

SMART VPN CLIENT İLE WINDOWS'TAN VIGOR ROUTER'A IPsec VPN

Smart VPN Client resmi DrayTek VPN Client yazılımıdır. Çeşitli VPN protokollerini destekler. Bu belge routerın IPsec VPN sunucusu olarak nasıl ayarlanacağını, Windows Smart VPN Client'ın IPsec modunda nasıl ayarlayacağınızı ve IPsec bağlantısının nasıl başlatılacağını anlatır.



Vigor Router Kurulumu

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin, **Pre-shared Key** değerini girin ve tekrar şifreyi onaylayın sonra **OK**'a tıklayın.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Certificate for Dial-in

Pre-Shared Key

Pre-Shared Key

Confirm Pre-Shared Key

IPsec Security Method

Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

OK

Cancel

2. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin ve uygun olan bir indexe tıklayın.



Remote Access User Accounts:

| [Set to Factory Default](#) |View: All Online Offline

Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---

3. Remote Dial-in kullanıcısı için IPsec profili oluşturun.
 - a. **Enable this account** 'u seçin.
 - b. Allowed Dial-in Type bölümünde **IPsec Tunnel** 'in seçtiğinden emin olun.
 - c. Kaydetmek için **OK** 'a tıklayın.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="???"/> Password <input type="text" value="Max: 19 characters"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> IPsec XAuth		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="Max: 64 characters"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
<input type="checkbox"/> Specify Remote Node Remote Client IP <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)		IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/>
Subnet <input type="text" value="LAN 1"/> <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>		

Note:

Username can not contain characters " and '.

4. (İsteğe bağlı) Bağlantıyı yalnızca belirtilen IP adresinden ve bu hesap için özelleştirilmiş bir IKE Pre-Shared Key kullanmaya (genel pre-shared key yerine) izin vererek güvenliği artırmak için **Specify Remote Node** kullanın.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account

Idle Timeout second(s)

Allowed Dial-In Type

PPTP

IPsec Tunnel

L2TP with IPsec Policy

SSL Tunnel

IPsec XAuth

Specify Remote Node

Remote Client IP

or Peer ID

Netbios Naming Packet Pass Block

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet

Assign Static IP Address

Username Max: 19 characters

Password

Enable Mobile One-Time Passwords(mOTP)

PIN Code

Secret

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key

Digital Signature(X.509)

IPsec Security Method

Medium(AH)

High(ESP) DES 3DES AES

Local ID (optional)

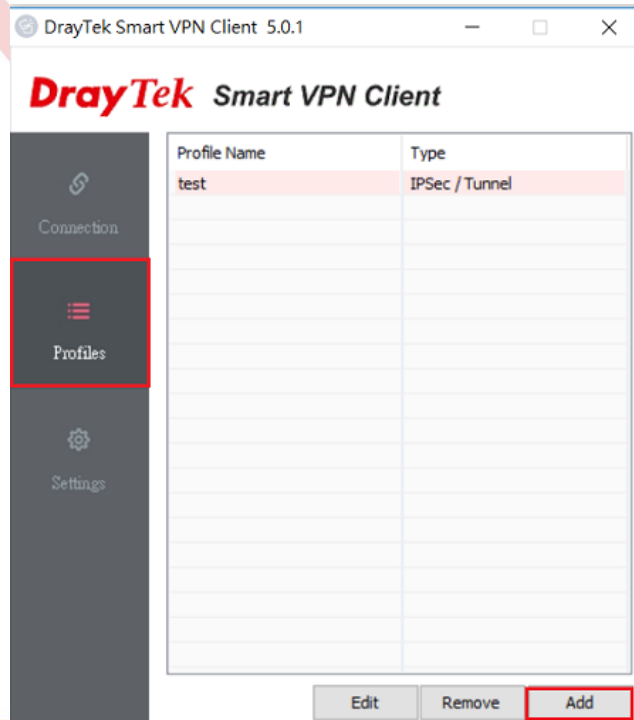
Note:

Username can not contain characters " and '.

OK Clear Cancel

VPN Client Kurulumu

1. VPN Client içinde Smart VPN Client'ı açın ve **Profiles >> Add**'e tıklayın.



Edit Profile
×

a. Profile Name

Server Information

b. Type IPSec Tunnel

c. IP or Hostname 111.108.99.25

Login Information

Authentication Type Username and Password

User Name

Password

Remember My Credentials

Always Prompt for Credentials

IP Property

Standard IPSec Tunnel

d. Remote Subnet 192 . 168 . 2 . 0

Remote Subnet Mask 255 . 255 . 255 . 0

Specify an IP Address on

IP Address 192 . 168 . 1 . 201

Subnet Mask 255 . 255 . 255 . 0

WINS Server . . .

Advanced Options

My IP 192.168.1.10

Mainmode Keyexchange Method

DH Group 1 DH Group 2 DH Group 14

Security Method

Medium(AH) High(ESP)

SHA1 AES256 with SHA1

Authentication Method

e. Pre-shared Key ●●●

Certificate Authentication

Browse

Enable PING to keep alive

Ping to the IP 0.0.0.0

(This IP should exist in the remote subnet!)

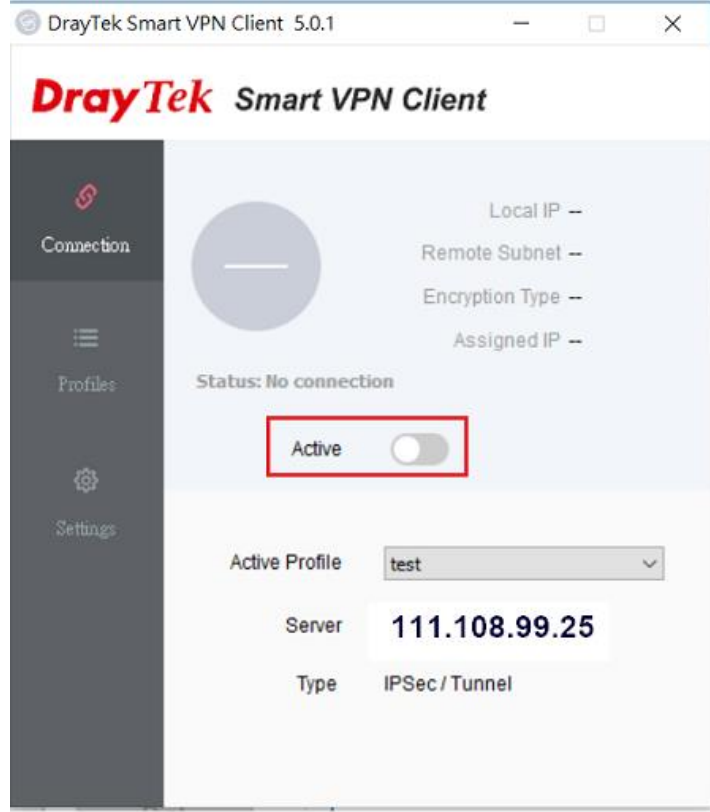
f.

Cancel
OK

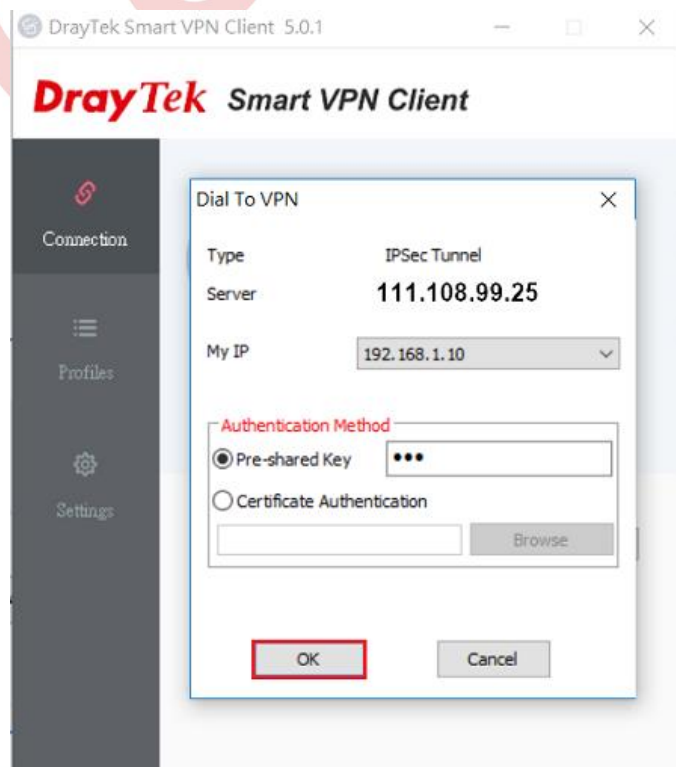
6. VPN profilini oluşturmak için aşağıdaki adımları takip edin.
 - a. **Profile Name** girin.
 - b. Type için **IPsec Tunnel** seçin.
 - c. Server Information bölümünde VPN Server'ın IP (routerın WAN IP adresi) adresini girin.
 - d. IP Property içinde **Remote Subnet** ve **Remote Subnet Mask** için VPN Server'ın LAN subnetini (alt ağını) girin.
 - e. Authentication Method bölümünde **Pre-shared Key** seçin ve 1. adımla aynı Pre-shared Key değerini girin.
 - f. Kaydetmek için **OK**'a tıklayın.

IPsec Bağlantısını Aktif Hale Getirme

7. Yeni oluşturduğumuz Active Profile 'i seçin ve Active seçeneğini açın.



8. Aramayı başlatmak için **OK**'a tıklayın.



9. IPsec ayarları nedeniyle VPN tarafına trafik çekerek IPsec bağlantısını başlatmamız gerekiyor. Yöneticinin LAN IP adresini pinglemek bunu yapmanın basit bir yoludur.

```
C:\Users\Will>ping 192.168.2.1

Ping 192.168.2.1 (使用 32 位元組的資料):
回覆自 192.168.2.1: 位元組=32 時間=243ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間=2ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間=2ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間=2ms TTL=255

192.168.2.1 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 2ms, 最大值 = 243ms, 平均 = 62ms
```

Network yöneticisi **VPN and Remote Access >> Connection Management** sayfasına giderek VPN clientlarını online olarak kontrol edebilir.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh

General Mode:	<input type="text"/>	Dial
Backup Mode:	<input type="text"/>	Dial
Load Balance Mode:	<input type="text"/>	Dial

VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 (Dynamic Client)	IPsec Tunnel AES-SHA1 Auth	via WAN2	192.168.1.10/32	634	455.54	515	40.93	0:0:13 Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.