

## LET'S ENCRYPT KULLANARAK WINDOWS'TAN VIGOR ROUTER'A EAP KİMLİK DOĞRULAMA İLE IKEv2 VPN

DrayOS firmware 3.9.0 versiyonundan bu yana Let's Encrypt sertifika fonksiyonu oluşturmayı desteklemektedir. Bildiğimiz gibi Let's Encrypt tarafından imzalanan sertifika geçerli bir sertifika olduğundan Vigor Router'da Let's Encrypt sertifikasını kullanmak farklı VPN clientları için VPN konfigürasyonunu basitleştirebilir, özellikle EAP kimlik doğruma VPN ile IKEv2 VPN kullanırken faydalıdır. Bu makalede Vigor Router'ın Let's Encrypt sertifikasını kullanılarak nasıl IKEv2 VPN sunucusu olarak kurulacağı ve iOS ile nasıl bağlantı kurulacağı gösterilmektedir.

### Vigor Router Kurulumu

1. Doğru saat dilimini seçin ve routera sistem saatinin doğru olduğundan emin olun.

System Maintenance >> Time and Date

---

**Time Information**

Current System Time	2019 Mar 12 Tue 9 : 55 : 51	Inquire Time
---------------------	-----------------------------	--------------

**Time Setup**

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT+08:00) Taipei
Enable Daylight Saving	<input type="checkbox"/> Advanced
Automatically Update Interval	30 mins
Send NTP Request Through	Auto

OK Cancel

2. Vigor Router'da **DrayDDNS** servisini **etkinleştirin**.
3. DrayDDNS için **Let's Encrypt** sertifikasını **uygulayın**.
4. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin. **DrayDDNS**'i ( Dial-in sertifikası olarak Let's Encrypt sertifikasını uygulamak için kullanılan Domain) seçin.

### VPN IKE/IPsec General Setup

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

<b>IKE Authentication Method</b>	
Certificate for Dial-in	DrayDDNS
<b>General Pre-Shared Key</b>	
Pre-Shared Key	.....
Confirm Pre-Shared Key	
<b>Pre-Shared Key for XAuth User</b>	
Pre-Shared Key	Max: 64 characters
Confirm Pre-Shared Key	
<b>IPsec Security Method</b>	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authenticated, but will not be encrypted.
High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	Data will be encrypted and authenticated.

5. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. Uygun bir index'i tıklayın ve aşağıdaki adımları takip ederek ayarlamaları yapın.
  - a. Account'u ve **IKEv2 EAP**'ı etkinleştirin.
  - b. **Username** ve **Password**'u girin
  - c. **Digital Signature(X.509)** seçin.
  - d. OK'a tıklayın.

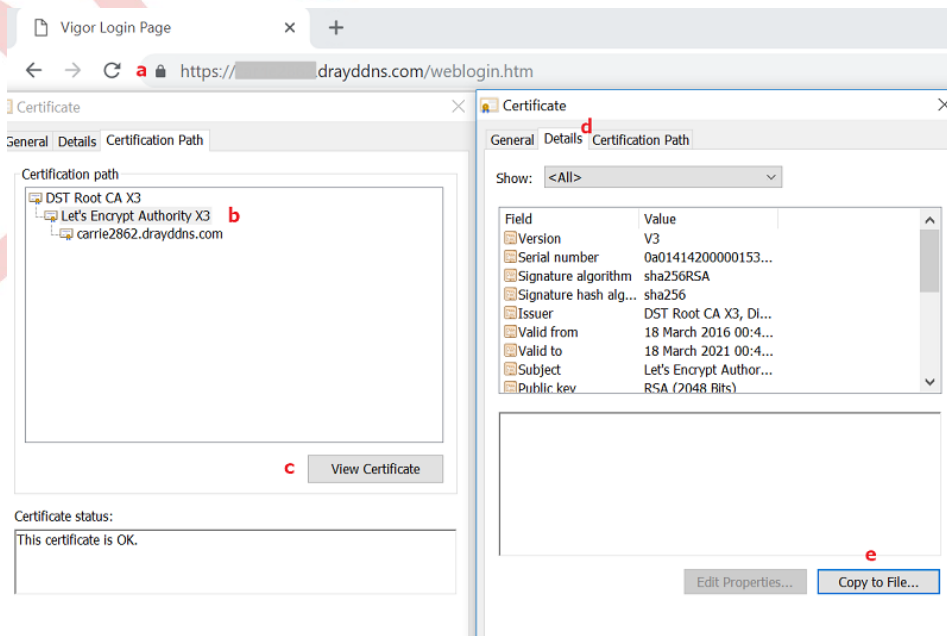
Index No. 1

<b>User account and Authentication</b> <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="0"/> second(s)	Username <input type="text" value="eap"/> Password <input type="password" value="*****"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
<b>Allowed Dial-In Type</b> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> IPsec XAuth <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> SSL Tunnel <input checked="" type="checkbox"/> OpenVPN Tunnel <input checked="" type="checkbox"/> <b>IKEv2 EAP</b> <input type="checkbox"/> Specify Remote Node	<b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value=""/> Max: 64 characters <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
	<b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AH)

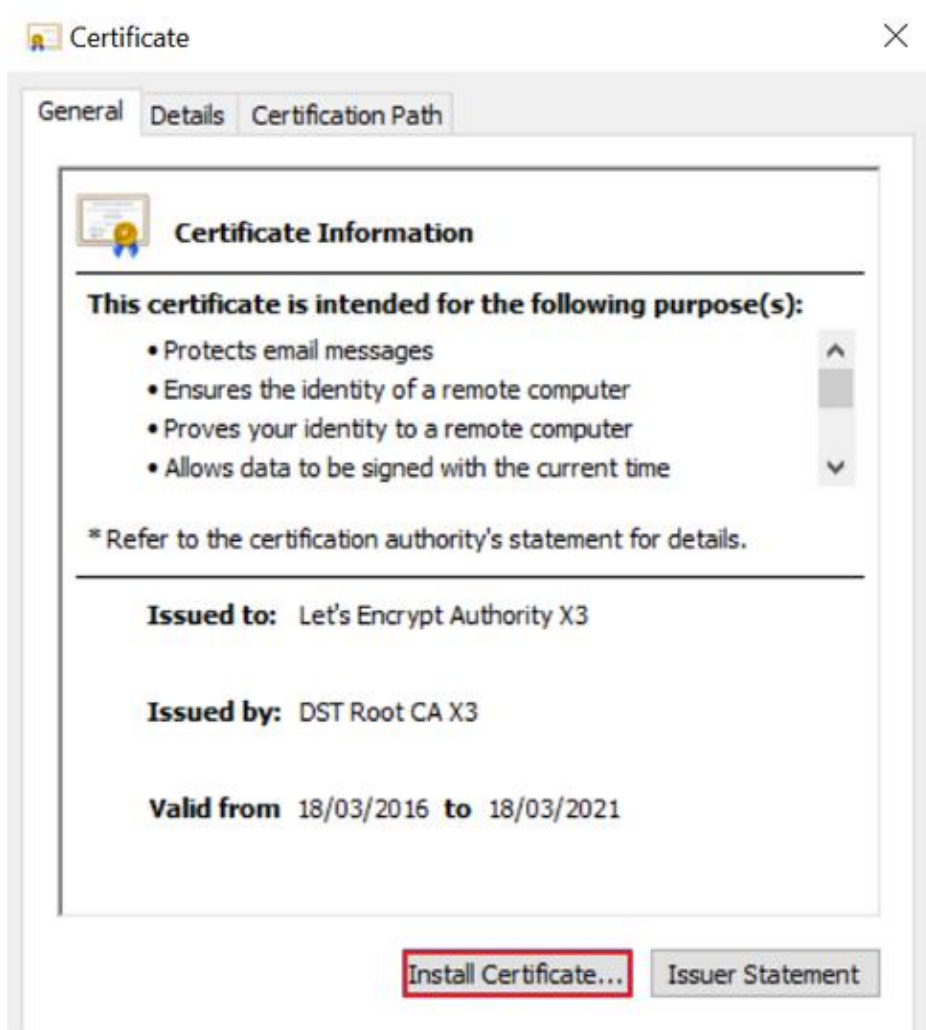
### Windows 10'dan Bağlanma

Windows 10, VPN sunucusunun tüm sertifika zincirini doğrulamasını gerektiriyor ancak Vigor Router intermediate sertifikayı mevcut firmware versiyonu 3.9.0 ile gönderirken bir sorun yaşıyor. Bu nedenle intermediate sertifikayı geçici olarak manuel indirip kurmanız gerekiyor. Gelecek yazılım versiyonunda 1 ile 5 arasındaki adımları atlayabiliriz.

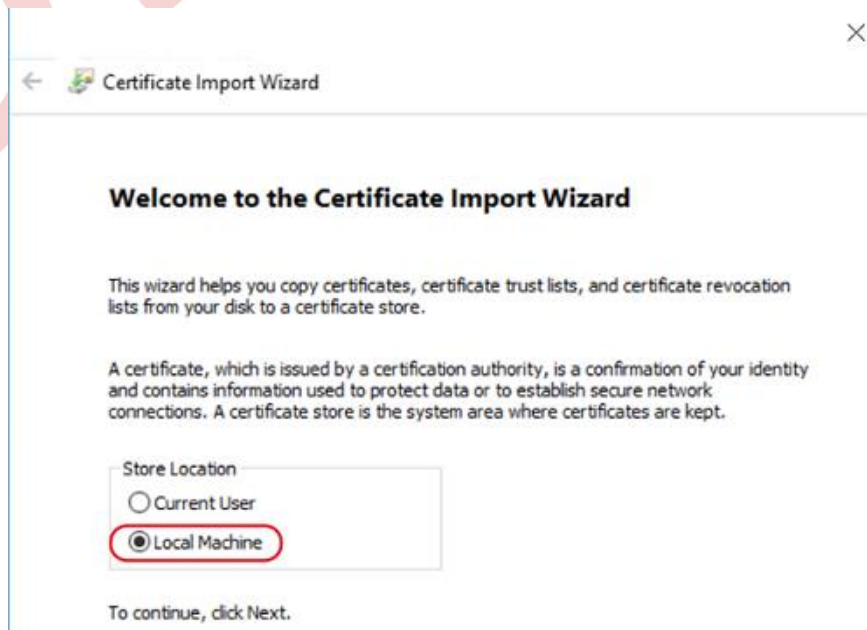
1. Aşağıdaki yöntemlerden biriyle **Let's Encrypt X3 sertifikasını indirin**.
  - a. **Let's Encrypt Authority X3'ü (IdenTrust cross-signed)** <https://letsencrypt.org/certificates/> adresinden indirin ve dosyayı bilgisayarınızda .pem veya .crt dosyası olarak kaydedin.
  - b. Vigor Routerınıza https ile göz atın ve sertifika bilgilerini görüntüleyip dosyaya kopyalayarak Let's Encrypt Authority X3 sertifikasını verin.



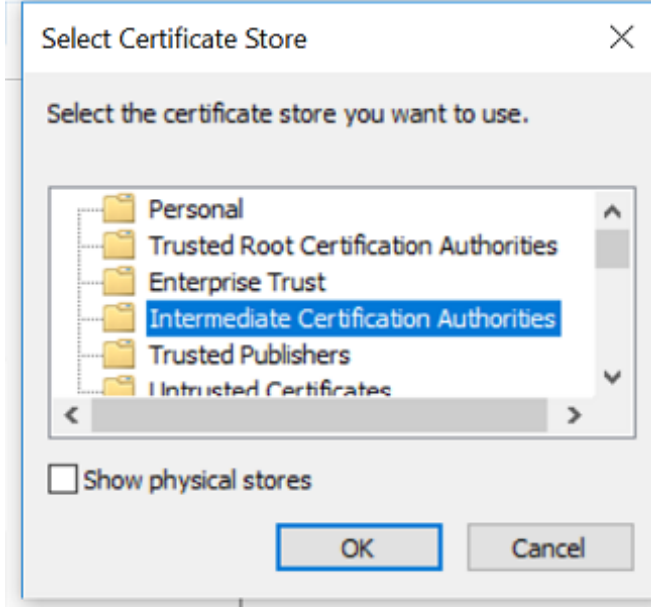
- İndirilen sertifika dosyasına çift tıklayın ve sertifikayı **kurun**.



- Sertifika eklemek için Certificate Import Wizard adımlarını takip edin. İlk olarak **Local Machine** seçin ve **Next**'e tıklayın.



4. Certificate Store'da olduđu gibi **Intermediate Certification Authorities**'i seřin ve **OK**'a tıklayın



5. Ekleme işlemi başarılıdır.

### Certificate Import Wizard



The import was successful.

OK

6. **Network and Internet Settings** >> **VPN**'e gidin ve **Add a VPN connectiona** tıklayın.
- VPN provider için **Window (built-in)** seřin.
  - **Server adı** ya da adres için routerın domainini girin.
  - VPN türü olarak **IKEv2** seřin.
  - **User name** ve **Password** girin.
  - **Remember my sign-in info** seřimini kaldırın.
  - **Save** 'e tıklayın.

## Add a VPN connection

VPN provider  
Windows (built-in) ▾

Connection name  
ToVigor2862

Server name or address  
[redacted].drayddns.com

VPN type  
IKEv2 ▾

Type of sign-in info  
Username and password ▾

Username (optional)  
eap

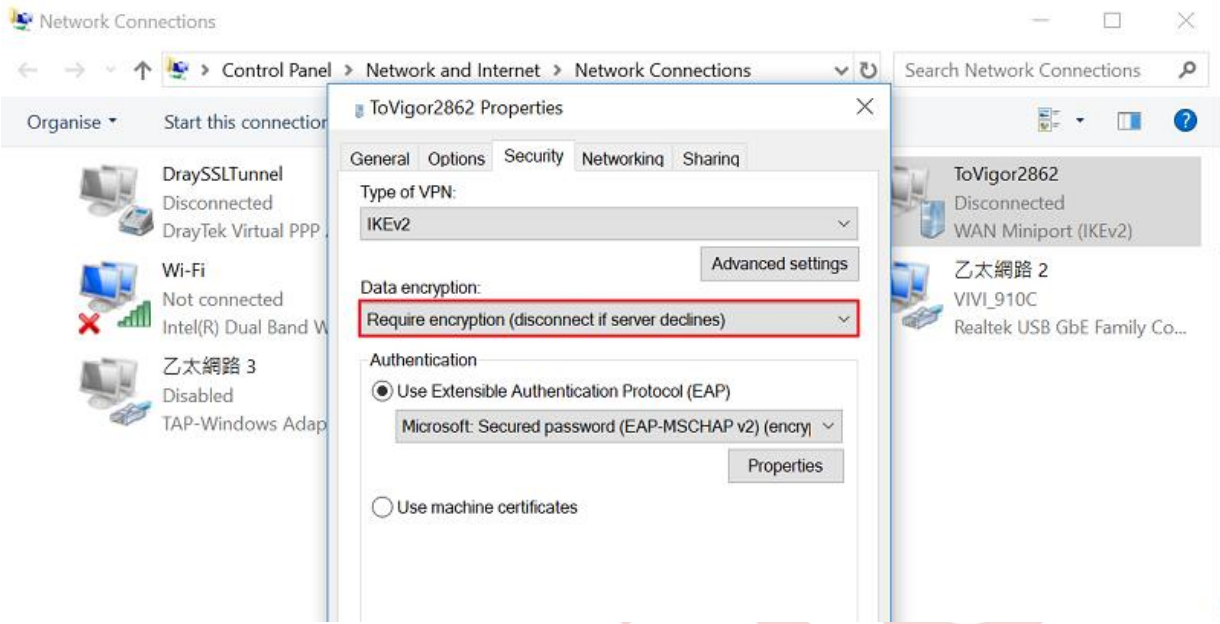
Password (optional)  
●●●●●●

Remember my sign-in info

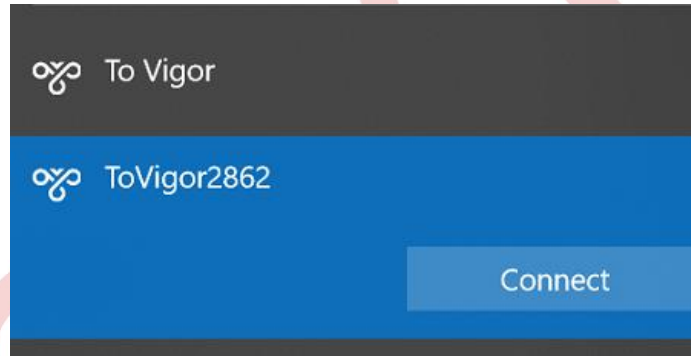
Save

1. **Network and Sharing Centre >> Change adapter settings** 'e gidin. Yeni oluşturduğunuz **VPN** profilini seçin, fareye sağ tıklayın ve **Properties** 'i seçin. Security sekmesinde veri şifreleme için **Require Encryption if Server declines (Sunucu reddederse şifreleme gerektir)** 'i seçin ve değişiklikleri kaydetmek için **OK**'a tıklayın.

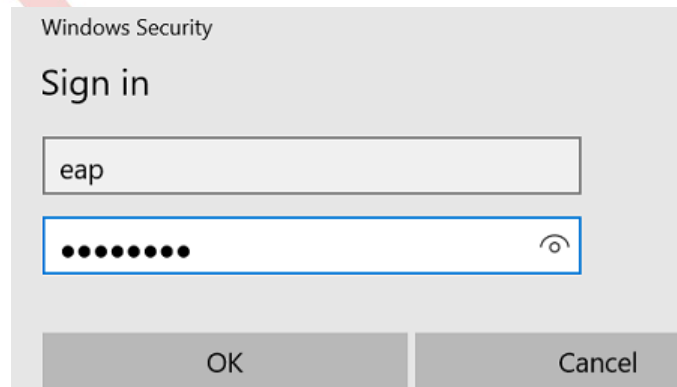




1. VPN profiline çift tıklayın ve VPN bağlantısı kurmak için **Connect**'e tıklayın.



2. Windows, kimlik doğrulama penceresini açacaktır ve bu nedenle VPN bağlantısını başarıyla oluşturmak için şifreyi iki kez girmemiz gerekiyor.



3. Sonra VPN bağlantısının başarılı bir şekilde gerçekleştiğini görebiliriz.

