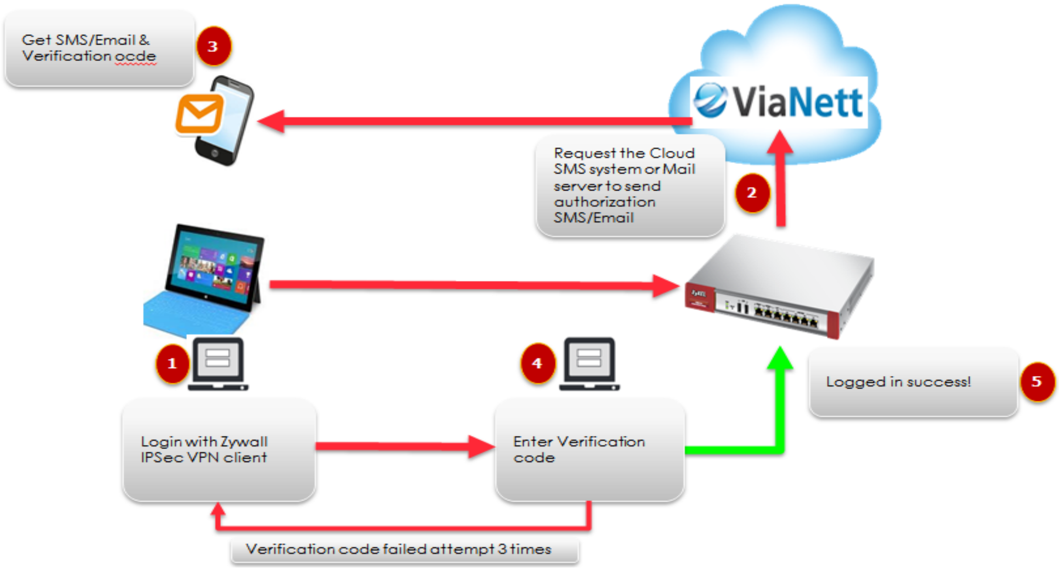
## How to Configure 2 factor for VPN connection?

This example shows how to use two-factor authentication to have double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel between a ZyWALL/USG and a ZyWALL IPSec VPN Client. The first layer is the VPN client user name / password and the second layer is an authorized SMS (via mobile phone number) or email address.


Get SMS/Email & Verification ocde
3
ViaNett
Request the Cloud SMS system or Mail server to send authorization SMS/Email
2
1
4
Login with Zywall IPSec VPN client
Enter Verification code
Logged in success!
5
Verification code failed attempt 3 times

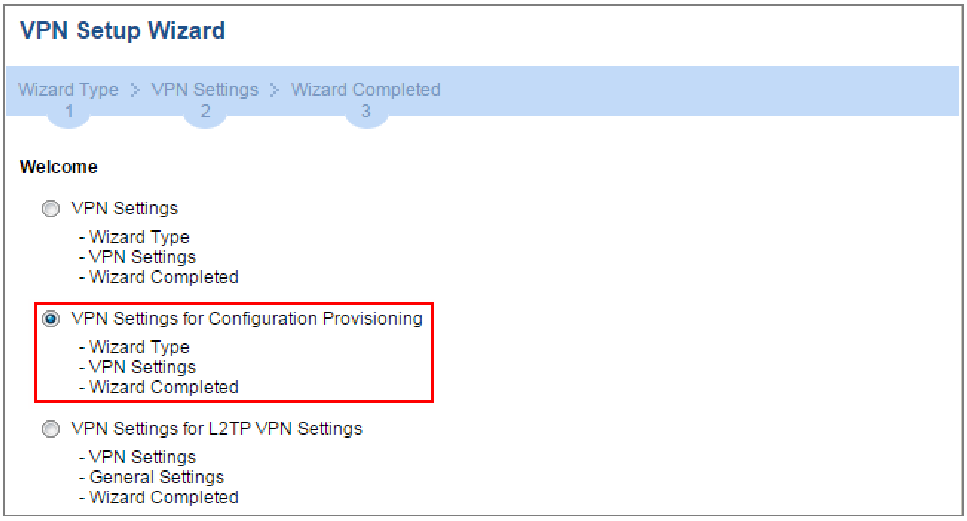
### Walkthrough

1. Set up the ZyWALL/USG IPSec VPN Tunnel on USG
2. Set up the ZyWALL IPSec VPN Client on windows client.
3. Set up notification for email and SMS message sending.
4. Enable 2 factor authentications for VPN service.

## Set up the ZyWALL/USG IPSec VPN Tunnel

In the ZyWALL/USG, go to **CONFIGURATION >Quick Setup > VPN Setup Wizard**, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the ZyWALL IPSec VPN Client. Click **Next**.

**Quick Setup > VPN Setup Wizard > Welcome**



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

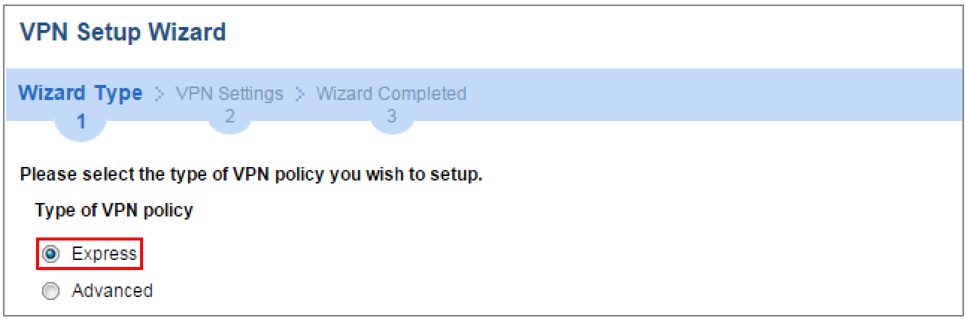
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

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**.

**Quick Setup > VPN Setup Wizard > Wizard Type**



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

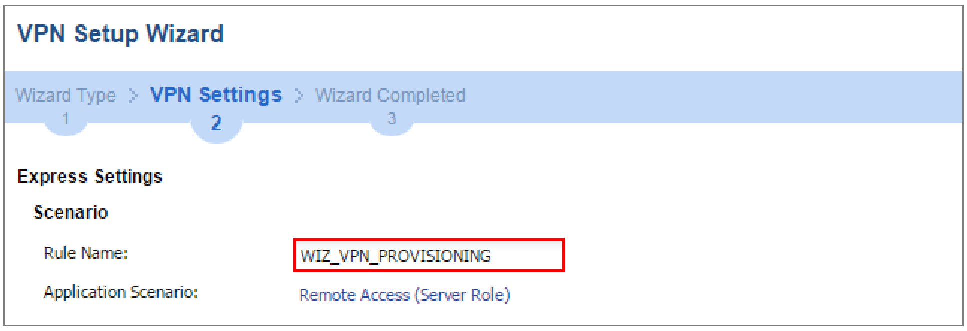
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

### Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-1



VPN Setup Wizard

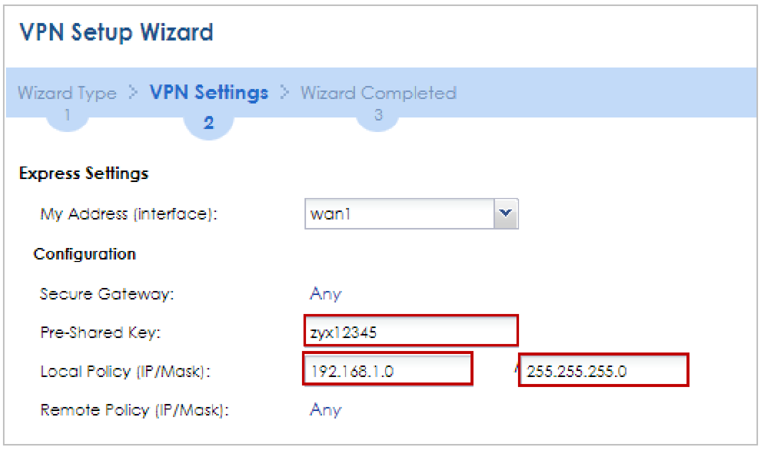
Express Settings

Scenario

| | |
|---|---|
| Rule Name: | WIZ_VPN_PROVISIONING |
| Application Scenario: | Remote Access (Server Role) |

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

### Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2



VPN Setup Wizard

Express Settings

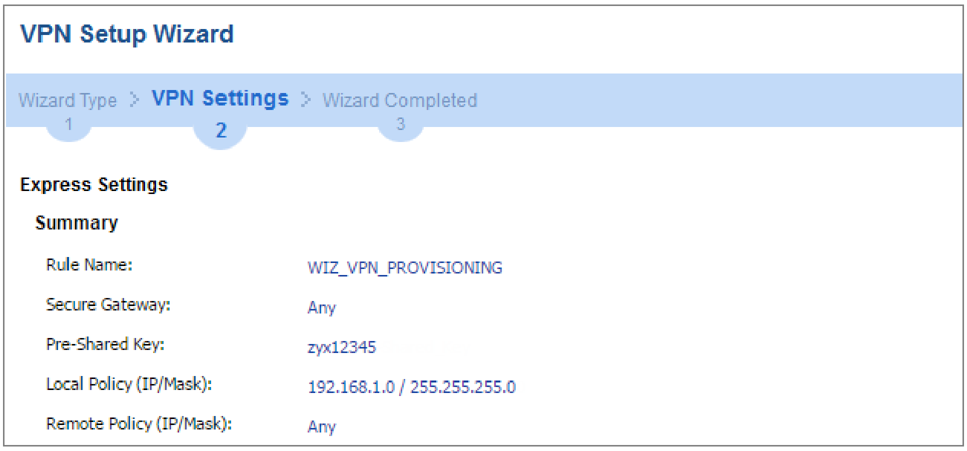
| | |
|---|---|
| My Address (interface): | wan1 |

Configuration

| | |
|---|---|
| Secure Gateway: | Any |
| Pre-Shared Key: | zyx12345 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

### Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-3



VPN Setup Wizard

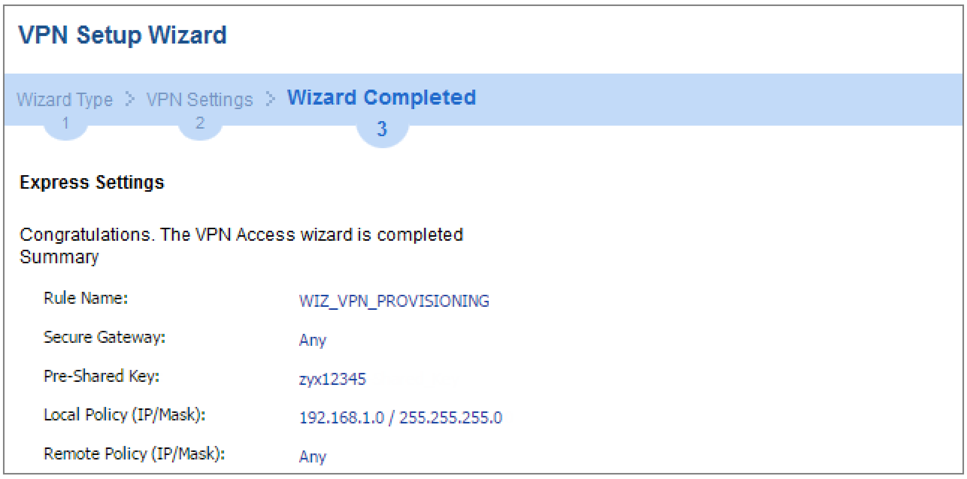
Express Settings

Summary

| | |
|---|---|
| Rule Name: | WIZ_VPN_PROVISIONING |
| Secure Gateway: | Any |
| Pre-Shared Key: | zyx12345 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

**Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed**



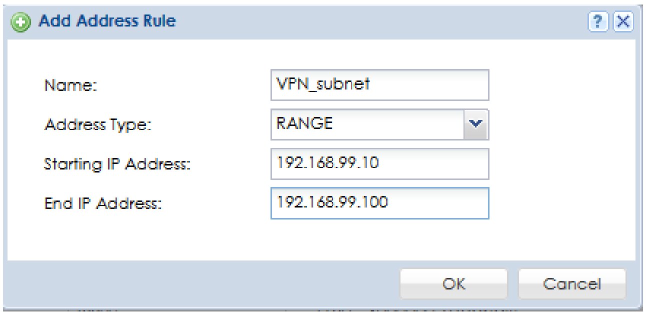
VPN Setup Wizard

**Express Settings**

Congratulations. The VPN Access wizard is completed
Summary

| | |
|---|---|
| Rule Name: | WIZ_VPN_PROVISIONING |
| Secure Gateway: | Any |
| Pre-Shared Key: | zyx12345 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

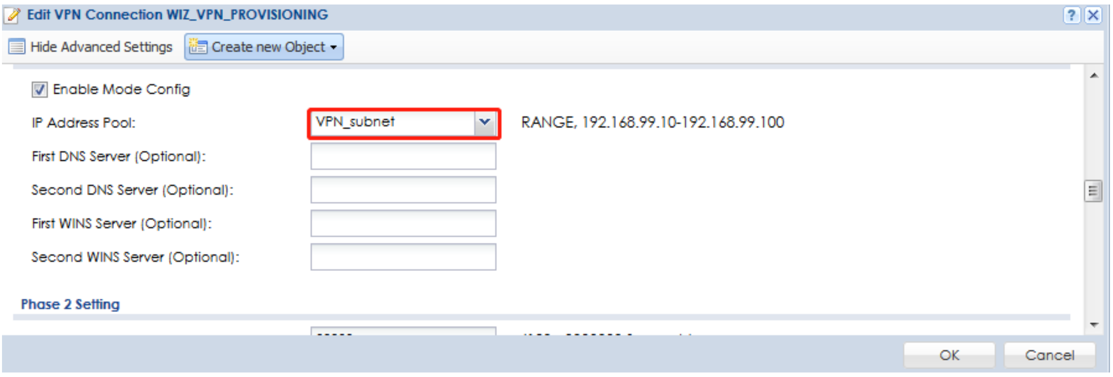
Go to **CONFIGURATION > VPN > IPSec VPN > VPN connection.** Enable **Mode config** for IPSec VPN client connection, create address object



Add Address Rule

| | |
|---|---|
| Name: | VPN_subnet |
| Address Type: | RANGE |
| Starting IP Address: | 192.168.99.10 |
| End IP Address: | 192.168.99.100 |

Select the address object for Mode Config VPN IP address Pool.



Edit VPN Connection WIZ_VPN_PROVISIONING

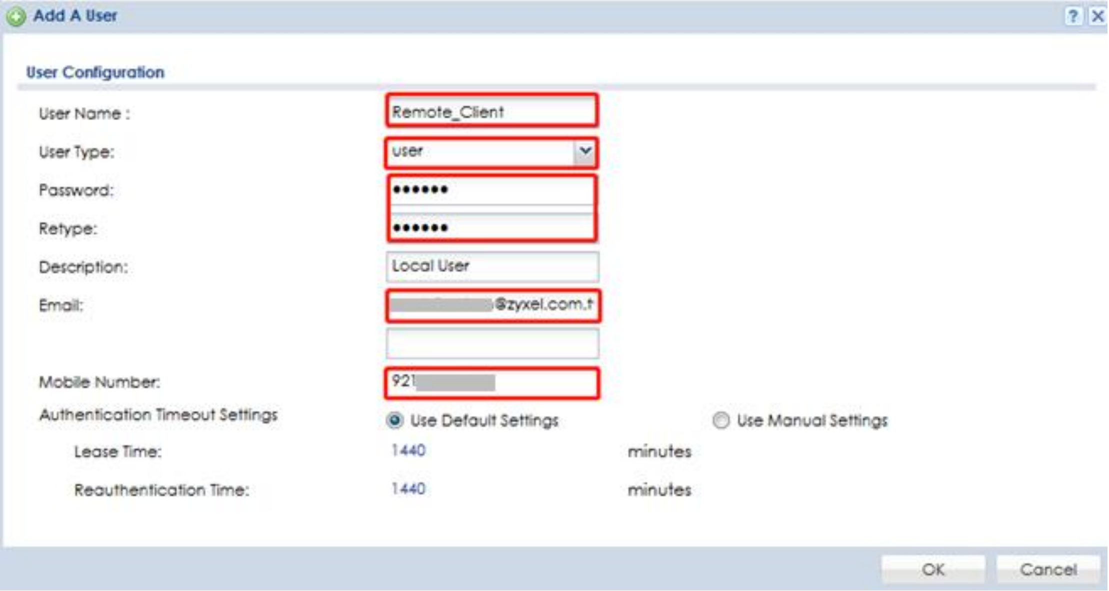
☑ Enable Mode Config

| | | |
|---|---|---|
| IP Address Pool: | VPN_subnet | RANGE, 192.168.99.10-192.168.99.100 |
| First DNS Server (Optional): | | |
| Second DNS Server (Optional): | | |
| First WINS Server (Optional): | | |
| Second WINS Server (Optional): | | |

Phase 2 Setting

Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user. Type one or more valid email addresses and valid mobile telephone number for this user so that messages can be sent to this user for 2 factor authentication.

**CONFIGURATION > Object > User/Group > Add A User**

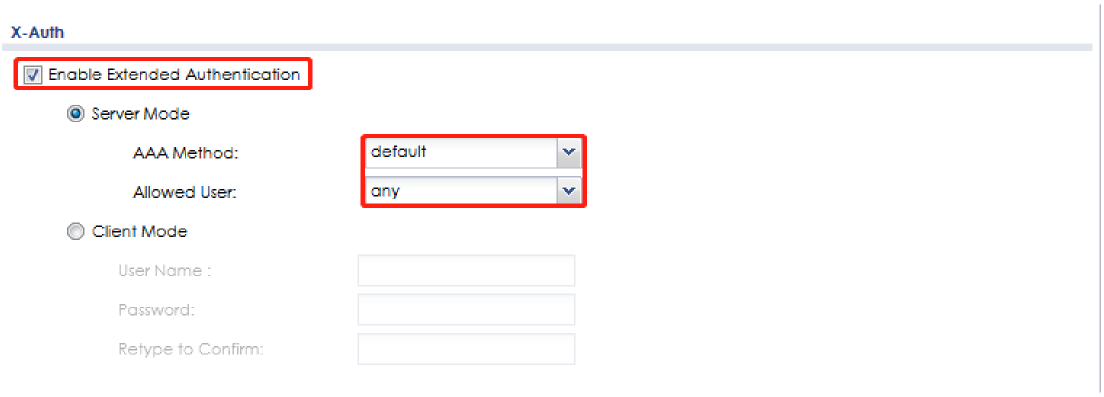


Add A User

User Configuration

| | | |
|---|---|---|
| User Name : | Remote_Client | |
| User Type: | user | |
| Password: | •••••• | |
| Retype: | •••••• | |
| Description: | Local User | |
| Email: | [redacted]@zyxel.com.t | |
| Mobile Number: | 921[redacted] | |
| Authentication Timeout Settings | ● Use Default Settings | ○ Use Manual Settings |
| Lease Time: | 1440 | minutes |
| Reauthentication Time: | 1440 | minutes |

Go to **CONFIGURATION > VPN > IPSec VPN > Gateway,** enable X-Auth for VPN client authentication.



X-Auth

☑ Enable Extended Authentication

● Server Mode

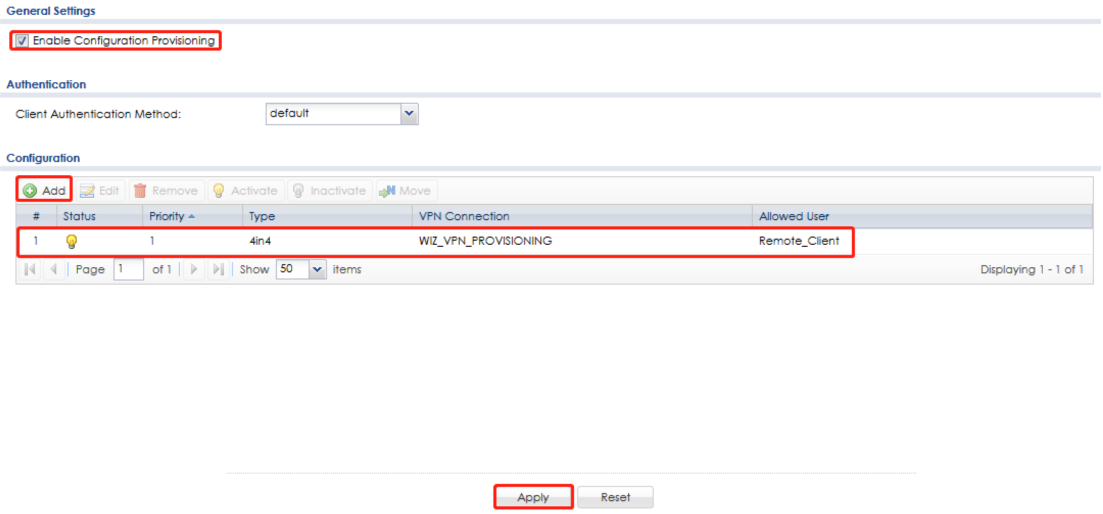
| | |
|---|---|
| AAA Method: | default |
| Allowed User: | any |

○ Client Mode

| | |
|---|---|
| User Name : | |
| Password: | |
| Retype to Confirm: | |

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** to **Allowed User**. Click **Activate** and **Apply** to save the configuration.

**CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning**



General Settings

☑ Enable Configuration Provisioning

Authentication

Client Authentication Method: default

Configuration

Add | Edit | Remove | Activate | Inactivate | Move

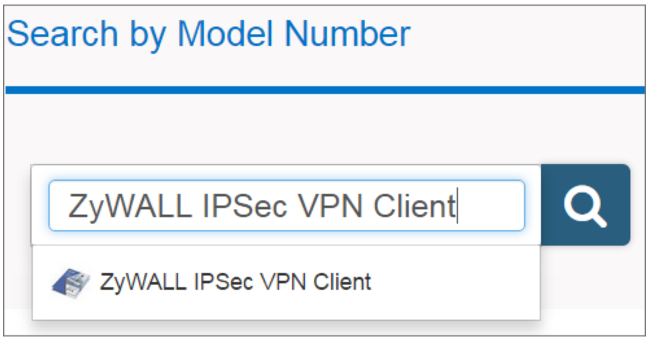
| # | Status | Priority | Type | VPN Connection | Allowed User |
|---|---|---|---|---|---|
| 1 | 💡 | 1 | 4in4 | WIZ_VPN_PROVISIONING | Remote_Client |

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Apply | Reset

## Set up the ZyWALL IPSec VPN Client

Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library: http://www.zyxel.com/support/download_landing.shtml



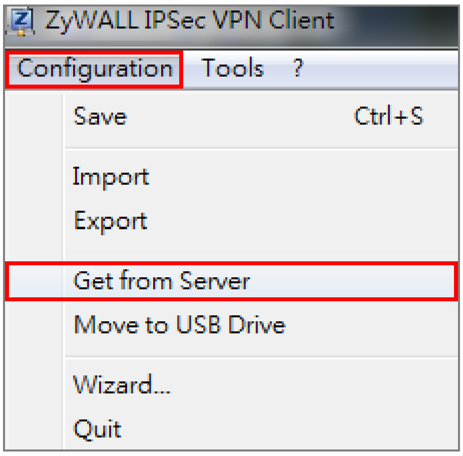
Search by Model Number

ZyWALL IPSec VPN Client

ZyWALL IPSec VPN Client

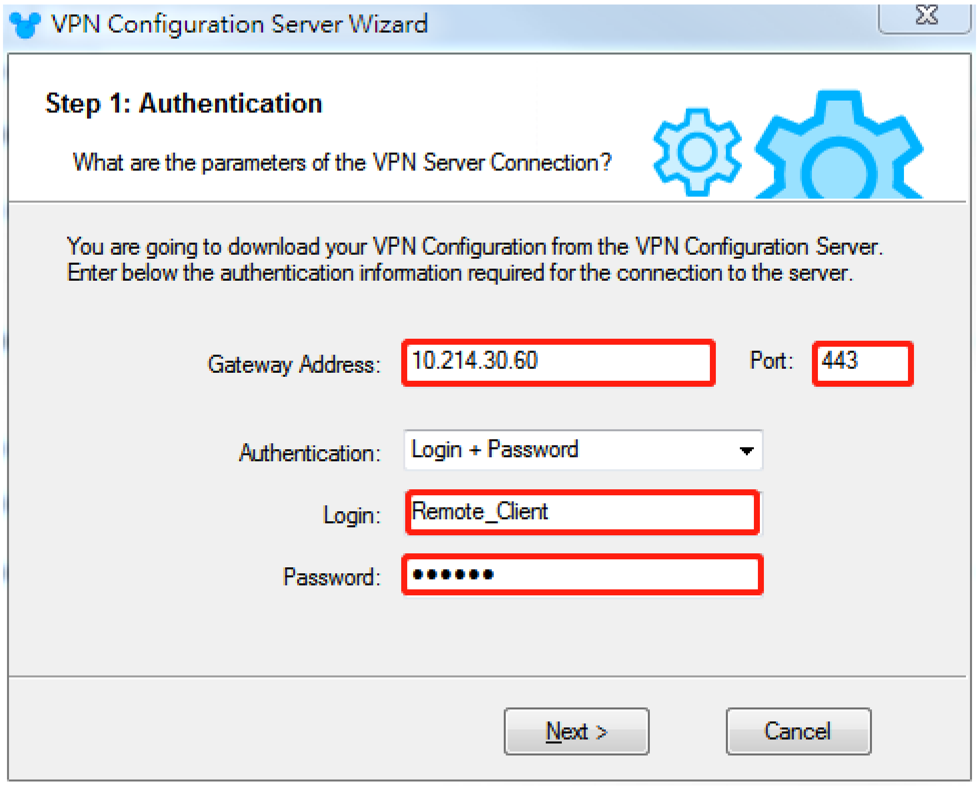
Open ZyWALL IPSec VPN Client, select **CONFIGURATION > Get from Server**.

**CONFIGURATION > Get from Server**



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, and then enter the new one here. Enter the **Login** user name and **Password** exactly as configured on the ZyWALL or external authentication server. Click **Next**, you will see it's processing VPN configuration from the server.

**CONFIGURATION > Get from Server > Step 1: Authentication**



**Step 1: Authentication**

What are the parameters of the VPN Server Connection?

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.

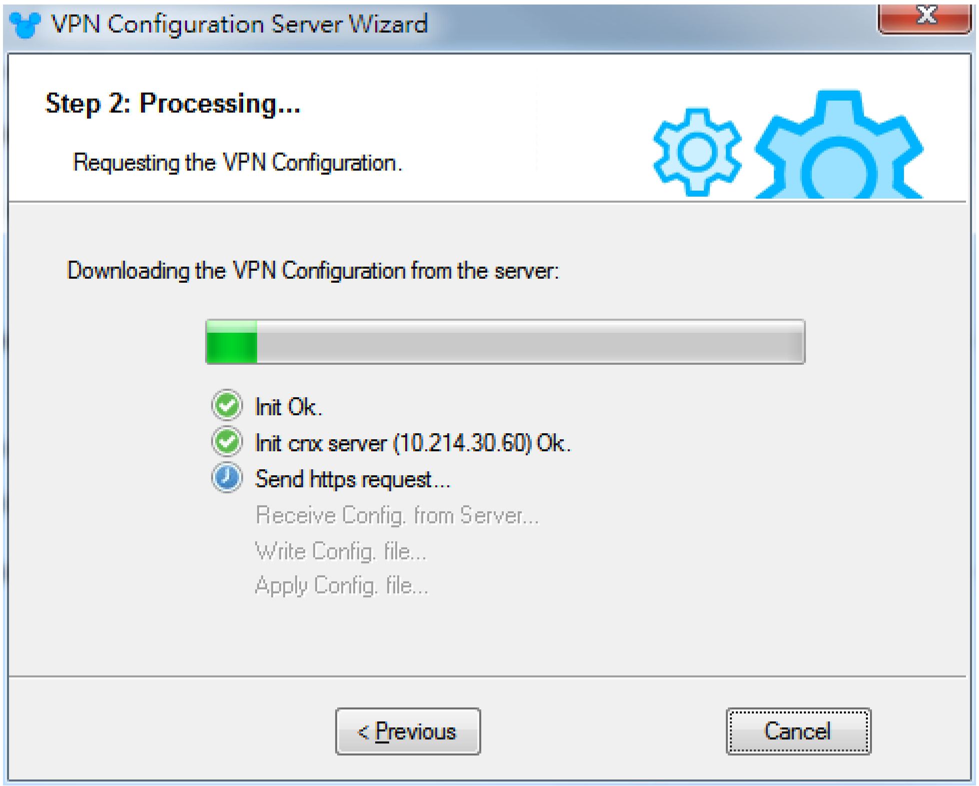
Gateway Address: 10.214.30.60 Port: 443

Authentication: Login + Password

Login: Remote_Client

Password: ••••••

CONFIGURATION > Get from Server > Step 2: Processing



Step 2: Processing...

Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

✓ Init Ok.

✓ Init cnx server (10.214.30.60) Ok.

Send https request...

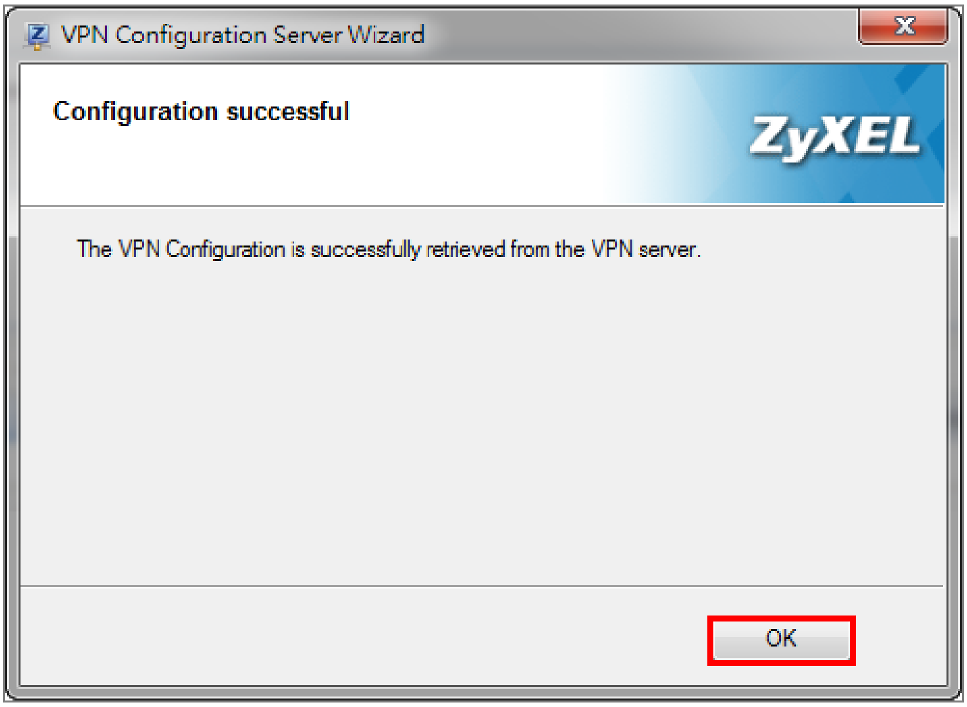
Receive Config. from Server...

Write Config. file...

Apply Config. file...

Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

**CONFIGURATION > Get from Server > Configuration successful**

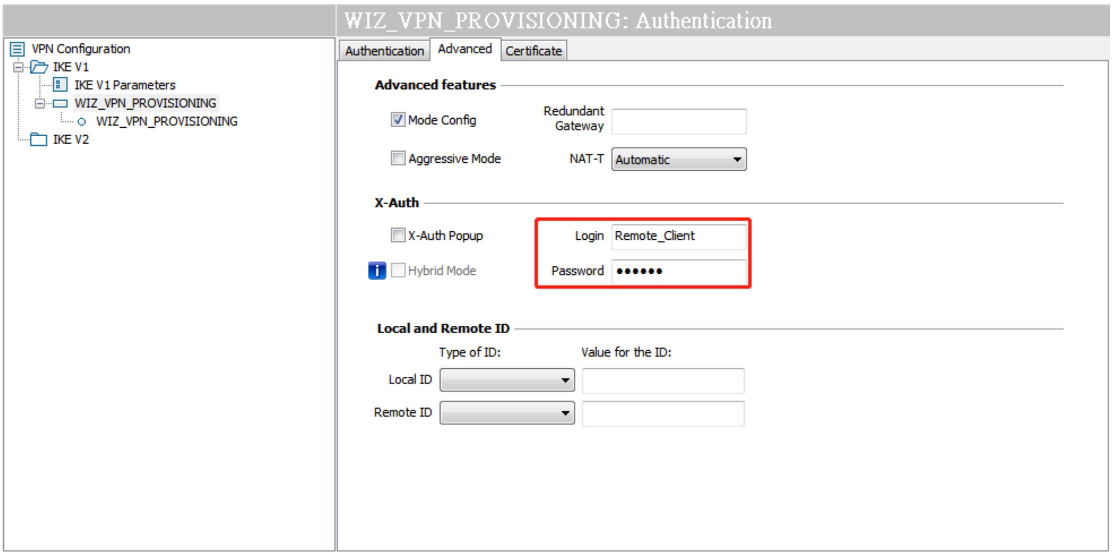


VPN Configuration Server Wizard

Configuration successful

The VPN Configuration is successfully retrieved from the VPN server.

**VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Advanced,** type Login account and password for authentication.



WIZ_VPN_PROVISIONING: Authentication

Advanced features

☑ Mode Config

Redundant Gateway

□ Aggressive Mode

NAT-T Automatic

X-Auth

□ X-Auth Popup

Login Remote_Client

□ Hybrid Mode

Password ••••••

Local and Remote ID

Type of ID:

Value for the ID:

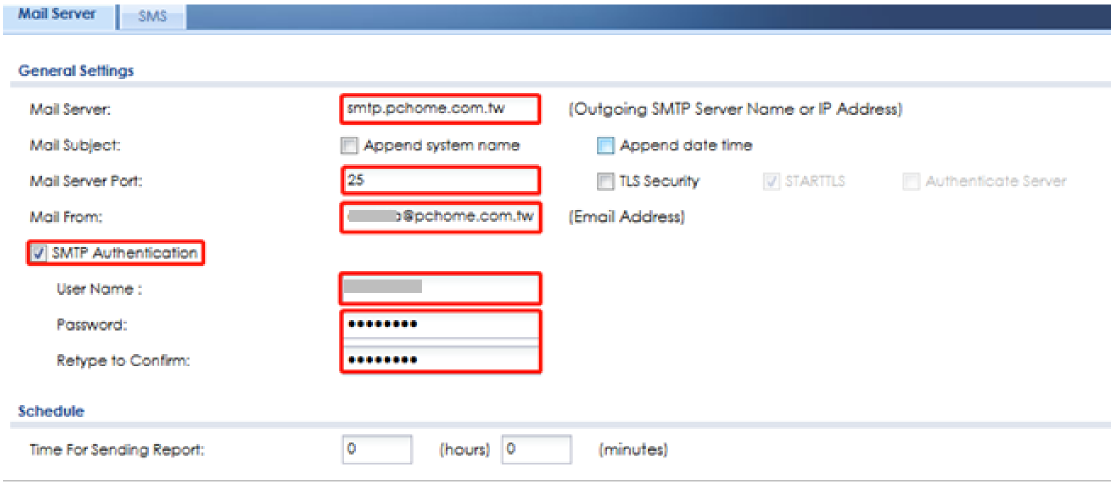
Local ID

Remote ID

## Set up notification for 2 factor authentication

In the ZyWALL/USG, go to **CONFIGURATION > System > Notification > Mail Server**

1. Type the name or IP address of the SMTP server.
2. Enter the service port for SMTP.
3. Type the e-mail address from which the outgoing e-mail is delivered.
4. Select this check box if it is necessary to provide a user name and password to the SMTP server.
5. Click **"Apply"** button to save your changes to the Zyxel Device.



General Settings

Mail Server: smtp.pchome.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: [redacted]@pchome.com.tw (Email Address)

☑ SMTP Authentication

User Name : [redacted]

Password: ••••••••

Retype to Confirm: ••••••••

Schedule

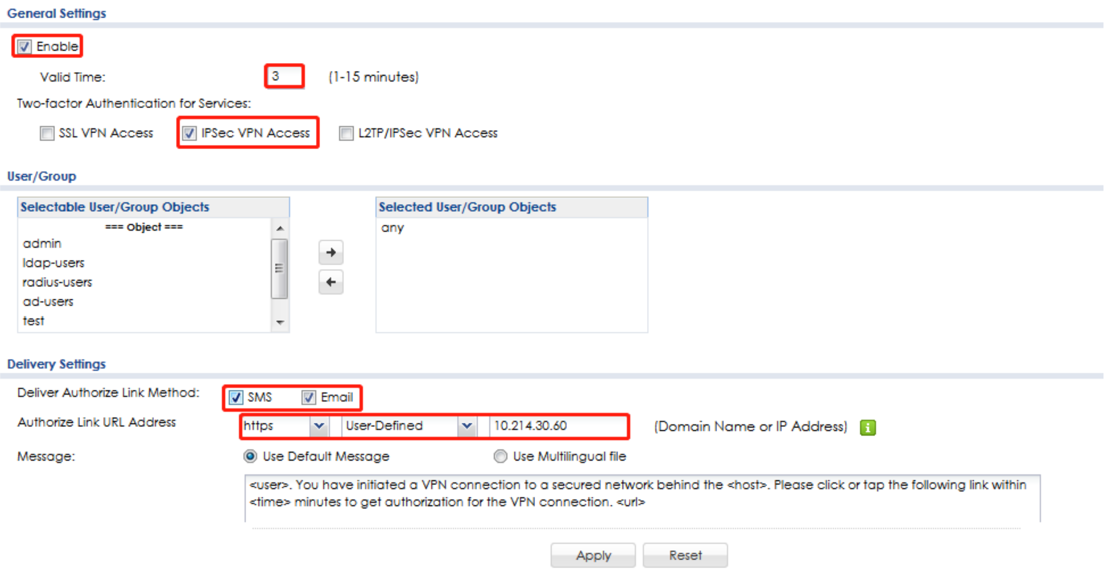
Time For Sending Report: 0 (hours) 0 (minutes)

## Set up authentication for 2 factor VPN connection

In the ZyWALL/USG, go to **CONFIGURATION > Object > Auth.Method > Two-factor Authentication.**

1. Select the check box **"Enable"** to enable 2 factor authentications.
2. Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection.
3. Select which kinds of VPN tunnels require Two-Factor Authentication. in this scenario, we enable 2 factor authentication on IPSec VPN Access
4. This list displays the names of the users and user groups that can be selected for two-factor authentication.
5. Use this section to configure how to send an SMS or email for authorization. We select both methods in this scenario.
6. Configure the link that the user will receive in the SMS or email. The user must be able to access the link.
7. You can either create a default message in the text box or upload a message file (Use Multilingual file) from your computer.

8. Click “**Apply**” button to save your changes to the Zyxel Device.



General Settings

☑ Enable

Valid Time: 3 (1-15 minutes)

Two-factor Authentication for Services:

□ SSL VPN Access ☑ IPSec VPN Access □ L2TP/IPSec VPN Access

User/Group

| Selectable User/Group Objects | Selected User/Group Objects |
|---|---|
| === Object === | any |
| admin | |
| ldap-users | |
| radius-users | |
| ad-users | |
| test | |

Delivery Settings

Deliver Authorize Link Method: ☑ SMS ☑ Email

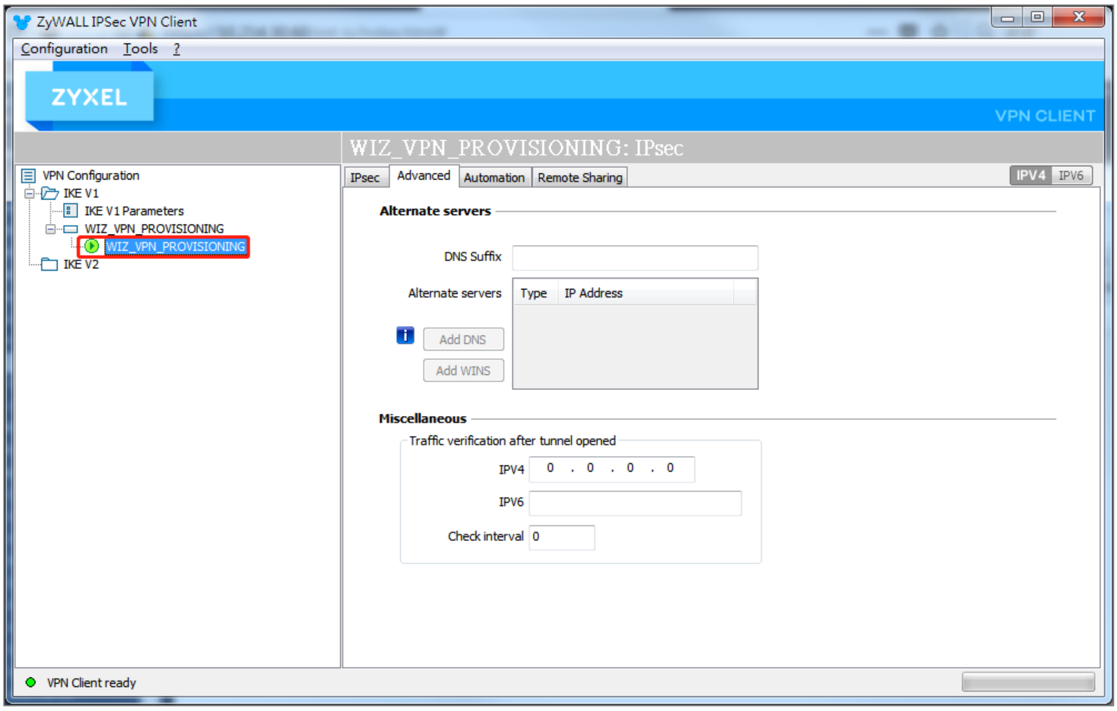
Authorize Link URL Address: https | User-Defined | 10.214.30.60 (Domain Name or IP Address)

Message: ● Use Default Message ○ Use Multilingual file

<user>. You have initiated a VPN connection to a secured network behind the <host>. Please click or tap the following link within <time> minutes to get authorization for the VPN connection. <url>

## Test the Result

Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on ZyWALL IPSec VPN client



WIZ_VPN_PROVISIONING: IPsec

Alternate servers

DNS Suffix

Alternate servers: Type | IP Address

Miscellaneous

Traffic verification after tunnel opened

IPV4 0 . 0 . 0 . 0

IPV6

Check interval 0

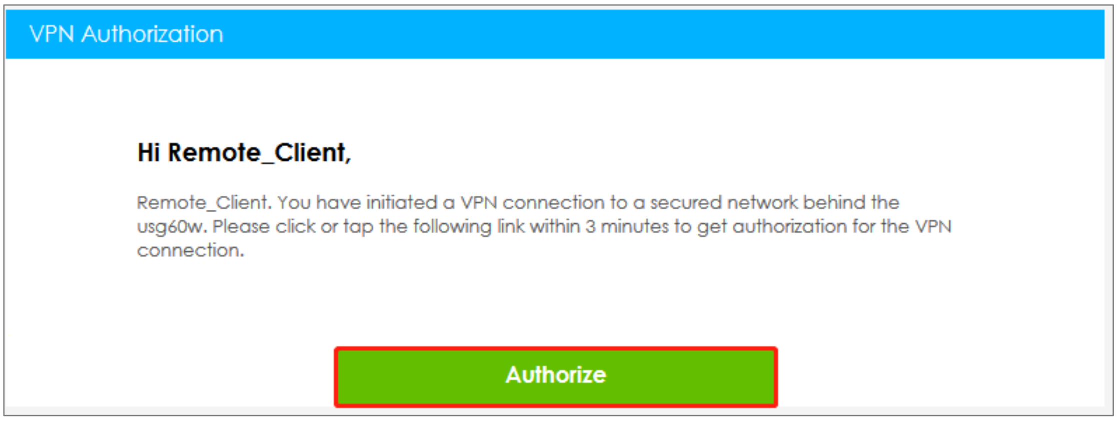
VPN Client ready

The VPN tunnel is created from the ZyWALL IPSec VPN client to the ZyWALL/USG, but we are still unable to access Intranet behind the ZyWALL/USG. The ZyWALL/USG send authorized link via phone number or email address in order to authenticate this user's use of the VPN tunnel (factor 2). If user does not click the link, then the Zyxel Device terminates the VPN connection. The client should access the authorization link sent via SMS or email by the Cloud SMS system within a specified deadline (Valid Time). If the authorization is correct and received on time, then the client can have VPN access to the secured network. If the authorization deadline has expired, then the client will have to run the VPN client again. If authorization credentials are incorrect or if the SMS/email was not received, then the client must check with the network administrator.

The following is authorized example by email and SMS

**Authorized by email link**

1. Received authorization mail with authorize link.

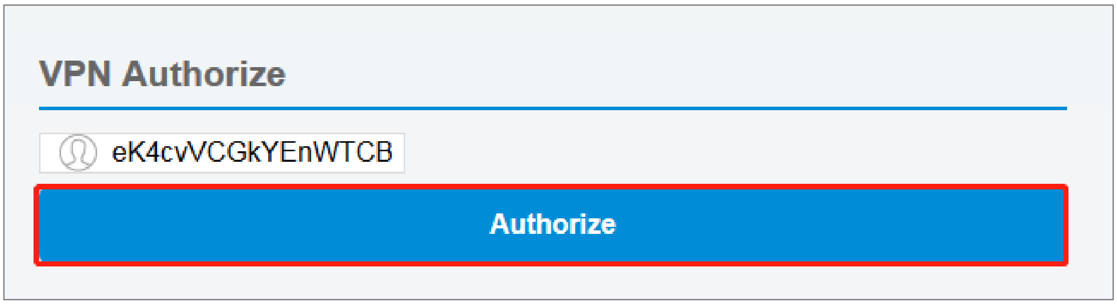


VPN Authorization

**Hi Remote_Client,**

Remote_Client. You have initiated a VPN connection to a secured network behind the usg60w. Please click or tap the following link within 3 minutes to get authorization for the VPN connection.

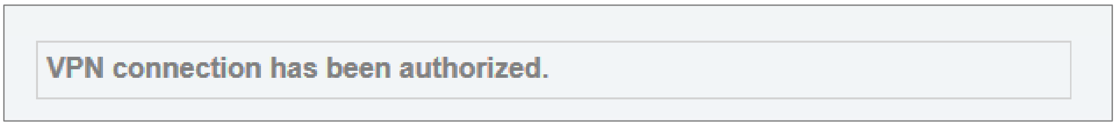
2. Click the **"Authorize" to** authorization.



VPN Authorize

eK4cvVCGkYEnWTCB

3. After we see "**VPN connection has been authorized**", we can access the secured network behind the ZyWALL/USG.



VPN connection has been authorized.