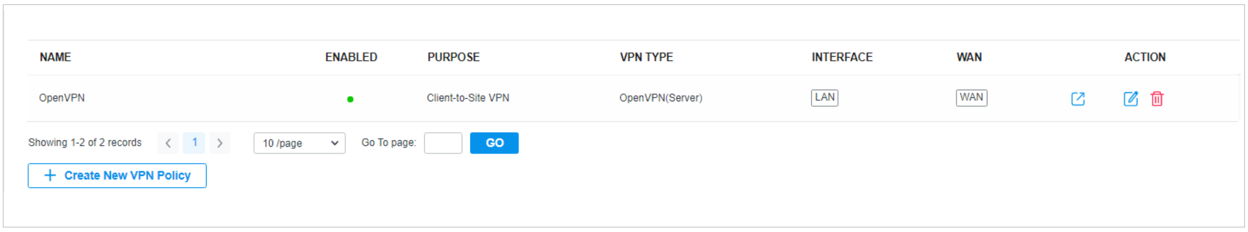
Create New VPN Policy

Name:	
Status:	☑ Enable
Purpose:	○ Site-to-Site VPN ● Client-to-Site VPN
VPN Type:	VPN Server - OpenVPN
Account Password:	□ Enable
Tunnel Mode:	● Split ○ Full
Protocol:	○ TCP ● UDP
Service Port:	1194 (1-65535)
Authentication Mode:	● Local ○ LDAP
Local Network Type:	● Network ○ Custom IP
Local Networks:	All
WAN:	Please Select...
IP Pool:	. . . /
Primary DNS Server:	. . .
Secondary DNS Server:	. . . (Optional)

2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - OpenVPN.
Account Password	Specify whether VPN clients need to enter a user account to access the VPN tunnel. When enabled, you need to create accounts on the VPN User page.
Tunnel Mode	Select the tunnel mode: Split or Full. Full tunneling uses the VPN for all your traffic, whereas split tunneling sends part of your traffic through a VPN and part of it through the open network. Full tunneling is more secure than split tunneling.
Protocol	Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP.
Service Port	Enter a VPN service port to which a VPN device connects.
Authentication Mode	Select the authentication mode: Local or LDAP. LDAP is used for SSO (single sign-on), which enables users to use the same password in multiple services.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. After clicking Create to save the VPN policy, go to VPN Policy List and click ↗ in the Action column to export the OpenVPN file that ends in .ovpn which is to be used by the remote client. The exported OpenVPN file contains the certificate and configuration information.



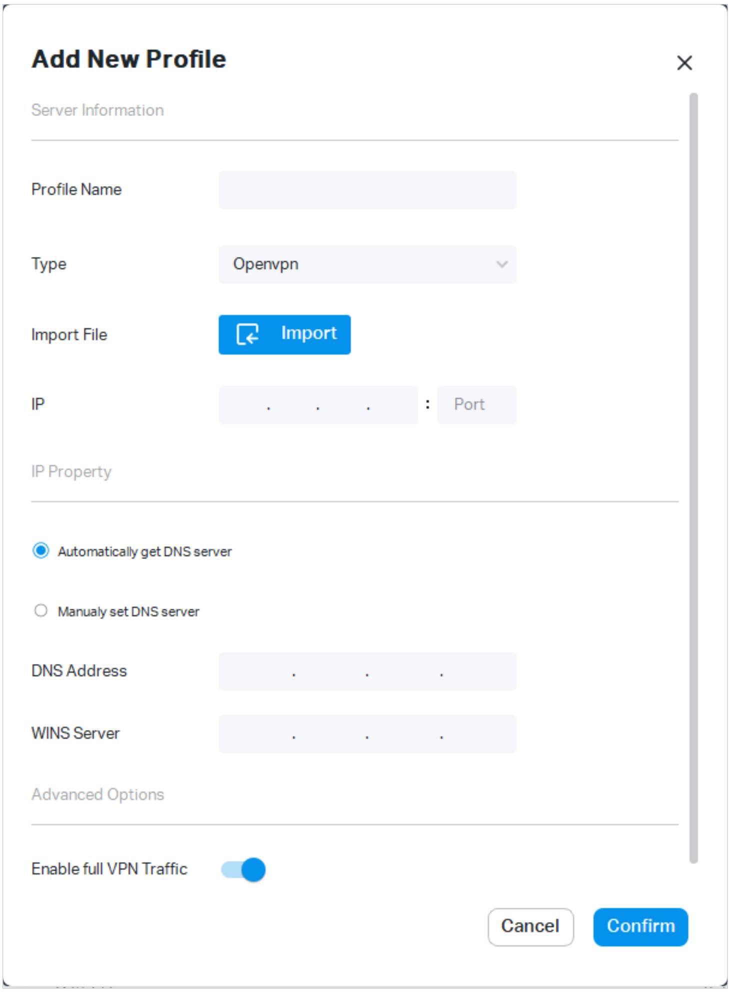
NAME	ENABLED	PURPOSE	VPN TYPE	INTERFACE	WAN	ACTION
OpenVPN	●	Client-to-Site VPN	OpenVPN(Server)	LAN	WAN	↗ ✎ 🗑

Showing 1-2 of 2 records < 1 > 10 /page Go To page: GO

+ Create New VPN Policy

2.3.2 Set up OpenVPN client.

1. Double-click the shortcut icon to launch Omada VPN Client. Go to Profiles, click Add, and select OpenVPN type.



Add New Profile ×

Server Information

Profile Name

Type: Openvpn

Import File: Import

IP: . . . : Port

IP Property

● Automatically get DNS server

○ Manualy set DNS server

DNS Address: . . .

WINS Server: . . .

Advanced Options

Enable full VPN Traffic: On

Cancel Confirm

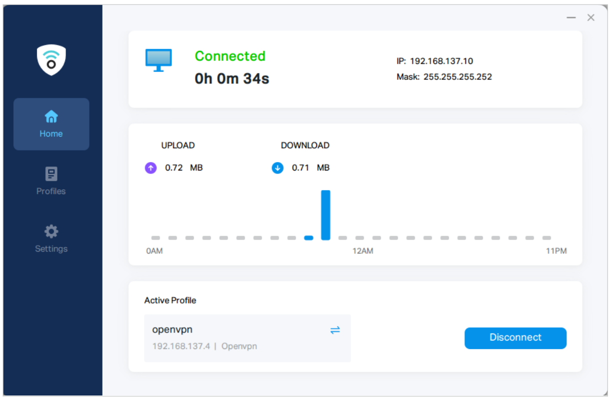
2. Specify the name of the profile.

3. Enter the WAN IP address of the OpenVPN server or click Import to import the configuration file of the OpenVPN server exported when establishing the OpenVPN server.

4. Click Confirm.

2.3.3 Active the OpenVPN connection.

1. Select the profile we created on the Home or Profiles page. Click Connect to active the connection.

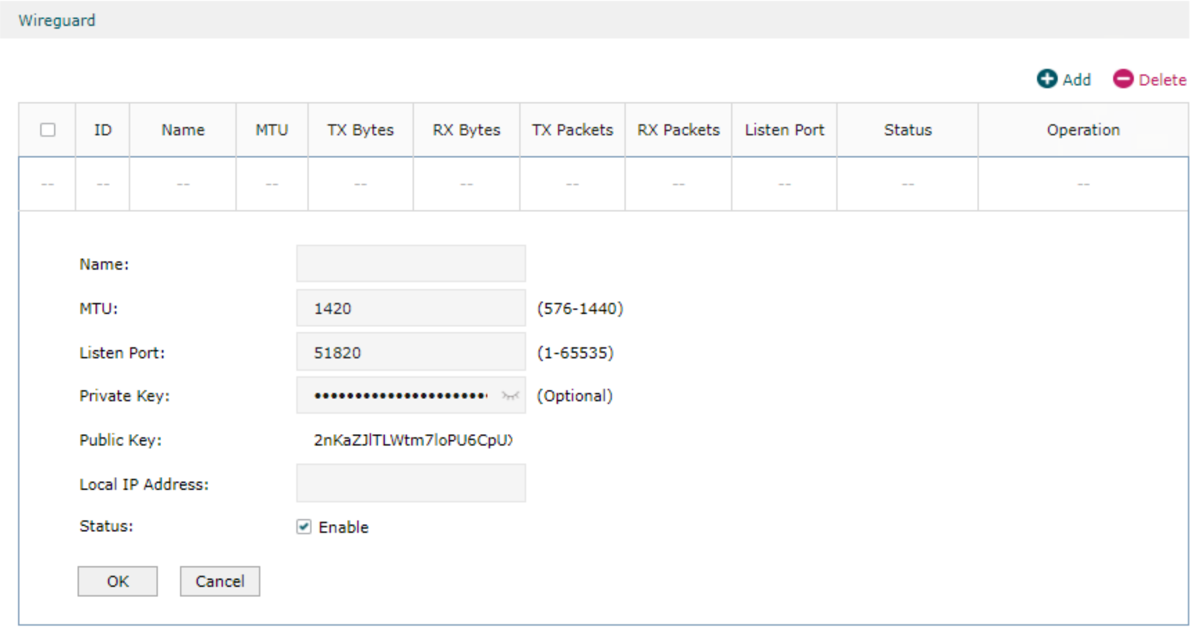


2. 4 Set Up WireGard VPN Connection

2.4.1 Set up the Omada router as a WireGuard VPN server.

■ **For Standalone Mode**

1. Choose the menu VPN > WireGuard > WireGuard and click Add to load the following page.



□	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Name:

MTU: 1420 (576-1440)

Listen Port: 51820 (1-65535)

Private Key: •••••••••••••••••••••• (Optional)

Public Key: 2nKaZJlTLWtm7loPU6CpU)

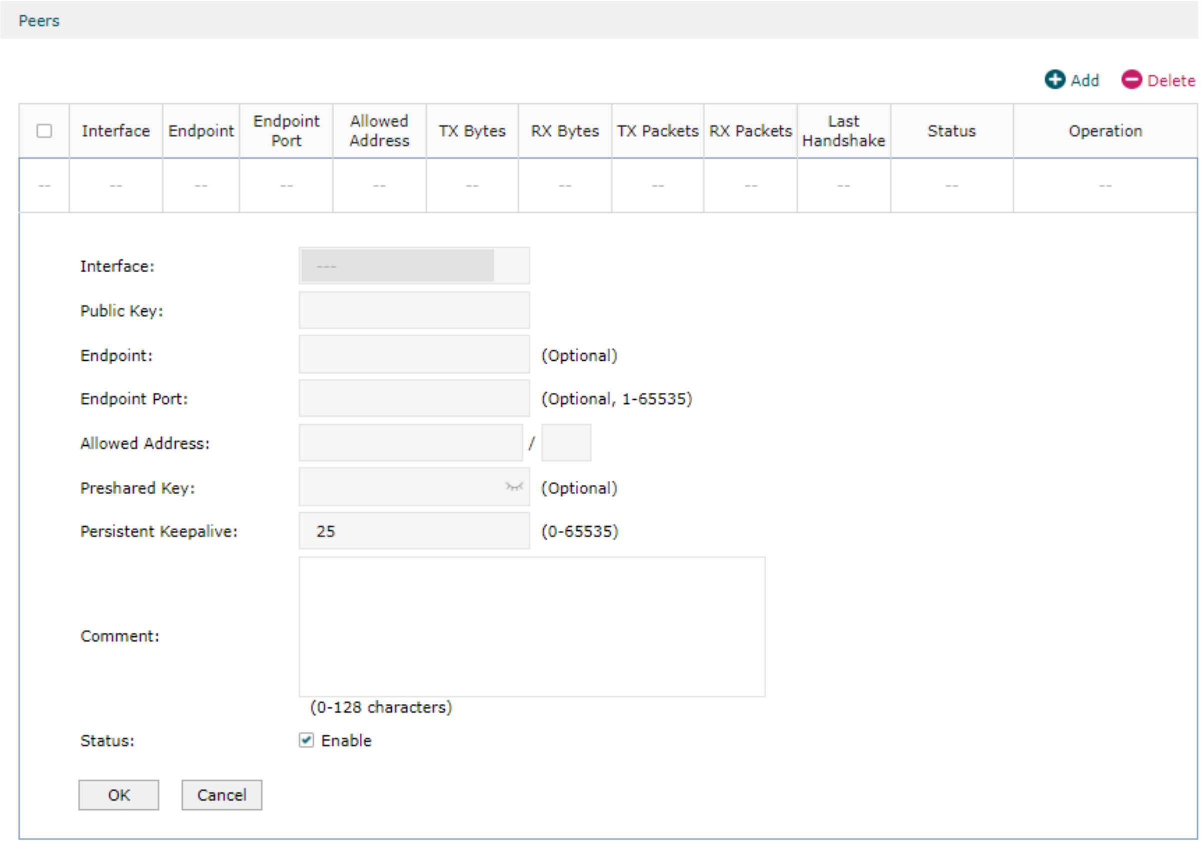
Local IP Address:

Status: ☑ Enable

Name	Specify the name that identifies the Wireguard interface.
MTU	Specify the MTU value of the Wireguard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the Wireguard interface listens to.

Service Port	Enter a VPN service port to which a VPN device connects. The default port is 1194.
Private Key	Specify the private key of the Wireguard interface. The value will be automatically generated on the device, and you can also modify it manually.
Public Key	Specify the public key of the Wireguard interface. This field will be automatically generated based on the private key.
Local IP Address	Specify the IP address of the WireGuard interface. Please select a reserved address to avoid IP conflicts.
Status	Specify whether to enable the Wireguard interface.

2. Choose the menu VPN > WireGuard > Peers and click Add to load the following page.



Peers

□	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
--	--	--	--	--	--	--	--	--	--	--	--

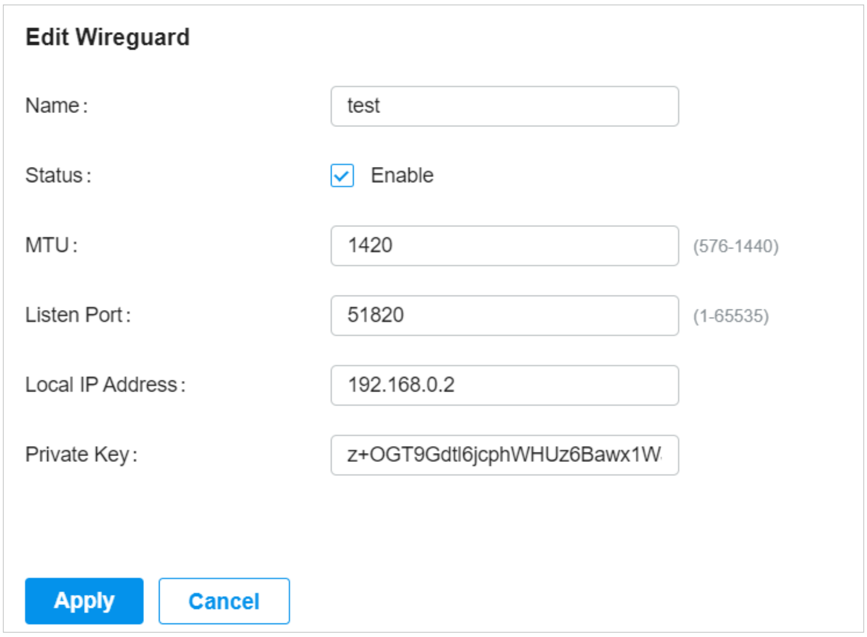
Interface:	---
Public Key:	
Endpoint:	(Optional)
Endpoint Port:	(Optional, 1-65535)
Allowed Address:	/
Preshared Key:	(Optional)
Persistent Keepalive:	25 (0-65535)
Comment:	(0-128 characters)
Status:	☑ Enable

Interface	Specify the Wireguard interface to which the peer belongs.
Public key	Specify the public key of the peer.
Endpoint	Specify the IP address of the peer.
Endpoint Port	Specify the port number of the peer.
Allowed Address	Specify the address segment that allows traffic to pass through. Generally, you can fill in the subnet address of the peer.

Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Status	Specify whether to enable the peer.

For Controller Mode

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > WireGuard.
2. Click Create New WireGuard. Configure the parameters and click Apply.



Edit Wireguard

Name: test

Status: ☑ Enable

MTU: 1420 (576-1440)

Listen Port: 51820 (1-65535)

Local IP Address: 192.168.0.2

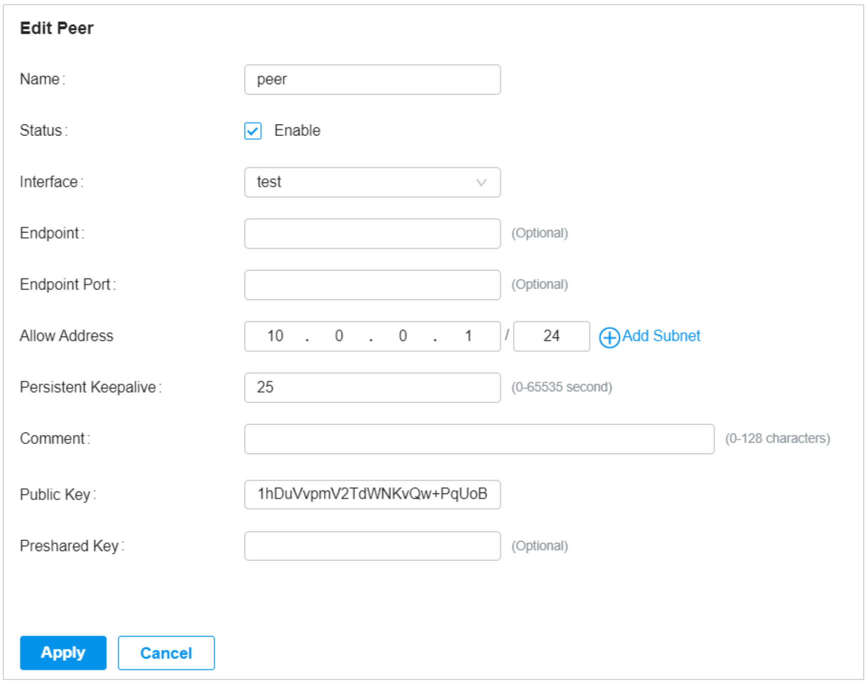
Private Key: z+OGT9Gdtl6jcphWHUz6Bawx1W

Name	Specify the name that identifies the WireGuard interface.
Status	Specify whether to enable the WireGuard interface.
MTU	Specify the MTU value of the WireGuard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the WireGuard interface listens to.
Local IP Address	Specify the IP address of the WireGuard interface.
Private Key	Specify the private key of the WireGuard interface. The value will be automatically generated on the device, and you can also modify it manually.

- **Peers**

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > WireGuard > Peers.

2. Click Create New Peer. Configure the parameters and click Apply.



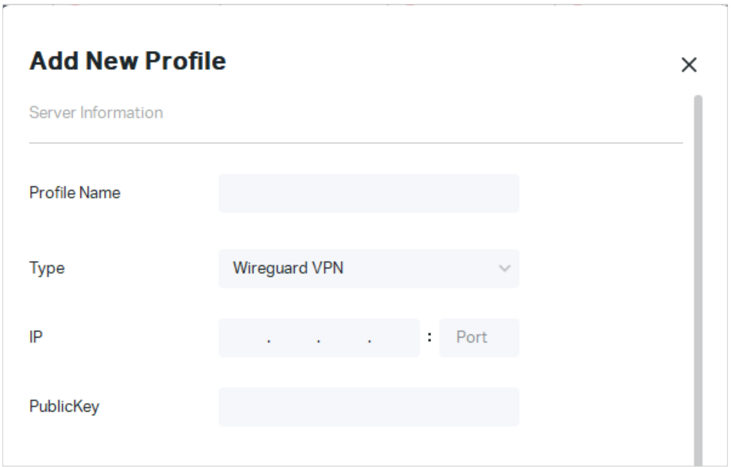
Edit Peer

Name:	peer	
Status:	☑ Enable	
Interface:	test	
Endpoint:		(Optional)
Endpoint Port:		(Optional)
Allow Address	10 . 0 . 0 . 1 / 24	⊕Add Subnet
Persistent Keepalive:	25	(0-65535 second)
Comment:		(0-128 characters)
Public Key:	1hDuVvpmV2TdWNKvQw+PqUoB	
Preshared Key:		(Optional)

Name	Specify the name that identifies the peer.
Status	Specify whether to enable the peer.
Interface	Specify the WireGuard interface to which the peer belongs.
Endpoint	Specify the IP address of the peer. This parameters is required when the Router actively connects to other WireGurad Server.
Endpoint Port	Specify the port number of the peer. This parameters is required when the Router actively connects to other WireGurad Server.
Allowed Address	Specify the address segment that allows traffic to pass through. Generally, it is the same as the WireGuard VPN interface IP configured on the remote device.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Public Key	Fill in the public key information exported from the remote device.
Preshared Key	Specify an optional shared key.

2.4.2 Set up WireGuard VPN client.

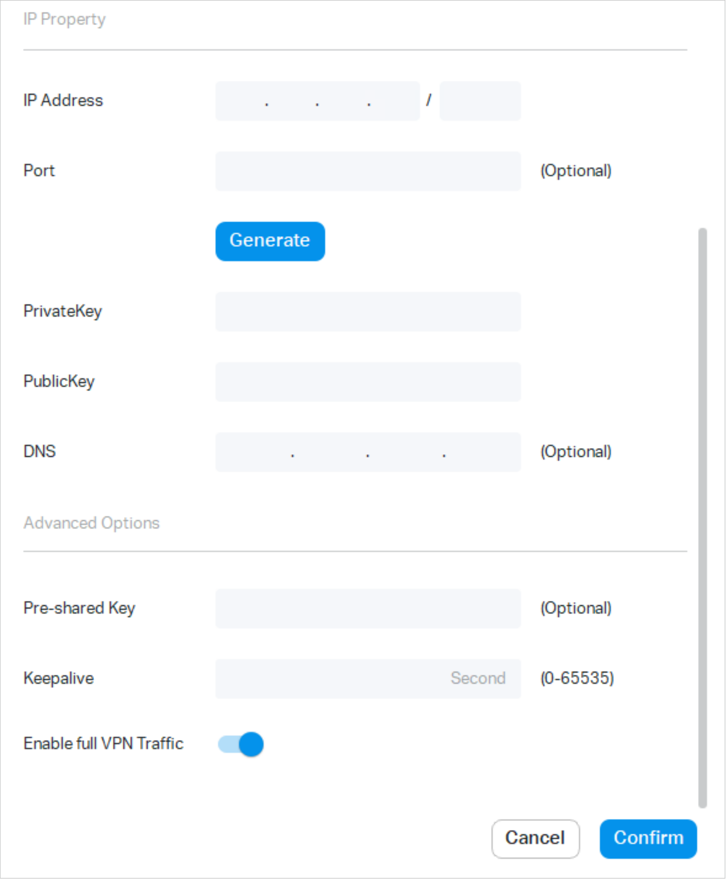
1. Double-click the shortcut icon to launch Omada VPN Client. Go to Profiles, click Add, and select WireGuard VPN type.



Type: Wireguard VPN

2. Specify the name of the profile.

3. Enter the WAN IP address of the WireGuard VPN server and the PublicKey of the WireGuard VPN server.

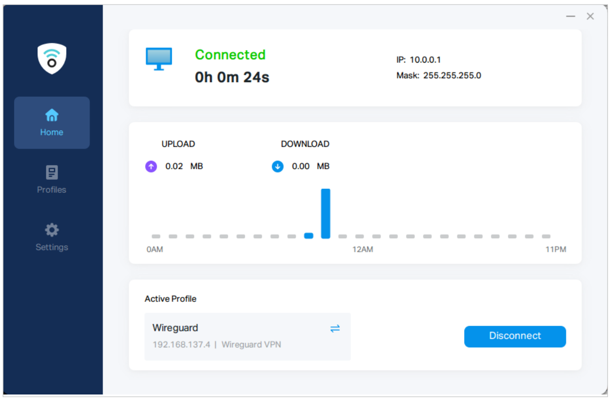


4. Enter the IP address of the clients that are allowed to access the VPN server, then click Generate. A private key and public key will be generated. Fill the key in the Peers settings of the server.

5. Click Confirm.

2.4.3 Active the WireGuard VPN connection.

1. Select the profile we created on the Home or Profiles page. Click Connect to active the connection.



Connected
0h 0m 24s

IP: 10.0.0.1
Mask: 255.255.255.0

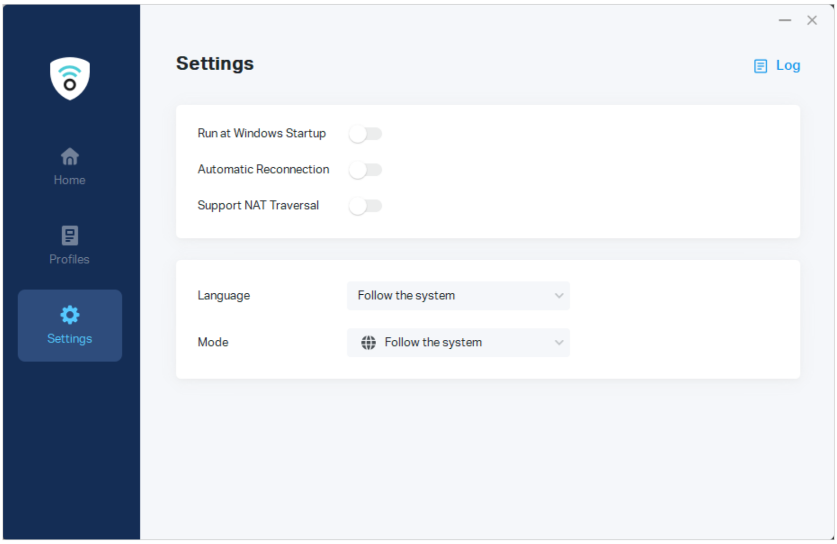
UPLOAD 0.02 MB
DOWNLOAD 0.00 MB

Active Profile
Wireguard
192.168.137.4 | Wireguard VPN

Chapter 3 System Settings

On the Settings page, you can configure when to run the VPN client, display languages and check the logs.

Double-click the shortcut icon to launch Omada VPN Client. Go to Settings.



Settings

Run at Windows Startup
Automatic Reconnection
Support NAT Traversal

Language: Follow the system
Mode: Follow the system

Run at Windows Startup	When enabled, the Omada Client will run when the PC starts up.
Automatic Reconnection	When enabled, the configured VPN connection will be automatically active.
Support NAT Traversal	Whether to enable the NAT traversal feature for VPN connection.
Language	Set the display language. You can choose to follow your system language or choose one specific language.

Mode	Set the display mode. You can choose to follow your system mode, or choose normal mode or dark mode.