

## SSL VPN İÇİN SERVER KİMLİK DOĞRULAMASINI ETKİNLEŞTİRME

Server kimlik doğrulaması istemcinin istediği sunucuya bağlanmasını sağlayarak SSL istemcilerini man-in-the-middle (ortadaki adam) saldırısından koruyabilir. SSL VPN ağ geçidi olarak, Vigor Router, SSL bağlantısı için gereken sunucu sertifikaları vermek için Root Certificate Authority (CA)'da oluşturabilir. Ayrıca Root CA'yı dışa aktarabilir ve sertifikanın orijinalliğini doğrulayabilmeleri için istemci cihazlardaki güvenilir CA listesini alabilirsiniz. Bu makale, SSL VPN için nasıl bir server sertifikası oluşturulacağını, Root CA'nın iOS'a nasıl alınacağını ve Root CA'nın Android telefonlara nasıl alınacağını içerir.

### DrayOS

#### Local Sertifika Oluşturma

1. Router'ın zaman ayarlarının doğru olduğundan emin olmak için **System Maintenance >> Time and Date** sayfasına gidin ve istemcinin zaman dilimi ile eşleştirilmesi daha iyidir. Çünkü serverın kimliğini doğrularken, istemci, geçerli saat ve tarihin server sertifikasının geçerlilik süresi içinde olup olmadığını kontrol eder.

#### System Maintenance >> Time and Date

##### Time Information

Current System Time	2015 Dec 7 Mon 11 : 6 : 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 min

OK Cancel

2. **Certificate Management >> Trusted CA Certificate** sayfasına gidin. **Create Root CA**'ya tıklayın.

#### Certificate Management >> Trusted CA Certificate

##### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create Root CA
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

3. Aşağıdaki bilgileri tamamlayın:

- **Subject Alternative Name** için "None" türünü seçin.
- Konum, organizasyon, ad ve E-mail dahil olmak üzere içeriği doldurun.
- Daha güçlü güvenlik için **Key Size**'ı "2048 Bit" olarak seçin.
- Root CA'yı oluşturmak için **Generate** 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)	Taiwan
Location (L)	Hsinchu
Organization (O)	DrayTek
Organization Unit (OU)	FAE
Common Name (CN)	Root CA
Email (E)	support@draytek.com
<b>Key Type</b>	RSA ▼
<b>Key Size</b>	2048 Bit ▼

Generate

4. Root CA'nın oluşturulması birkaç dakika sürecektir. Durumda **OK** görünene kadar bekleyin.

Certificate Management >> Trusted CA Certificate

#### X509 Trusted CA Certificate Configuration

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

5. Ardından bir Local Sertifika oluşturun. Bu routerın SSL VPN istemcilerine göndereceği sertifikadır. **Certificate Management >> Local Certificate** sayfasına gidin. **Generate**'e tıklayın.

Certificate Management >> Local Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	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

6. Aşağıdaki alanları doğru bilgilerle doldurun:

- **Certificate Name** girin.
- **Subject Alternative Name** için VPN istemcilerinin routera nasıl erişeceği türünü seçin. Örneğin IP adresini seçiyoruz.
- **IP Address** için routerın WAN IP'sini girin. VPN istemcilerinin Server ayarları için kullandıkları IP adresi olmalıdır.
- Konum, organizasyon, Ortak Ad (CN) ve E-mail adresinizi girin. CN, Subject Alternative Name ile aynı olmalıdır. Bu yüzden IP adresini buraya koyalım.
- Daha güçlü güvenlik için **Key Size**'ı "2048 Bit" olarak ayarlayın.
- Local Sertifika oluşturmak için **Generate**'e tıklayın.

Certificate Management >> Local Certificate

#### Generate Certificate Signing Request

Certificate Name	Local Certificate
<b>Subject Alternative Name</b>	
Type	IP Address ▼
IP	118.86.192.242
<b>Subject Name</b>	
Country (C)	TW
State (ST)	Taiwan
Location (L)	Hsinchu
Organization (O)	DrayTek
Organization Unit (OU)	FAE
Common Name (CN)	118.86.192.242
Email (E)	support@draytek.com
Key Type	RSA ▼
Key Size	2048 Bit ▼

Generate

7. İmzalama isteği hazır olana kadar birkaç dakika bekleyin. Ardından Root CA ile sertifikayı imzalamak için **Sign**'a tıklayın.

Certificate Management >> Local Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local Certificate	/C=TW/ST=Taiwan/L=Hsinchu/O=...	Requesting	<b>Sign</b> View Delete
---	---	---	View Delete
---	---	---	View Delete

8. Local sertifikanın bitiş tarihini girin ve **Sign**'a tıklayın.

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

## Local Certificate Signing

Certificate Name	Test
Validity	YYYY-MM-DD
Not Before	2016-01-28
Not After	2025 - 1 - 28

Sign Back

1. Local Sertifikanın durumunun OK olduğundan emin olun.

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

## X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local Certificate	/C=TW/ST=Taiwan/L=Hsinchu/O=...	OK	View Delete
---	---	---	View Delete
---	---	---	View Delete

2. Artık sertifikayı SSL VPN olarak kullanabiliriz. **SSL VPN >> General Setup** sayfasına gidin. **Server Certificate** için önceki adımlarda oluşturulan sertifikayı seçin. Ayarları kaydetmek için **OK**'a tıklayın.

## SSL VPN &gt;&gt; General Setup

## SSL VPN General Setup

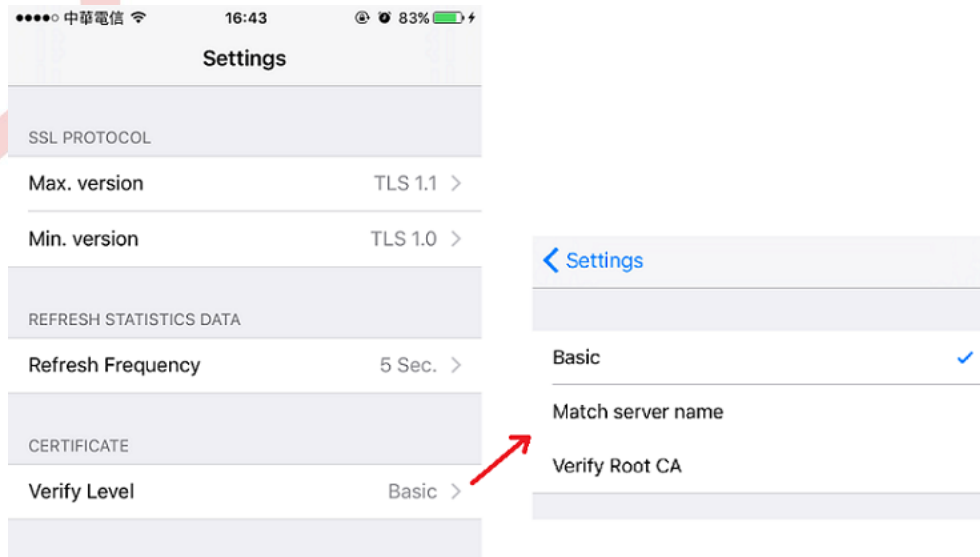
Port	443	(Default: 443)
Server Certificate	Test	

Note: The settings will act on all SSL applications.

Please go to **System Maintenance >> Management** to enable SSLv3.0 .

OK Cancel

3. Şimdi VPN istemcileri, doğrulama için "Match Server Name" kullanabilir. Başka bir deyişle, SSL bağlantısı kurarken serverın sertifikasındaki domain adı veya IP adresinin, domain adı veya bağlandığı IP adresiyle eşleşip eşleşmediğini kontrol eder.



## Root CA'yı iSO'a Verme

1. Root CA'yı Certificate Management >> Trusted CA Certificate sayfasında oluşturduktan sonra Root CA'yı indirmek için **Export**'a tıklayın. Ardından e-mail ile istemci cihaza gönderin.

Certificate Management >> Trusted CA Certificate

### X509 Trusted CA Certificate Configuration

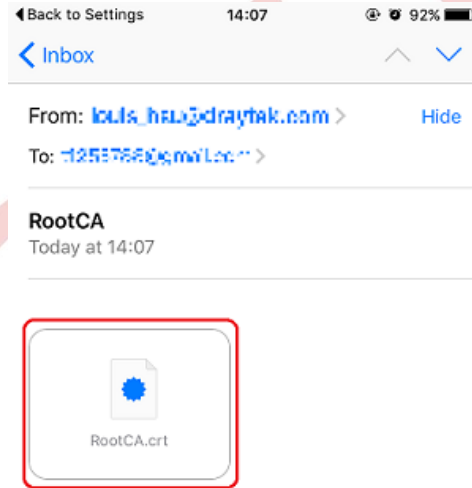
Name	Subject	Status	Modify
Root CA	/C=TW/ST=Taiwan/L=Hsinchu/O=...	OK	<b>Export</b> View Delete
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

#### 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

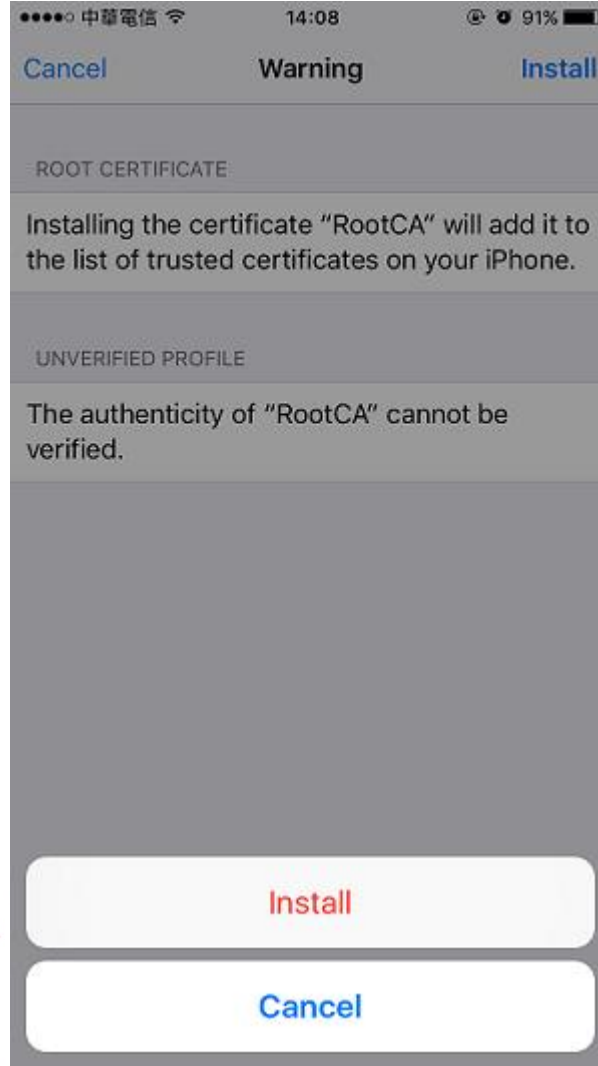
2. İstemci cihazda, .cret dosyasını açın.



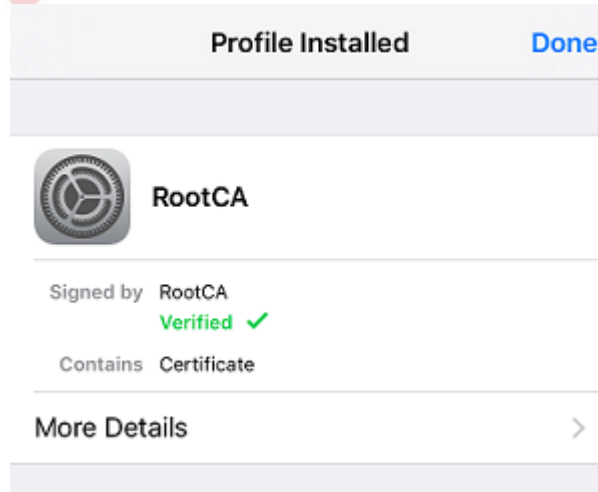
3. Kurulumu başlatmak için **Install**'a dokunun ardından şifreyi girin.



4. Uyarı mesajını okuyun ardından **Install**'a dokununuz.



5. Kurulum tamamlandıktan sonra Root CA'nın doğrulanmış olduğunu göreceksiniz.



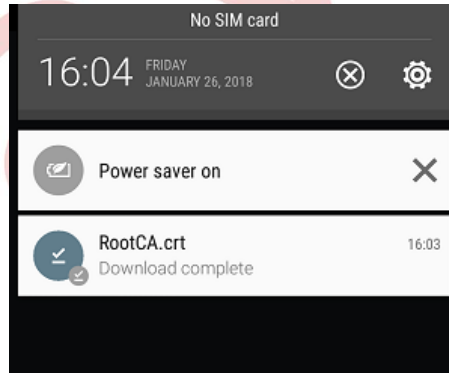
6. İstemci cihazda **General** >> **About** >> **Certificate Trust Settings**'e gidin. Yüklenen Root CA'yı etkinleştirin.



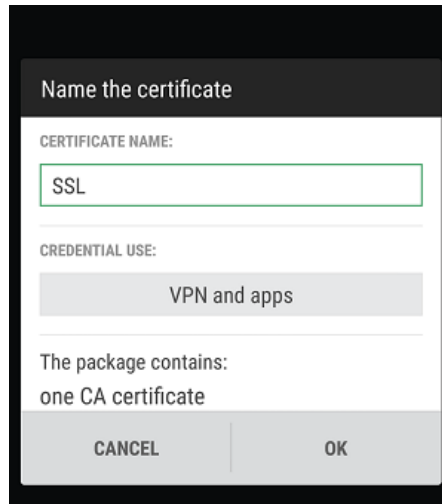
7. Şimdi sertifika doğrulama ayarları için Verify Root CA'yı kullanabiliriz. Yani SSL anlaşması sırasında, cihaz sadece server sertifikasını kontrol etmekte kalmayacak aynı zamanda sertifikayı veren sertifikayı da doğrulayacaktır. VPN yalnızca server güvenilir, Root CA tarafından imzalanmış bir sertifika sunarsa bağlantı kurar .

### Root CA'yı Cihazlara Aktarma

1. Root CA'yı indir.

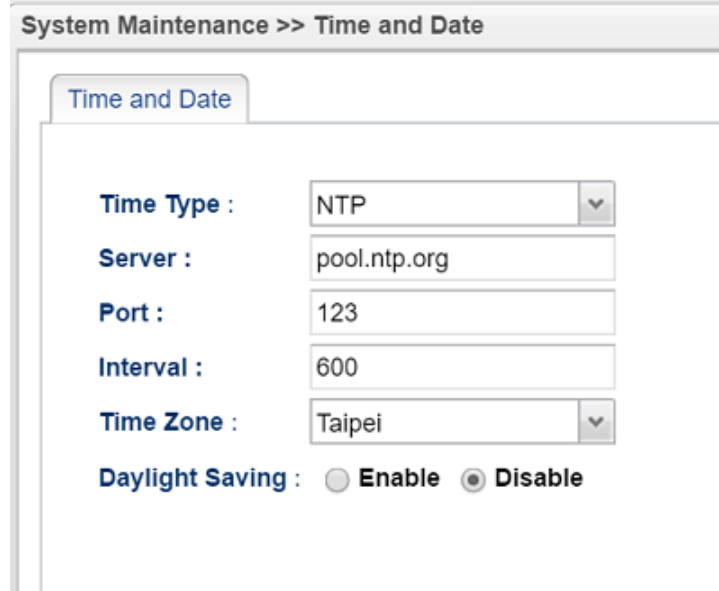


2. .crt dosyasını açın. VPN ve uygulamalar için kullanın. Ardından **OK**'a dokununuz.



## Linux

1. Router'ın zaman ayarlarının doğru olduğundan emin olmak için **System Maintenance >> Time and Date** sayfasına gidin ve istemcinin zaman dilimi ile eşleştirilmesi daha iyidir. Çünkü serverın kimliğini doğrularken, istemci, geçerli saat ve tarihin server sertifikasının geçerlilik süresi içinde olup olmadığını kontrol eder.



System Maintenance >> Time and Date

Time and Date

Time Type : NTP

Server : pool.ntp.org

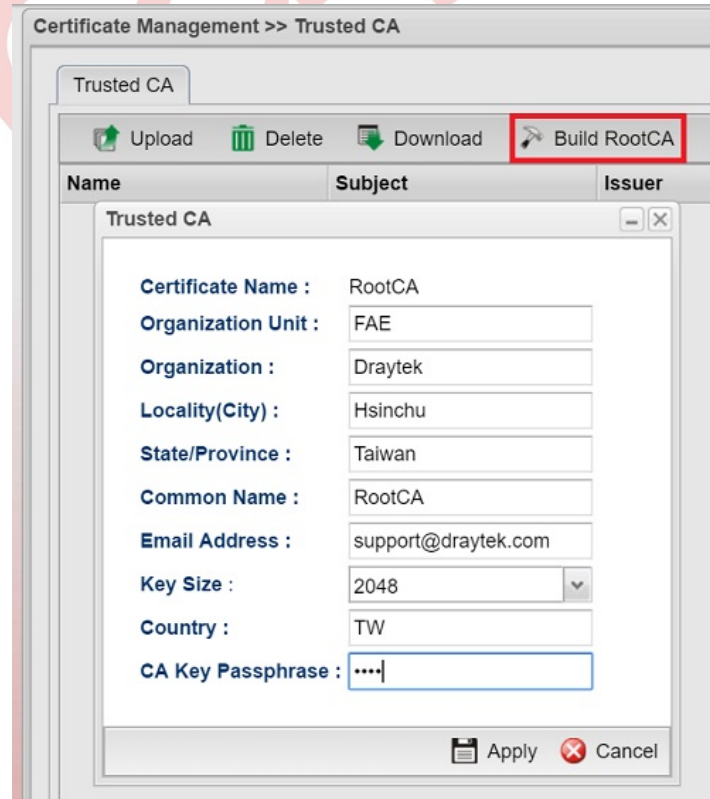
Port : 123

Interval : 600

Time Zone : Taipei

Daylight Saving :  Enable  Disable

2. **Certificate Management >> Trusted CA**'ya gidin ve **Root CA** oluşturun.
  - Tüm bilgileri doldurun.
  - Daha güçlü güvenlik için **Key Size**'ı "2048 Bit" olarak seçin.
  - Bir **CA Key Passphrase** ( CA Anahtarı Şifresi) girin.
  - Ayarları bitirmek için **Apply**'a tıklayın.



Certificate Management >> Trusted CA

Trusted CA

Upload Delete Download Build RootCA

Name	Subject	Issuer
Trusted CA		

Trusted CA

Certificate Name : RootCA

Organization Unit : FAE

Organization : Draytek

Locality(City) : Hsinchu

State/Province : Taiwan

Common Name : RootCA

Email Address : support@draytek.com

Key Size : 2048

Country : TW

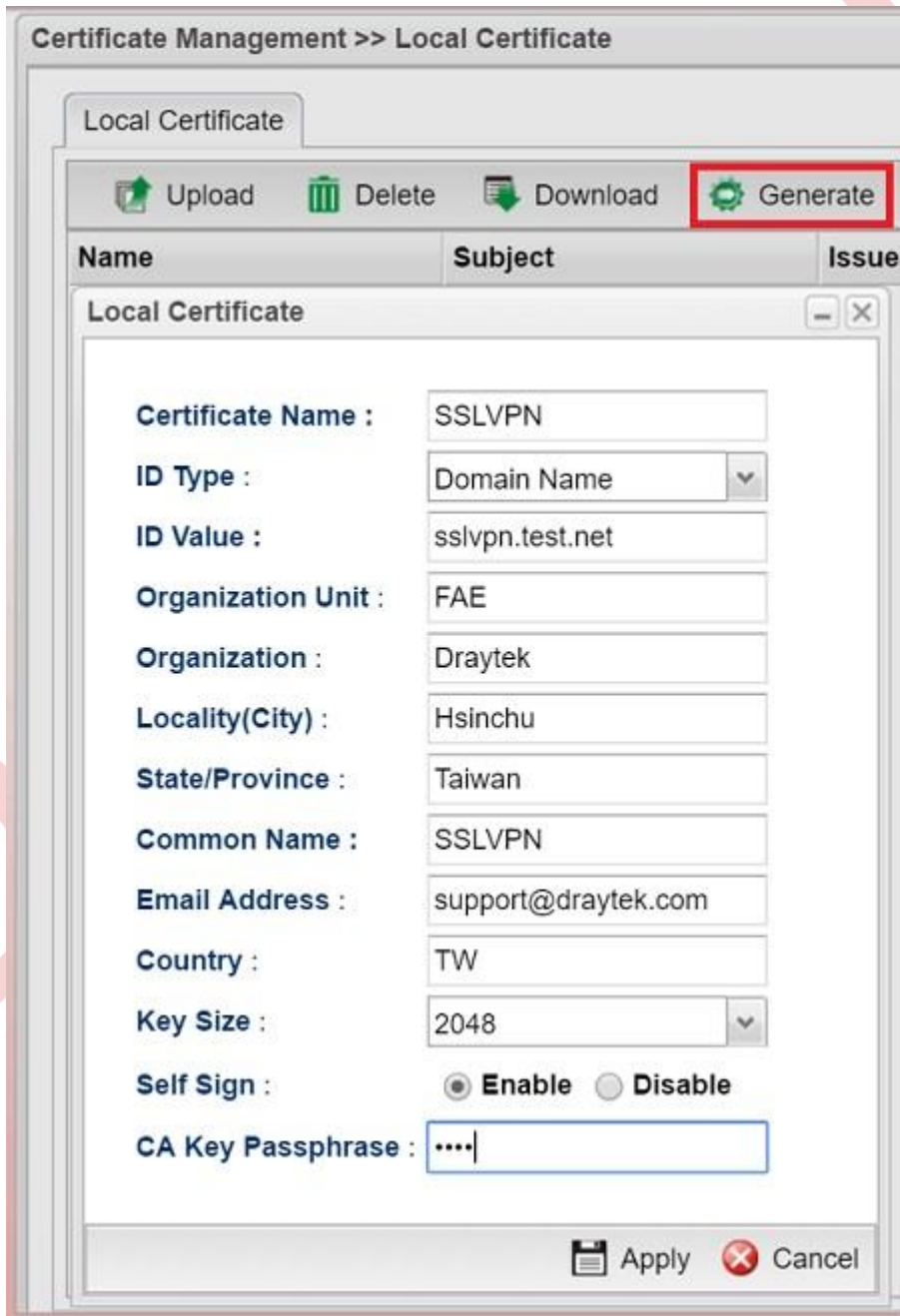
CA Key Passphrase : .....

Apply Cancel



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

- Domain adı veya IP adresi olarak **ID Type**'i seçin. Hangisinin VPN istemcisinin servera bağlanmak için kullanacağına göre değişir.
- Routerın domain adı veya IP adresi olarak **ID Value** türünü girin. VPN istemcilerinin server ayarlarında kullandıkları domain adı veya IP adresi olmalıdır.
- Tüm bilgileri doldurun.
- **Self Sign** için "Enable" seçin.
- Root CA'nın CA Key Passphrase ile eşleşmesi için **CA Key Passphrase** girin.
- Bitirmek için **Apply**'a tıklayın.



Certificate Management >> Local Certificate

Local Certificate

Upload Delete Download **Generate**

Name	Subject	Issuer
Local Certificate		

Local Certificate

Certificate Name : SSLVPN

ID Type : Domain Name

ID Value : sslvpn.test.net

Organization Unit : FAE

Organization : Draytek

Locality(City) : Hsinchu

State/Province : Taiwan

Common Name : SSLVPN

Email Address : support@draytek.com

Country : TW

Key Size : 2048

Self Sign :  Enable  Disable

CA Key Passphrase : ....

Apply Cancel

4. **System Maintenance >> Access Control >> Access Control**'e gidin ve Server Sertifikası için oluşturulan local sertifikayı seçin. Kaydetmek için **Apply**'a tıklayın.

System Maintenance >> Access Control >> Access Control

Access Control | Fail to Ban | Access Barrier

Internet Access Control

Apply to WAN Interface : wan1, wan2, wan... X

Web Allow :  Enable  Disable

Telnet Allow :  Enable  Disable

SSH Allow :  Enable  Disable

HTTPS Allow :  Enable  Disable

FTP Allow :  Enable  Disable

SAMBA Allow :  Enable  Disable

Server Certificate : SSLVPN

Access List : Default, SSLVPN

Add Save Profile Name

IP	Subnet Mask
No items to show.	

IP List :

Allow Ping from the WAN :  Enable  Disable

- Şimdi VPN istemcileri, doğrulama için "Match Server Name" kullanabilir. Başka bir deyişle, SSL bağlantısı kurarken serverın sertifikasındaki domain adı veya IP adresinin, domain adı veya bağlandığı IP adresiyle eşleşip eşleşmediğini kontrol eder.

Settings

SSL PROTOCOL

Max. version TLS 1.1 >

Min. version TLS 1.0 >

REFRESH STATISTICS DATA

Refresh Frequency 5 Sec. >

CERTIFICATE

Verify Level Basic >

Settings

Basic ✓

Match server name

Verify Root CA