

DrayTek

HTTPS Certificaat
Let's Encrypt



Inhoudsopgave

- Let's Encrypt 3
- Let's Encrypt vereisten 4
- Let's Encrypt certificaat aanvragen 5
- Let's Encrypt certificaat controle 7
- Auto Update Let's Encrypt 9

Let's Encrypt

Let's Encrypt is een dienstverlener die gratis certificaten uitgeeft. Door gebruik te maken van een geldig certificaat in de router, worden geen certificaat fouten weergegeven wanneer de router benaderd wordt op het DNS adres waarvoor het certificaat is afgegeven.

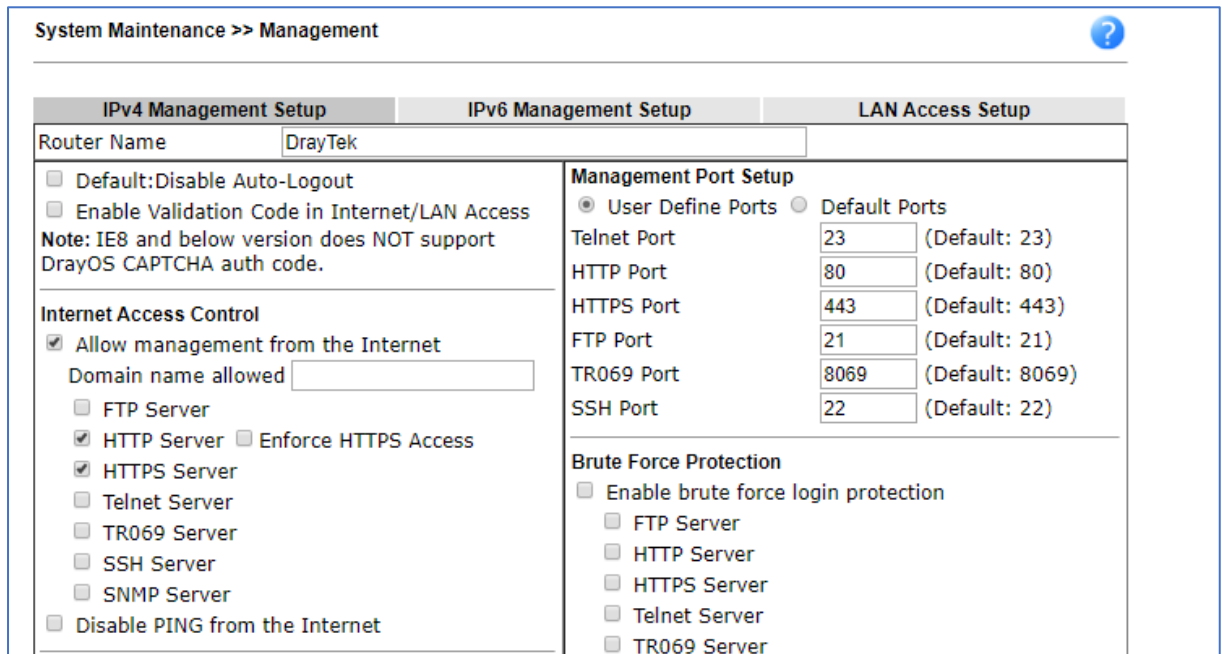
Om gebruik te kunnen maken van Let's Encrypt dient u een DrayDDNS account te registreren. Met DrayDDNS kunt u een eigen hostname kiezen op het drayddns.com domein. De DrayDDNS dienst is een jaar geldig, na dit jaar dient u de registratie opnieuw te verlengen. Voor het aanmaken van een DrayDDNS account kunt u onze handleiding op www.draytek.nl volgen.

Belangrijk: niet elke DrayTek modem/router kan overweg met Let's Encrypt, dit kunt u controleren in het Dynamic DNS profiel. Hier moet de mogelijkheid 'Let's Encrypt' beschikbaar zijn.

Let's Encrypt vereisten

Om succesvol een Let's Encrypt certificaat aan te vragen, zijn er een aantal vereisten waar u rekening mee dient te houden.

1. **HTTP management** op poort 80 dient open te staan, zodat communicatie tussen de DrayTek en de Let's Encrypt servers mogelijk is. Wanneer dit een andere poort is dient u deze tijdelijk terug te zetten naar poort 80.



The screenshot shows the 'System Maintenance >> Management' page. It features three tabs: 'IPv4 Management Setup', 'IPv6 Management Setup', and 'LAN Access Setup'. The 'Router Name' is set to 'DrayTek'. Under 'Management Port Setup', the 'User Define Ports' radio button is selected. The configuration table is as follows:

Service	Port	Default
Telnet Port	23	(Default: 23)
HTTP Port	80	(Default: 80)
HTTPS Port	443	(Default: 443)
FTP Port	21	(Default: 21)
TR069 Port	8069	(Default: 8069)
SSH Port	22	(Default: 22)

Other settings include 'Brute Force Protection' (disabled) and 'Internet Access Control' (with 'Allow management from the Internet' checked).

2. U dient gebruik te maken van de meest recente firmware versie. U kunt hiervoor onze website www.draytek.nl raadplegen.

Let's Encrypt certificaat aanvragen

Ga in de DrayTek naar Applications > Dynamic DNS Setup, klik op het profiel waar u het DrayDDNS account heeft geconfigureerd. Hier kunt u een Let's Encrypt certificaat aanvragen door op 'Create' te klikken.

Index : 1

Enable Dynamic DNS Account

Service Provider

Status **Activated** [Start Date:2018-06-25 Expire Date:2019-06-25]

Domain Name

Determine WAN IP IPv4 IPv6

WAN Interfaces WAN 1 WAN 2 WAN 3 WAN 4

Let's Encrypt certificate

Status Empty

Auto Update

DrayTek zal contact zoeken met de Let's Encrypt servers om een certificaat aan te vragen.

192.168.26.1/doc/letsencrypt.htm - Google Chrome

Not secure | 192.168.26.1/doc/letsencrypt.htm

Your Vigor router is working hard to get you a certificate from Let's Encrypt. Give it 2 to 3 minutes. Please don't close the browser.

```
2018-07-31 08:36:42 check HTTP and WAN setting ok
2018-07-31 08:36:42 domain:louis2862.drayddns.com
IP:WAN2:111.251.239.107
2018-07-31 08:36:42 certificate status: Empty
2018-07-31 08:36:42 certificate operation: Renew
2018-07-31 08:36:42 looking up for let's encrypt server ...
2018-07-31 08:36:45 key pair validation success
2018-07-31 08:36:45 waiting server to verify domain ..
```

Wanneer dit is afgerond, krijgt u onderstaande melding te zien, door op 'Use this certificate for all my services' te klikken kunt u het certificaat in uw DrayTek gebruiken.

A certificate from Let's Encrypt is now in your device and ready to be used.
You may active any services required a certificate for securing connection.

```
2018-07-31 08:36:42 certificate status: Empty
2018-07-31 08:36:42 certificate operation: Renew
2018-07-31 08:36:42 looking up for let's encrypt server ...
2018-07-31 08:36:45 key pair validation success
2018-07-31 08:36:45 waiting server to verify domain ..
2018-07-31 08:36:55 domain verify success
2018-07-31 08:36:55 start generating certificate ...
2018-07-31 08:37:02 send certificate status to myvigor
2018-07-31 08:37:03 Update certificate status successfully.
2018-07-31 08:37:07 generating certificate success
2018-07-31 08:37:07 sending certificate signing request
2018-07-31 08:37:08 downloading certificate from server ..
2018-07-31 08:37:08 certificate updated successfully
2018-07-31 08:37:09 downloading issuer certificate ..
2018-07-31 08:37:09 certificate update finished !!
```

Let's Encrypt certificaat controle

Onder Certificate Management > Local Certificate kunt u de status inzien van het Let's Encrypt certificaat. De Status OK geeft aan dat het certificaat succesvol is ingeladen.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
Self Sign	/C=TW/ST=Hsinchu/L=Hsinchu/O...	OK	<input type="button" value="View"/>	<input type="button" value="Delete"/>
DrayDDNS	/CN=louis2862.drayddns.com	OK	<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!!

Om gebruik te maken van het Let's Encrypt certificaat kunt u bij SSL VPN > General Setup het server certificate aan te passen van 'Self-Signed' naar 'DrayDDNS'.

SSL VPN >> General Setup

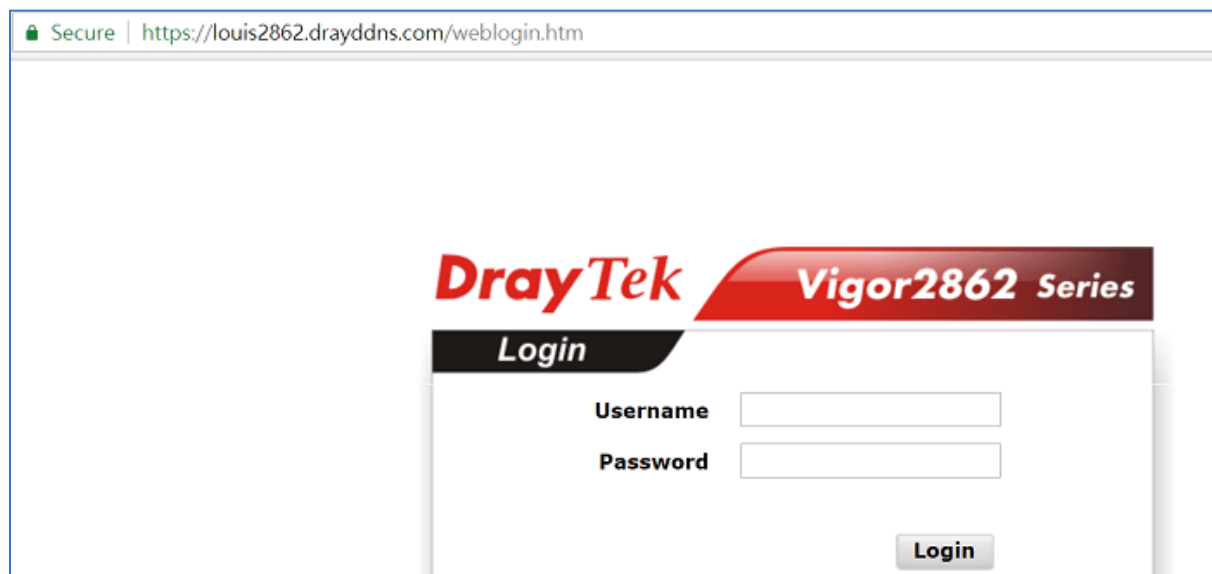
SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> WAN3 <input checked="" type="checkbox"/> WAN4
Port	<input type="text" value="443"/> (Default: 443)
Server Certificate	<input type="text" value="DrayDDNS"/> ▼

Note:

1. The settings will act on all SSL applications.
2. Please go to **System Maintenance >> Management** to enable SSLv3.0 .
3. Please go to **System Maintenance >> Self-Signed Certificate** to generate a new "self-signed" certificate.

Wanneer u de DrayTek vervolgens benaderd op HTTPS zult u zien dat er een beveiligde verbinding gemaakt wordt.



Secure | <https://louis2862.draydns.com/weblogin.htm>

DrayTek **Vigor2862 Series**

Login

Username

Password

Login

Auto Update Let's Encrypt

Een Let's Encrypt certificaat is standaard 3 maanden geldig, na afloop zult u het certificaat moeten vernieuwen. Dit kan de DrayTek tevens voor u uitvoeren. Hiervoor dient u de optie 'Auto update' aan te vinken. De DrayTek zal het certificaat dan automatisch vernieuwen.

Index : 1

Enable Dynamic DNS Account

Service Provider

Status **Activated** [Start Date:2018-06-25 Expire Date:2019-06-25]

Domain Name

Determine WAN IP IPv4 IPv6

WAN Interfaces WAN 1 WAN 2 WAN 3 WAN 4

Let's Encrypt certificate

Status **Signed** [Valid To: Oct 29 06:37:09 2018 GMT]

Auto Update

Voorbehoud

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

Copyright verklaring

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.