



## ZyWall/USG IPSec VPN Client Guide

1. In the Zywall/USG, go to **Configuration->Quick Setup->VPN Setup Wizard**, please use the **VPN Settings for Configuration Provisioning**. This will create a VPN rule that can be used with the Zywall/USG IpSec VPN client. Click **Next**.

The screenshot shows the 'VPN Setup Wizard' interface. At the top, there's a breadcrumb trail: 'Wizard Type > VPN Settings > Wizard Completed'. Below this, there are three numbered steps: 1, 2, and 3. Step 2 is highlighted. The main content area is titled 'Welcome'. It lists three options for VPN Settings:

- ☐ VPN Settings
  - Wizard Type
  - VPN Settings
  - Wizard Completed
- ☒ VPN Settings for Configuration Provisioning
  - Wizard Type
  - VPN Settings
  - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
  - VPN Settings
  - General Settings
  - Wizard Completed

2. Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

The screenshot shows the 'VPN Setup Wizard' interface. At the top, there's a breadcrumb trail: 'Wizard Type > VPN Settings > Wizard Completed'. Below this, there are three numbered steps: 1, 2, and 3. Step 2 is highlighted. The main content area is titled 'Please select the type of VPN policy you wish to setup.' It lists two options for Type of VPN policy:

- ☒ Express
- ☐ Advanced

3. Type the **Rule Name** used to identify this VPN connection and gateway. Click **Next**.

The screenshot shows the 'VPN Setup Wizard' interface. At the top, there's a breadcrumb trail: 'Wizard Type > VPN Settings > Wizard Completed'. Below this, there are three numbered steps: 1, 2, and 3. Step 2 is highlighted. The main content area is titled 'Express Settings'. It lists two options for Scenario:

- Rule Name: WIZ\_VPN\_PROVISIONING
- Application Scenario: Remote Access (Server Role)



4. Type a secure Pre-shared Key (8-32 characters). Set the Local Policy to be the IP address range of the network connected to the Zywall/USG.

The screenshot shows the 'VPN Setup Wizard' interface. At the top, a breadcrumb trail reads 'Wizard Type > VPN Settings > Wizard Completed'. Below this, three numbered tabs (1, 2, 3) are visible, with tab 2 being the active one. The main section is titled 'Express Settings' and contains a 'Configuration' subsection. It lists five settings: 'Secure Gateway' (Any), 'Pre-Shared Key' (zyx12345), 'Local Policy (IP/Mask)' (192.168.1.33 / 255.255.255.0), and 'Remote Policy (IP/Mask)' (Any). The values for 'Pre-Shared Key', 'Local Policy', and 'Remote Policy' are highlighted with red rectangular boxes.

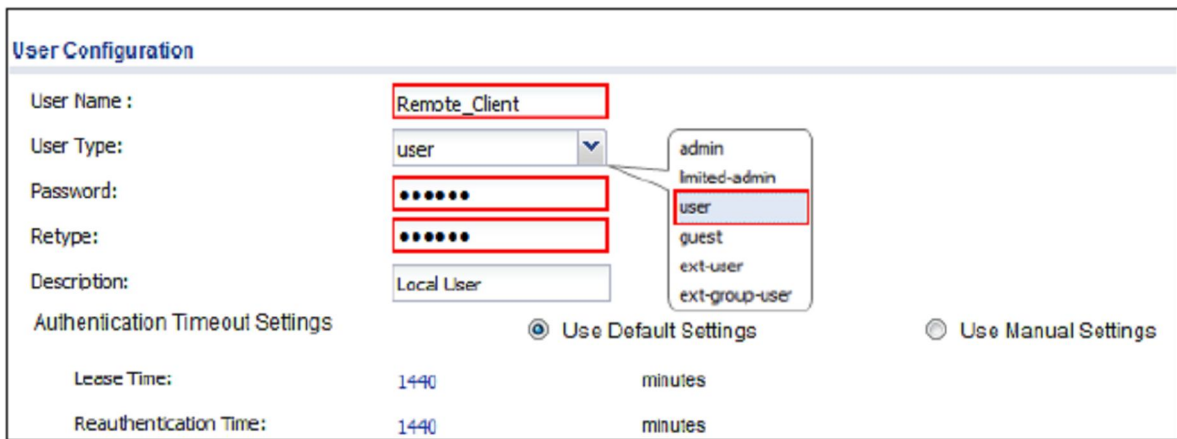
5. The final screen provides a read-only summary of the VPN tunnel. Click **Save**.

The screenshot shows the 'VPN Setup Wizard' interface, specifically the 'Summary' screen. The breadcrumb trail is 'Wizard Type > VPN Settings > Wizard Completed'. Tab 2 is active. The 'Express Settings' section contains a 'Summary' subsection. It lists the same five settings as the previous screen, but they are now read-only: 'Rule Name' (WIZ\_VPN\_PROVISIONING), 'Secure Gateway' (Any), 'Pre-Shared Key' (zyx12345), 'Local Policy (IP/Mask)' (192.168.1.0 / 255.255.255.0), and 'Remote Policy (IP/Mask)' (Any).

6. Now the rule is configured on the Zywall/USG. The Phase 1 rule will appear under **Configuration->VPN->IPSec VPN->VPN Gateway** and the Phase 2 rule will appear under **Configuration->VPN->IPSec VPN->VPN Connection**. Please click **Close** to exit the wizard.

This is a duplicate of the previous screenshot, showing the 'VPN Setup Wizard' Summary screen with the same configuration details.

- Next go to **Configuration->Object->User/Group->Add a User** and create a user account for the IPSec VPN Client user.



**User Configuration**

User Name : Remote\_Client

User Type: user

Password: .....

Retype: .....

Description: Local User

Authentication Timeout Settings

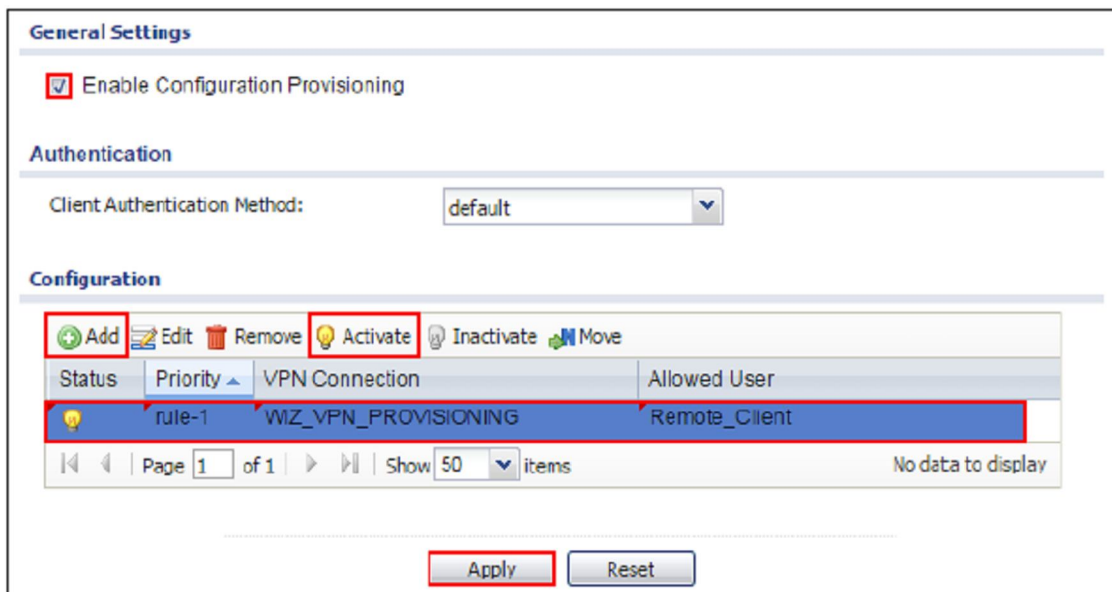
☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Dropdown menu options: admin, limited-admin, user, guest, ext-user, ext-group-user

- Next go to **Configuration->VPN->IPSec VPN ->Configuration Provisioning**. In the **General Settings** section, select the **Enable Configuration Provisioning**. Then, go to the **Configuration** section and click **Add** to bind a configured **VPN Connection** for the **Allowed User**. Click **Activate** and **Apply** to save the configuration.



**General Settings**

☒ Enable Configuration Provisioning

**Authentication**

Client Authentication Method: default

**Configuration**

Buttons: Add, Edit, Remove, Activate, Inactivate, Move

Status	Priority	VPN Connection	Allowed User
rule-1		WIZ_VPN_PROVISIONING	Remote_Client

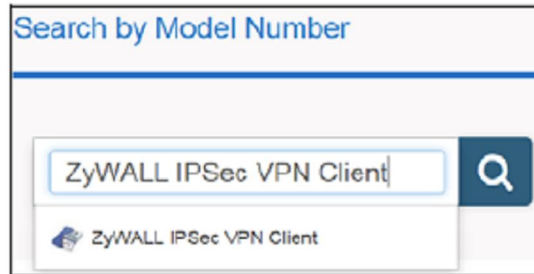
Page 1 of 1 | Show 50 items | No data to display

Buttons: Apply, Reset

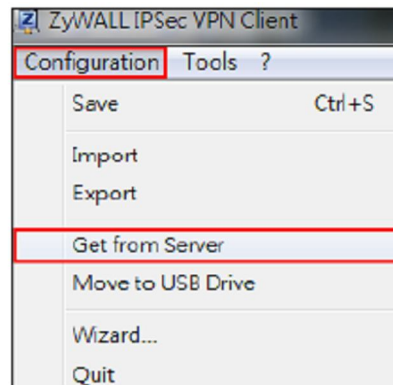


9. Next, if you have not already done so, please download the IPSec VPN Client software from the Zyxel download library.

[http://www.zyxel.com/support/download\\_landing.shtml](http://www.zyxel.com/support/download_landing.shtml)



10. Once installed, open the IPSec VPN Client, select **Configuration->Get from Server**.





11. Enter the WAN IP address or URL for the Zywall/USG in the **Gateway Address**. If you changed the default HTTPS port on the Zywall/USG, then please enter the new one here. Enter the **Login user name** and **password** exactly as configured in the previous steps (step 7). Click **Next** and you will see the client process the configuration from the Zywall/USG.

The screenshot shows the 'VPN Configuration Server Wizard' window at 'Step 1: Authentication'. The title bar says 'VPN Configuration Server Wizard'. The main heading is 'Step 1: Authentication' with the ZyXEL logo. Below it, the text asks 'What are the parameters of the VPN Server Connection?'. A sub-header states: 'You are going to download your VPN Configuration from the VPN Configuration Server. Enter below the authentication information required for the connection to the server.'

The form contains the following fields:

- 'Gateway Address:' with the value '172.124.163.150' entered.
- 'Port:' with the value '443' entered.
- 'Authentication:' with a dropdown menu set to 'Login + Password'.
- 'Login:' with the value 'Remote\_Client' entered.
- 'Password:' with masked characters '\*\*\*\*\*' entered.

At the bottom right, there are two buttons: 'Next >' and 'Cancel'.

The screenshot shows the 'VPN Configuration Server Wizard' window at 'Step 2: Processing...'. The title bar says 'VPN Configuration Server Wizard'. The main heading is 'Step 2: Processing...' with the ZyXEL logo. Below it, the text says 'Requesting the VPN Configuration.'.

The main area shows 'Downloading the VPN Configuration from the server:' with a progress bar that is approximately 25% full.

Below the progress bar, there is a list of steps with status icons:

- ✓ Init Ok.
- ✓ Init cnx server (172.124.163.150) Ok.
- ⌚ Send https request...

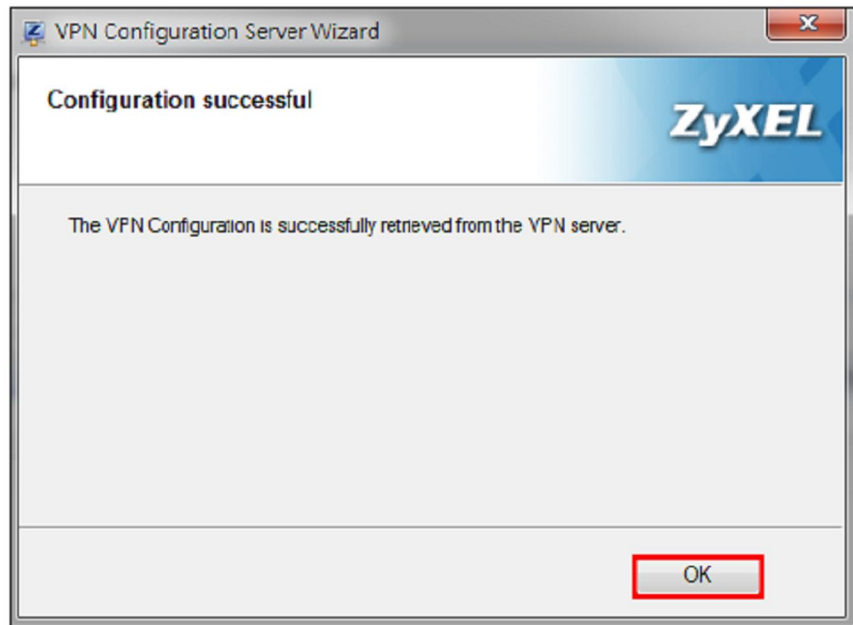
Below the list, there are three sub-steps:

- Receive Config. from Server...
- Write Config. file...
- Apply Config. file...

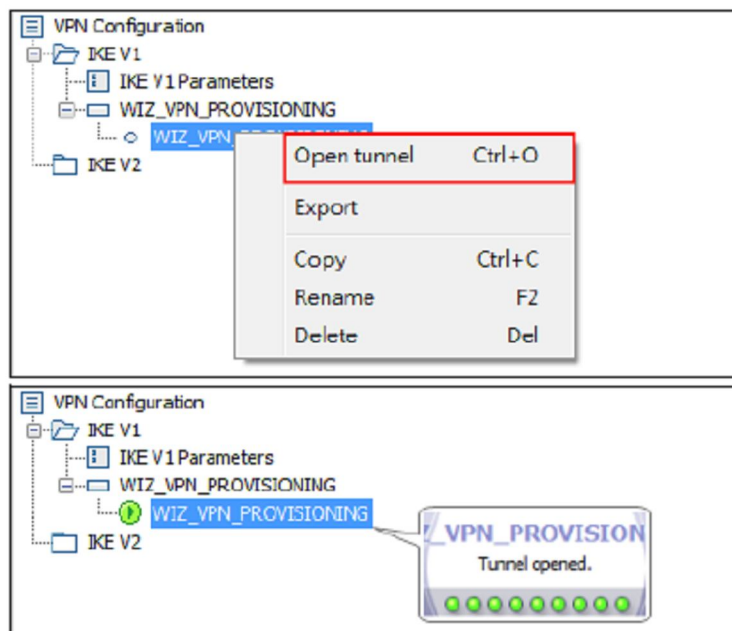
At the bottom, there are two buttons: '< Previous' and 'Cancel'.



12. Once finished, you will see the **Configuration Successful** page. Click to exit.



13. Go to **VPN Configuration ->IKEv1**, right click the **WIZ\_VPN\_Provisioning** and select **Open tunnel**. You will see the **Tunnel Opened** message on the bottom right of the screen.





14. Finally, test the IPSec VPN Tunnel. From the GUI of the Zywall/USG got to **Monitor->VPN Monitor->IPSec** to verify that the tunnel is up and passing traffic. You should see the **Up Time** and **Inbound** and **Outbound** bytes.

If we are only seeing **Inbound** traffic, but no **Outbound** traffic that may be due to a routing policy on the Zywall /USG that is sending the response traffic out another interface. If you are not seeing any **Inbound** traffic please make sure the LAN network of the USG does not conflict with the same subnet as the network you are trying to connect from. If both networks are on the same subnet, this can cause traffic to not properly route through the client's VPN interface.