



ShareTech UTM Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw



ZTA (Zero Trust Access) VPN

WireGuard VPN Features



Performance

It is able to reach the highest throughput values.



Efficiency

Its lightweight design, potentially offers lower latency.



Privacy

It uses only UDP that lost data can not be retrieved.



Availability

It is easy to setup and not exclusively locked to any platforms.

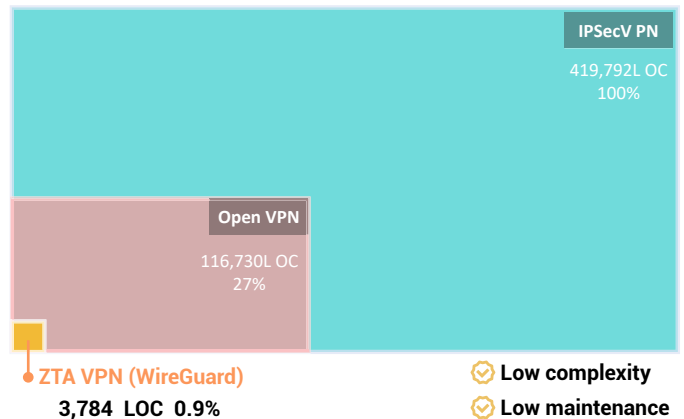


Security

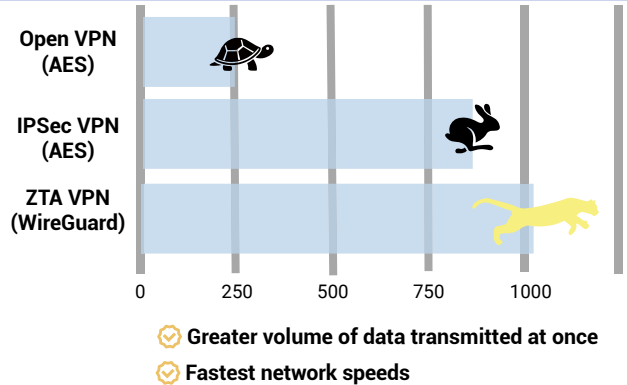
It uses up-to-date algorithms (ChaCha20-Poly1305) that are less vulnerable to timing attacks.

ShareTech ZTA VPN vs. Mainstream VPNs

1. Software Metric LOC (Lines of Code)



2. Bandwidth (Mbps)



ShareTech ZTA VPN vs. Mainstream VPN Protocols

VPN Protocol	Encryption	Speed	Stability	Streaming / P2P
PPTP	Poor	Fast	Fair	Poor
L2TP/IPSec	Average	Medium	Good	Poor
SSL VPN	Good	Fast	Good	Good
ZTA VPN	Excellent	Excellent	Excellent	Good

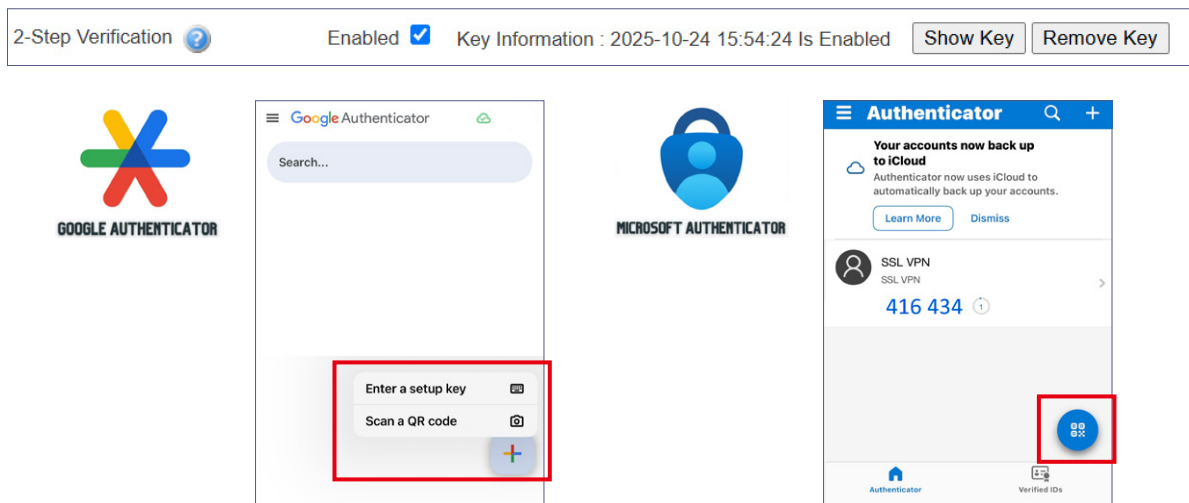
UTM Configuration Guide (Administrator)

Step 1: Create User Groups

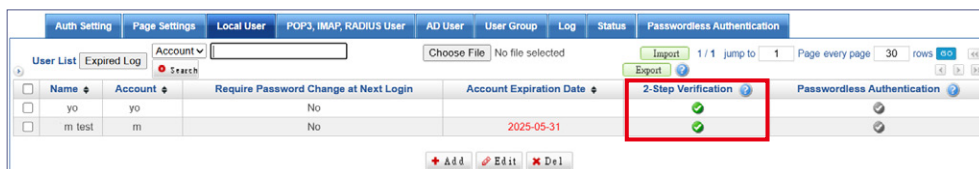
Go to **Object** → **Authentication** → **Select authentication mode (Local User / POP3, IMAP / RADIUS / AD Server)** → **User Group** to create the group used for ZTA VPN authentication. Whether to enable **two-step verification** (2FA) for ZTA VPN.

If 2FA is enabled, users can use **Microsoft Authenticator**, **Google Authenticator**, or a **third-party authenticator app**. Future login will use the same authenticator app (same device).

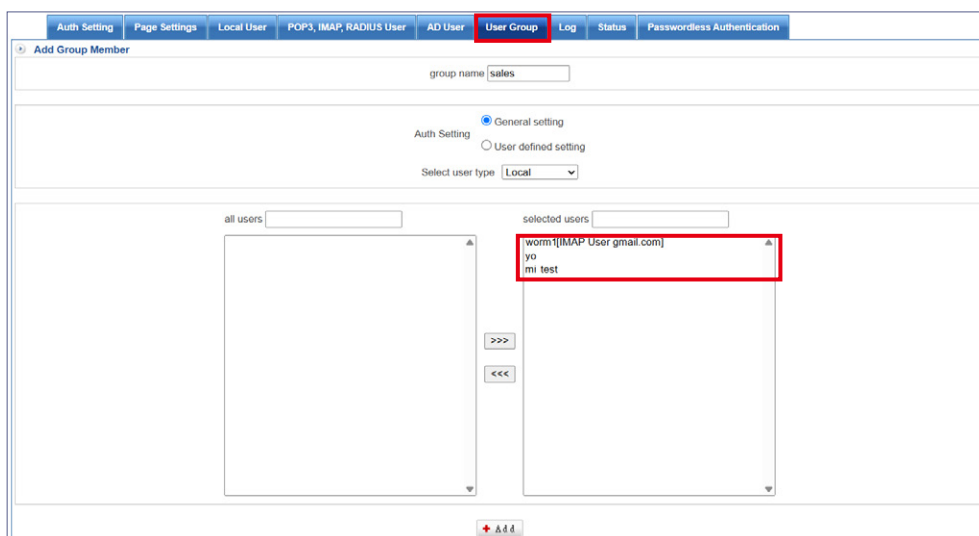
Note: If a user changes devices or deletes key, the administrator can display the **key** and send it to the user for manual input. **For security, it is recommended that administrators regenerate the key.**



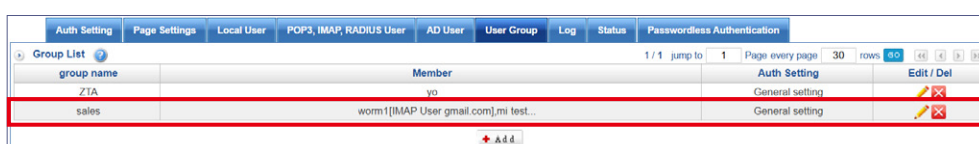
Example: Using the **Local User** → **User Group** with **two-step verification**.



← Figure 1



← Figure 2



← Figure 3

Step 2: Configure Remote Internet Access

Go to [ZTA VPN](#) → [Client-to-Site](#) → [ZTA VPN Setup](#) to configure VPN parameters.

Besides, administrators can choose whether to [allow clients to access the Internet through VPN](#).

If disabled, the system automatically removes corresponding routes from the client side, reducing unnecessary bandwidth and resource usage.

The screenshot shows the 'ZTA VPN Setup' configuration page. The 'Server Setting' section is highlighted with a red box. It includes the following fields and values:

- Service Status: Start
- Enable: Note: It will take a while to activate the ZTA VPN. Please wait patiently.
- Local Interface: Hide ppp4000
- Client Linking Setting *: Hide ppp4000
- Local Port *: (Use both TCP and UDP protocols)
- Max concurrent connections: (Range: 20 ~ 200)
- Connection Timeout: seconds (Range: 30 ~ 180)
- 2-Step Verification Expiry Time: Minutes (Range: 10 ~ 60, 0 means disabled.)
- Client IP Range: / (Client IP range need different with Zone interface.)
- DNS Server 1:
- DNS Server 2:

The 'Client Route Setup' section is also highlighted with a red box. It includes the following fields and values:

- Enable remote connection over the Internet:
- Push Route: Hide

▲ Figure 4

Step 3: Configure Client-to-Site ZTA VPN

Go to [ZTA VPN](#) → [Client-to-Site](#) → [Client List](#) to configure ZTA VPN group.

You can define whether users are [redirected to a specific webpage](#) after connecting.

Note: Once connected successfully, the displayed URL will automatically sync remote settings.

Administrators can configure settings dynamically, simplifying management.

The screenshot shows the 'New Certificate Group' configuration page. The 'Address of information message' field is highlighted with a red box. It contains the following text:

Address of information message: (Maximum 1024 Characters)

▲ Figure 5

Users can access it directly via a download URL that the administrator must preconfigure:

[https://\[interface_IP_or_domain\]:\[HTTPS_port\]/ztavpn.php](https://[interface_IP_or_domain]:[HTTPS_port]/ztavpn.php)

Example:

<https://168.168.168.168:4433/ztavpn.php> or <https://domain:4433/ztavpn.php>

The screenshot shows the 'Client List' configuration page. The 'Download client software and certificate from a URL' field is highlighted with a red box. It contains the following text:

Download client software and certificate from a URL: [https://\[Wan IP Address or Domain\]:\[HTTPS Port\]/ztavpn.php](https://[Wan IP Address or Domain]:[HTTPS Port]/ztavpn.php)

Below this, a table shows the configuration for a certificate group named 'test':

Comment	Authentication Group	User Management	Delete
test	sales	Group Member Number: 3	<input type="button" value="X"/>

▲ Figure 6

Configuration → Basic Setting → Administrative Access → HTTPS Port

Administrative Access :

HTTPS Port:

Idle Timeout: (5 ~ 60) Minutes

Security: TLSv1.1 TLSv1.2 TLSv1.3

▲ Figure 7

Otherwise, Administrators can download and provide the ZTA client software to users.

User Account	Certificate	Download Software	Download Certificate	User Static IP address	User Static MAC Address	Enable	Edit
worm1	Cancel Regenerate	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
yo	Cancel Regenerate	<input type="checkbox"/>	<input type="checkbox"/>	10.0.1.254		<input type="checkbox"/>	<input type="checkbox"/>
mi	Cancel Regenerate	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>

▲ Figure 8

Step 4: Modify User Download Page

Administrators can customize the user download page and preview it.

Note: The logo is shared with the Internet authentication page.

Go to **Object > Authentication > Page Settings** → Client Login Message → Upload Logo to modify.

Client Download Page Setting **Download Page Preview**

Content Block Color: Word:

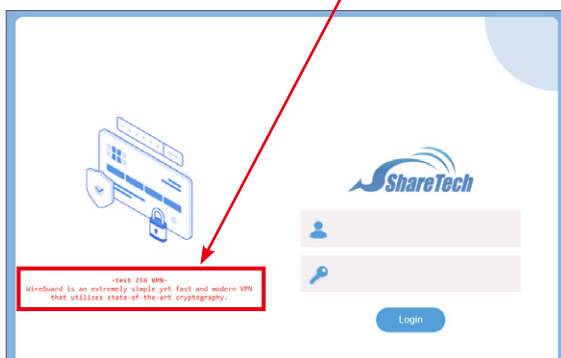
Foreground Block Color: Word:

Background Block Color: Background:

Content:

```
<p>
<strong style="color:#f00;">-test ZTA VPN-</strong>
WireGuard is an extremely simple yet fast and modern VPN that
utilizes state-of-the-art cryptography.
</p>
```

▲ Figure 9



▲ Figure 10



▲ Figure 11

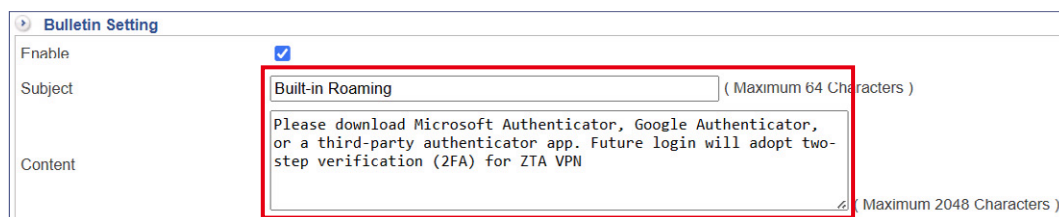
Note: When a key has already been generated, the verification page (QR Code) will **not** display key information. If a user changes devices or deletes key, the administrator can see the earlier [Step 1](#)).



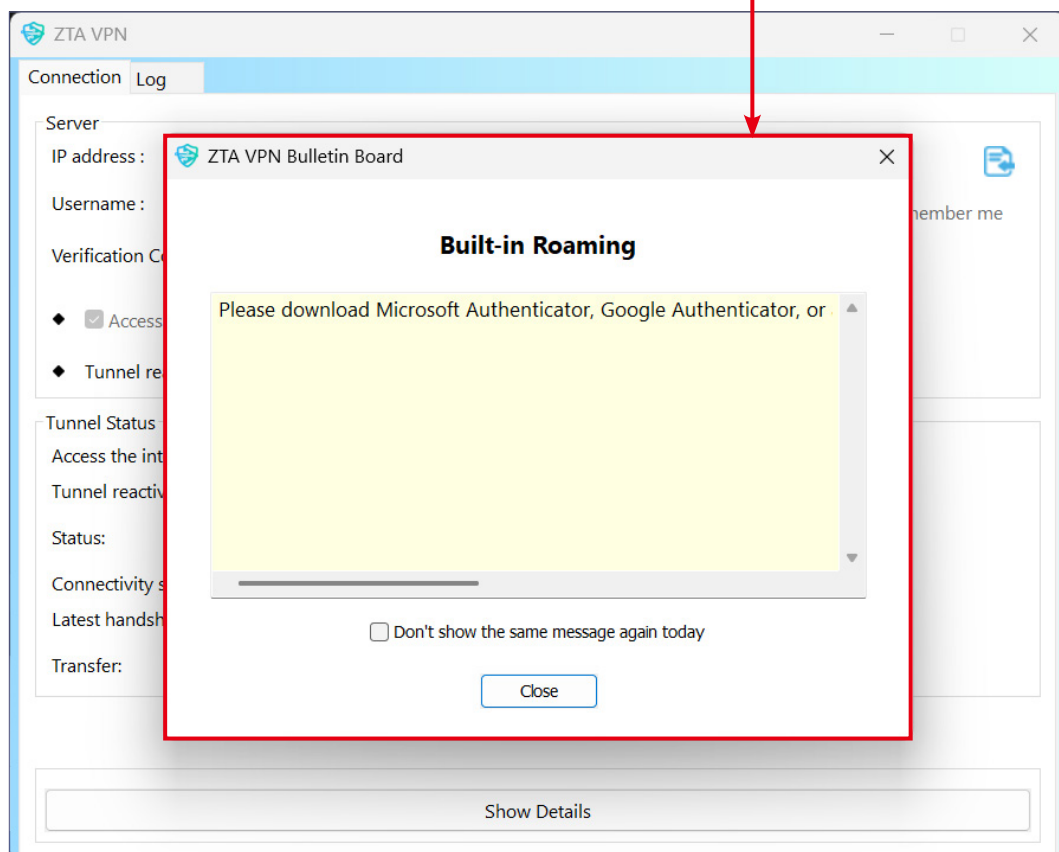
▲ Figure 12

Step 5: Bulletin Board Configuration

ZTA VPN provides an interface for administrators to [set announcements](#).



▲ Figure 13



▲ Figure 14

Step 6: Connection Monitoring

Administrators can check the authentication connection status and can search for historical logs.

The screenshot shows the 'Connection Status' tab. At the top, there are navigation tabs: 'ZTA VPN Setup', 'Client List', 'Page Setting', 'Connection Status' (highlighted), and 'Connection Log'. Below these is a 'Refuse Connection Log' section with a search bar and 'Start/Stop' buttons. The main area is a table with the following columns: Account, Status, Source IP Address, Local IP Address, MAC, Last Connection / Connection Duration, Local Interface, and Kick. A single row is visible with the account 'yo', status 'On line', and last connection time '2025-09-11 15:13:06'.

▲ Figure 15

The screenshot shows the 'Connection Log - Search Condition' section with a search form. The 'Search Result' section displays a table with the following columns: Time, Account, Source IP, Source Port, The machine dispensed IP, MAC, Local Interface, and Event. The table contains 10 rows of log entries, including login and logout events for various users and interfaces.

Time	Account	Source IP	Source Port	The machine dispensed IP	MAC	Local Interface	Event
2025-09-17 16:18:21	ist26	2	3	14	10.0.1.101	WAN1 PPPOE (WAN1)	Login
2025-09-17 16:05:29	esi8	6		3	10.0.1.146	WAN1 PPPOE (WAN1)	Login
2025-09-17 16:01:04	ist38	6		0	10.0.1.5	WAN1 PPPOE (WAN1)	Login (Connection Timeout)
2025-09-17 15:07:48	esi7	2	3	32	10.0.1.169	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:44:15	ist18			17	10.0.1.236	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:36:45	esi8	6		3	10.0.1.146	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:30:58	esi4	2	3	17	10.0.1.234	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:30:16	esi4	2	3	17	10.0.1.234	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:28:49	esi7	2	3	32	10.0.1.169	WAN1 PPPOE (WAN1)	Login
2025-09-17 14:25:54	esi7	2	3	19	10.0.1.203	WAN1 PPPOE (WAN1)	Login

▲ Figure 16