

## EAP KİMLİK DOĞRULAMA İLE iOS'TAN VIGOR ROUTER'A IKEv2 VPN

DrayOS firmware 3.9.0 versiyonundan beri EAP kimlik doğrulaması ile IKEv2'yi desteklemektedir. Vigor3900 ile Vigor2960 da firmware 1.4.0 versiyonundan beri EAP kimlik doğrulaması ile IKEv2'yi destekliyor. Ek olarak kullanıcı adı/şifre ve sertifika doğrulama ile IKEv2 VPN'i daha güvenli hale getirebilirsiniz. Bu makale server kimlik doğrulaması için self-signed bir sertifika oluşturmayı, Vigor Router'ı bir IKEv2 VPN server kurmayı ve iOS ile bağlantı kurmayı gösterir.

### Vigor Router Kurulumu

#### DrayOS

1. **Certificate Management >> Trust CA Certificate** sayfasına gidin. Ve **Create**'e tıklayın.

Certificate Management >> Trusted CA Certificate

#### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	<b>Create</b>
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

#### Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT

REFRESH

2. Sertifika bilgilerini girin. **Key Size** için "2048 Bit" girin. Sonra **Generate**'e tıklayın.

Certificate Management >> Root CA Certificate

#### Generate Root CA

<b>Certificate Name</b>	Root CA
<b>Subject Alternative Name</b>	
Type	None
<b>Subject Name</b>	
Country (C)	TW
State (ST)	Hsinchu
Location (L)	Hukou
Organization (O)	Draytek
Organization Unit (OU)	Vigor
Common Name (CN)	Root
Email (E)	example@ikev2vpn.net
<b>Key Type</b>	RSA
<b>Key Size</b>	2048 Bit
<b>Algorithm</b>	SHA-256

Generate

3. RootCA'yı indirmek için **Export**'a tıklayın.

## Certificate Management &gt;&gt; Trusted CA Certificate

## X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	/C=TW/ST=Hsinchu/L=Hukou/O=D...	OK	<b>Export</b> View Delete
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

## Note:

- Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
- The Time Zone MUST be setup correctly!!

IMPORT

REFRESH

## 4. Certificate Management &gt;&gt; Local Certificate sayfasına gidin ve Generate'e tıklayın.

- Subject Alternative Name Type için "Domain Name" girin.
- Domain Name ve Common Name(CN) için routerın domainini girin.
- Sertifika için diğer tüm bilgileri doldurun.
- Key Size için "2048 Bit" girin.
- Generate'e tıklayın.

## Generate Certificate Signing Request

Certificate Name	certificate
<b>Subject Alternative Name</b>	
Type	Domain Name
Domain Name	ikev2server.ddns.net
<b>Subject Name</b>	
Country (C)	TW
State (ST)	Hsinchu
Location (L)	Hukou
Organization (O)	Draytek
Organization Unit (OU)	Vigor
Common Name (CN)	ikev2server.ddns.net
Email (E)	example@ikev2vpn.net
Key Type	RSA
Key Size	2048 Bit
Algorithm	SHA-256

Generate

## 5. Sertifikayı oluşturmak için Sign'a tıklayın.

## Certificate Management &gt;&gt; Local Certificate Signing

## Local Certificate Signing

Certificate Name	certificate
<b>Validity</b>	
Not Before	YYYY-MM-DD
Not After	2025 - 9 - 13
Algorithm	SHA-256

Sign

Back

6. Geçerli olan tarihi belirtin sonra **Sign**'a tıklayın.

**Certificate Management >> Local Certificate**

**X509 Local Certificate Configuration**

Name	Subject	Status	Modify	
certificate	/C=TW/ST=Hsinchu/L=Hukou/O=D...	Requesting	<b>Sign</b>	View Delete
---	---	---		View Delete
---	---	---		View Delete

**Note:**

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

GENERATE

IMPORT

REFRESH

7. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin, **Certificate for Dial-in** için önceki adımlarda oluşturulan yerel sertifikayı seçin.

**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 **certificate** ▾

Local ID

Alternative Subject Name First

Subject Name First

**General Pre-Shared Key**

Pre-Shared Key [.....]

Confirm Pre-Shared Key [.....]

**Pre-Shared Key for XAuth User**

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

8. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. Uygun bir index numarasını seçin ve profili aşağıdaki gibi düzenleyin.
- **Allowed Dial-In Type**'de **IKEv2 EAP** seçin.
  - **Username** ve **Password** girin.
  - Kaydetmek için **OK**'a tıklayın.

## VPN and Remote Access &gt;&gt; Remote Dial-in User

Index No. 3

**User account and Authentication**

Enable this account  
Idle Timeout  second(s)

**Allowed Dial-In Type**

PPTP  
 IPsec Tunnel  
 IPsec XAuth  
 L2TP with IPsec Policy   
 SSL Tunnel  
 **IKEv2 EAP**  
 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.)

**Username**   
**Password(Max 19 char)**   
 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)**

## Linux

- Certificate Management >> Trusted CA** 'ya gidin **Build RootCA**'yi tıklayın.
  - Tüm bilgileri girin.
  - Key Size** için "2048" girin.
  - Yerel sertifikayı imzalamak için **Passphrase**'yi (Parolayı) girin.
  - Kaydetmek için **Apply**'a tıklayın.

**Certificate Management >> Trusted CA**

Trusted CA

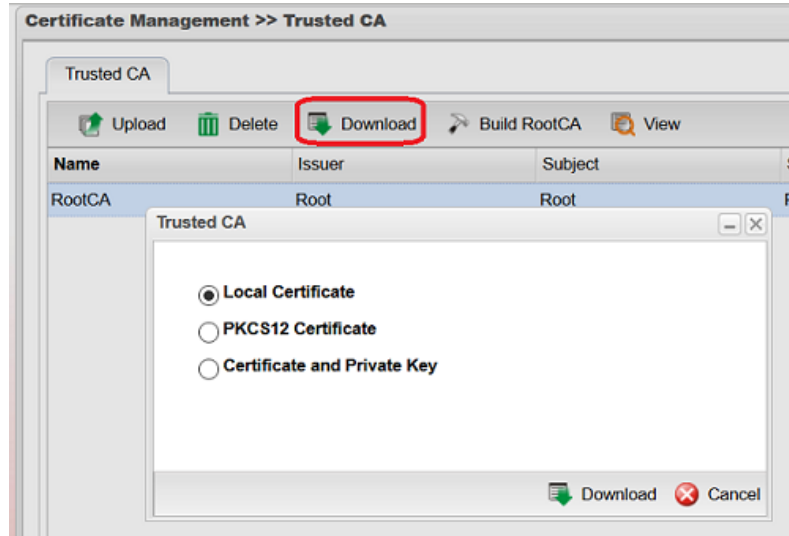
Upload Delete Download **Build RootCA** View

Name	Issuer	Subject
Trusted CA		

**Certificate Name** : RootCA  
**Organization Unit** : Vigor  
**Organization** : Draytek  
**Locality(City)** : Hukou  
**State/Province** : Hsinchu  
**Common Name** : Root  
**Email Address** : example@test.net  
**Key Size** : 2048  
**Country** : TW  
**Passphrase** : .....

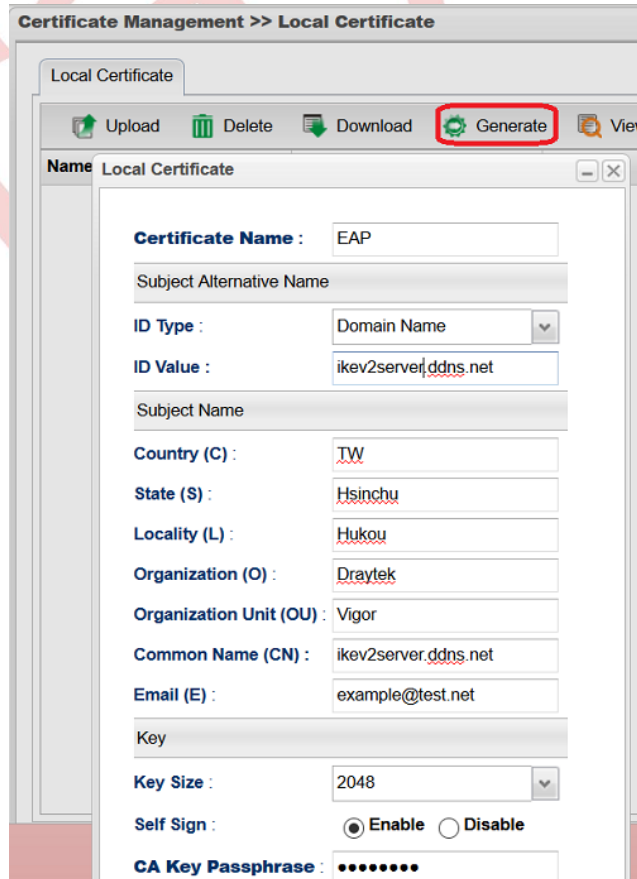
Apply Cancel

2. VPN istemcisine kurulması gereken Root CA'yı dışa aktarmak için **Download**'a tıklayın.



3. **Certificate Management >> Local Certificate** 'e gidin. **Generate** 'e tıklayın.

- **ID Type** için "Domain Name" seçin ve **ID Value** için routerın domainini girin.
- Tüm bilgileri girin.
- **Common Name** için routerın domainini girin.
- **Key Size** için "2048" seçeneğini seçin.
- **Self Sign** için "Enable" seçeneğini seçin.
- **CA Key Passphrase**'de Root CA'nın parolasını girin.
- **Apply**'a tıklayın.

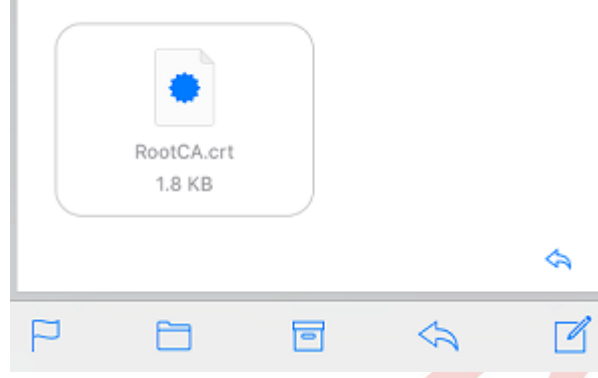


4. Kullanıcı profili eklemek için **User Management >> User Profile**'a gidin.
- **Enable**'yi aktifleştirin.
  - **Username** ve **Password** girin.
  - PPTP/L2TP/SSL/OpenVPN Server'da Xauth/EAP için "Enable" seçin.

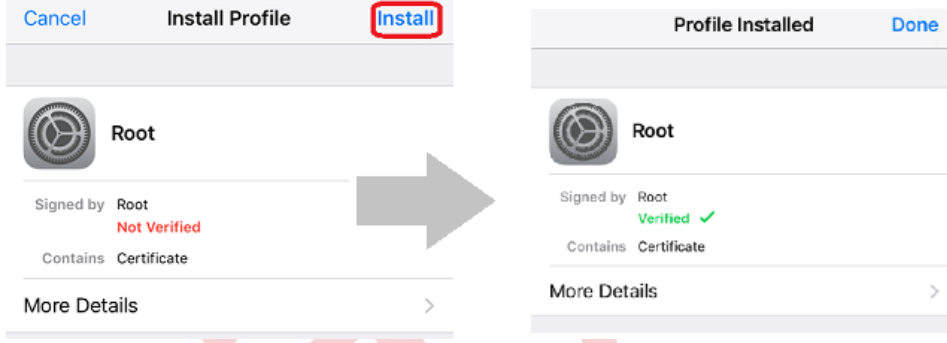
5. Profil eklemek için **VPN and Remote Access >> VPN Profiles >> IPsec**'e gidin.
- **Profil adı** girin ve **Enable**'yi aktifleştirin.
  - **Remote Dial-In User** için "Enable" seçeneğini seçin.
  - **Local IP / Subnet Mask** için routerın LAN ağını girin.
  - **IKE Protocol** için "IKEv2" seçeneğini seçin.
  - **Auth Type** için "RSA" seçin ve Local Certificate için önceki adımlarda oluşturulan sertifikayı seçin.

## iOS'tan Bağlantı

1. Router'dan indirilen RootCA dosyasını iOS cihazına gönderin.

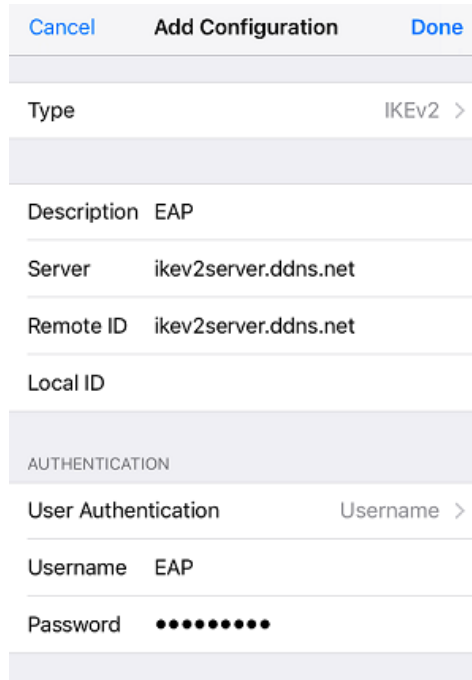


2. Dosyayı açarak CA'yı iOS cihazına CA'yı yükleyin ve **Install**'a tıklayın. RootCA'nın doğrulandığından emin olduktan sonra **Done**'a tıklayın.

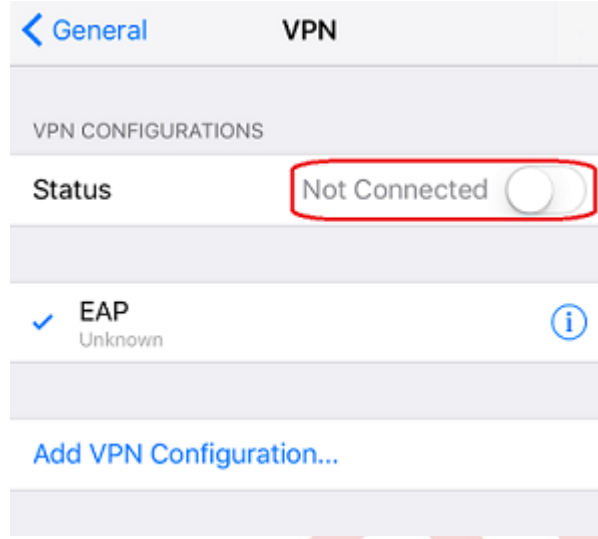


3. **General** >> **VPN** 'e gidin ve konfigürasyonu ekleyin.

- **Type** için "IKEv2" seçin.
- **Server** ve **Remote ID** için routerın domainini girin.
- **Username** ve **Password** girin.



4. VPN bağlantısını açarak VPN'i başlatın.



5. Başarılı bir şekilde bağlanırsa VPN durumu aşağıdaki gibi görünür.

