

Router Üzerinde Benzersiz Bir Kendinden İmzalı Sertifika Kullanın

Güvenlik endişeleri nedeniyle, kendinden imzalı SSL için her cihazda benzersiz bir özel anahtar bulundurmanız şiddetle önerilir. Bu makale, kendinden imzalı benzersiz bir sertifikanın nasıl üretileceğini ve ardından VigorRouter'da varsayılan olanın nasıl değiştirildiğini gösterir.

Root CA Oluştur

1. Router'ın zaman ayarlarının doğru olduğundan emin olun. İstemci tarafına uygun zaman ayarlarını kullanmanızı şiddetle öneririz.

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'e gidin ve 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

3. Root CA'nın konularını girin ve Generate'ye tıklayın.

Certificate Management >> Root CA Certificate

Generate Root CA

Certificate Name	Root CA
Subject Alternative Name	
Type	IP Address ▼
IP	<input type="text"/>
Subject Name	
Country (C)	TW
State (ST)	Hsinchu
Location (L)	Hsinchu
Organization (O)	DrayTek
Organization Unit (OU)	FAE
Common Name (CN)	CAServer
Email (E)	support@draytek.com
Key Type	RSA ▼
Key Size	2048 Bit ▼

Generate

4. RootCA "OK" durumuyla gösterilecektir. (Not: Bir Router yalnızca bir Root CA'ya sahip olabilir. Yeni bir Root CA oluşturmak için önce eskisini silmeniz gerekir.)

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

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

Root CA ile Local Sertifika İmzalayın

5. Certificate Management >> Local Certificate'e gidin ve bir sertifika isteği oluşturun.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="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!!

6. Yerel sertifikanın konularını girin ve Generate düğmesine tıklayın.

Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	<input type="text" value="Server"/>
Subject Alternative Name	
Type	<input type="text" value="IP Address"/>
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text" value="TW"/>
State (ST)	<input type="text" value="Hsinchu"/>
Location (L)	<input type="text" value="Hsinchu"/>
Organization (O)	<input type="text" value="DrayTek"/>
Organization Unit (OU)	<input type="text" value="FAE"/>
Common Name (CN)	<input type="text" value="Server"/>
Email (E)	<input type="text" value="support@draytek.com"/>
Key Type	<input type="text" value="RSA"/>
Key Size	<input type="text" value="2048 Bit"/>

7. Listede durum Requesting(Talep) olan yeni bir yerel sertifika talebi olacak. Yerel sertifikayı imzalamak için Sign'e tıklayın.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	Sign View Delete
---	---	---	View Delete
---	---	---	View Delete

8. Geçerlilik tarihini ayarlayın ve Sign'e tıklayın.

Certificate Management >> Local Certificate Signing

Local Certificate Signing

Certificate Name	Server
Validity	YYYY-MM-DD
Not Before	2015-12-07
Not After	2020 - 12 - 7

Sign Back

9. Yerel sertifika durumu "OK" olarak değişecektir.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	OK	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

Varsayılan Sertifikayı Değiştir

10. SSL >> General Setup'a gidin ve Server Certificate için 6. adımda oluşturulan yeni sertifikayı seçin.

SSL VPN >> General Setup

SSL VPN General Setup

Port	443	(Default: 443)
Server Certificate	Server	self-signed

Note: The settings will act on all SSL applications.

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

OK Cancel

11. Tarayıcıdan, sertifikanın ayarladığımızda değiştiğini görmeliyiz. Şimdi Router benzersiz bir kendinden imzalı sertifika kullanıyor.

