

HowTo own SSL Certificate on DSR-Series (neue WebGUI)

# [Voraussetzungen]

- 1. DSR-150N A2-Rev mit Firmwareversion 2.11B301 und höher
- 2. DSR-250N mit Firmwareversion 2.11B301 und höher
- 3. DSR-500N mit Firmwareversion 2.11B301 und höher
- 4. DSR-1000N mit Firmwareversion 2.11B301 und höher
- 5. DSR-1000AC mit Firmwareversion 3.08B301 und höher

## [Szenario]

Es soll ein eigenes SSL Zertifikat für den HTTPS-Zugriff auf dem Gerät installiert werden.

## [Voraussetzungen]

Stellen Sie bitte sicher, dass sich Server und Client in der korrekten, gleichen Zeitzone befinden.

Bitte kontaktieren Sie den in Ihrer Organisation für die Zertifikatsaustellung verantwortlichen Mitarbeiter.

Alternativ suchen Sie sich bitte einen für Sie passenden Zertifikatsaussteller (z.B. verisign.com) oder erstellen Ihre eigene CA-Struktur. Das Stammzertifikat muss BASE64 Codiert sein.

In diesem Beispiel wird ein lokaler Zertifizierungsserver (Windows Server 2012R2) benutzt. ⇒ Download CA-Stammzertifikat vom Zertifizierungsserver (http://<IPServer>/certsrv)

*Microsoft*-Active Directory-Zertifikatdienste -- dlink-dce-WIN2K12R2RADIUS-CA-2

Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkett

Installieren Sie diese Zertifizierungsstellen-Zertifikatkette, damit von dies

Wählen Sie das Zertifikat und die Codierungsmethode für den Download

Zertifizierungsstellenzertifikat:

Aktuelles [dlink-dce-WIN2K12R2RADIUS-CA-2]

Codierungsmethode:

ODER Base 64

Cownload des Zertifizierungsstellenzertifikats> Download der Zertifizierungsstellen-Zertifikatkette Download der aktuellen Basissperrliste Download der aktuellen Deltasperrliste



[Installation des CA-Stammzertifikates]

- 1. greifen Sie auf Ihren DSR-1000AC zu
  - a. gehen Sie auf "VPN > Certificates"

D-Link Unified Services Router - DSR-1000AC		Logged in as: adr Serial:	nin (ADMIN)   Language:   Firmware: 3.   Wizard	age: English [US] () Logout 3.08B301C_WW d System Search 4		
🛜 Wireless	💻 Network	CA VPN	Security	<sup>©</sup> Maintenance		
PPTP VPN	L2TP VPN	SSL VPN	OpenVPN	GRE		
Server	Server	SSL VPN Server Policy	Settings	GRE		
Client	Client	Portal Layouts	Local Networks			
Active Users	Active Users	Resources	Remote Networks			
		SSL VPN Client	Authentication			
		Client Routes				
	r - DSR-1000AC Wireless PPTP VPN Server Client Active Users	r - DSR-1000AC        Wireless     Network       PPTP VPN     L2TP VPN       Server     Server       Client     Client       Active Users     Active Users	r - DSR-1000AC	r - DSR-1000AC       Language         Serial:       Firmware: 3         Wizard       Wizard         PPTP VPN       L2TP VPN         Server       Server         Client       Client         Active Users       Active Users         Resources       Remote Networks         SSL VPN Client       Authentication		

b. wählen Sie "Upload New CA Certifikat" um ein neues Stammzertifikat auf den DSR-1000AC hochzuladen

VPN » IPSec VPN » Certificates » Trusted Certificates				<b>? 0</b>
Trusted Certificates Active Self Certificates Self C	Certificate Requests			
Trusted Certificates or CA certificates are used to verify the trusted organization or authority called the Certificate Author presents a digital certificate, the authentication process verif CA certificates are used in this authentication process.	validity of certificates signed by rity. The table contains the certi fies that the presented certifical	them. W ificates o te is issue	'hen a certificate is generated, f each CA.When a remote VPN ed by one of the trusted author	it is signed by a gateway or client ities. The Trusted
Trusted Certificates (CA Certificate) List				
Show 10 • entries [Right click on record to get more options	s]			
CA Identity (Subject Name)	🔂 Issuer Name	⇔	Expiry Date & Time	⇔
	No data available in table			
Showing 0 to 0 of 0 entries			First    Previous	Next 🔪 Last 刘
Upload New CA Certificate				

c. wählen Sie Ihr gültiges Stammzertifikat (CA Certifikat) aus und laden Sie dieses auf den DSR-1000AC

Trusted Certificates (CA Cert	rtificate) Configuration	×
Certificate File	Durchsuchen CA-certnew.p	
		Upload



# d. nachdem das Stammzertifikat (CA) erfolgreich hochgeladen wurde sehen Sie CA-Identität

VPN » IPSec VPN » Certif	icates » Trusted Certificates						0
	•		Operation Succ	eeded			
Trusted Certificates	Active Self Certificates	Self (	Certificate Requests				
Trusted Certificates or CA trusted organization or au presents a digital certifica CA certificates are used in <b>Trusted Certificates</b>	certificates are used to veri thority called the Certificate te, the authentication proces this authentication process. (CA Certificate) List	fy the v Author ss verif	validity of certificates ity. The table contain ies that the presented	signed by them. When a the certificates of each certificate is issued by o	certificate is CA.When a re ne of the tru:	generated, it is signed emote VPN gateway or sted authorities. The Tr	by a client rusted
Show 10 • entries [Ri	ght click on record to get more	options	J				
CA Identity (Subject N	Name)	÷	Issuer Name		⇔	Expiry Date & Tim	e ⊖
DC=de, DC=dlink-dce, CN=dlin	nk-dce-WIN2K12R2RADIUS-CA-2		DC=de, DC=dlink-dce, CI	l=dlink-dce-WIN2K12R2RADIU	5-CA-2	Jun 14 16:02:29 2021 G	MT
Showing 1 to 1 of 1 entries					H First	Previous 1 Next > L	ast 🕅
Upload New CA Certi	ificate						

[Erstellen eines CSR (Certificate Self Request)]

- 1. greifen Sie auf Ihren DSR-1000AC zu
  - a. gehen Sie auf "VPN > Certificates > Self Certificate Requests"
  - b. wählen Sie "New Self Certificate" zur Erstellung eines neuen CSR aus

VPN » IPSec VPN » Certificates » Self Certificate Requests		0 0
Trusted Certificates Active Self Certificates Self Certificate	Requests	
The Self Certificate Requests table displays a list of all the certificate req	uests made.	
Self Certificate Requests List		
Show 10 • entries [Right click on record to get more options]		
Name 🗘	Status	$\ominus$
No data	available in table	
Showing 0 to 0 of 0 entries		K First Previous Next > Last >
New Self Certificate		



- c. tragen Sie die notwendigen Daten für Ihr CSR ein
  - i. Name
  - ii. Subjekt
  - iii. Hash Algorithmus
  - iv. Signature Key Length
- = SHA1 = 2048
- v. Application Tye
- = HTTPS für SSL oder IPSEC für Tunnel
- vi. IP Adresse
- vii. Domain Name
- viii. eMail Address
- = optional = optional

= Name Ihres CSR

= Ihre Daten für das Zertifikat

= optional

Generate Self Certificate Reques	t	8
Name	LAB	
≪ubject	DEUR, CN=marcus.dlink-dce.de	
Hash Algorithm	SHA1	
Signature Key Length	2048	
Application Type	Https	
IP Address	192.168.10.241	
Domain Name		
Email Address		
		Save

In diesem Beispiel wurden folgende Daten verwendet:

C=DE,ST=Germany,L=Eschborn,O=D-Link,OU=DEUR,CN=marcus.dlink-dce.de

C = Land, ST = Land/Bundesland, L = Ort, O = Organisation, OU = Abteilung, CN = Common Name

- d. nachdem Sie den CSR Erstellt haben,können Sie es sich anschauen
- e. klicken Sie mit der rechten Maustaste auf den CSR und wählen "View" aus

VPN » IPSec VPN » Certificates »	Self Certificate Requests	2 🧿
	Operation Succeeded	
Trusted Certificates Activ	e Self Certificates Self Certificate Requests	
The Self Certificate Requests table Self Certificate Requests L	displays a list of all the certificate requests made.	
Show 10  rentries [Right click	on record to get more options]	
Name 🗘	Status	θ
LAB Showing 1 to 1 of 1 entries	Active Self Certificate Not Uploaded	First J Previous 1 Next > Last >
New Self Certificate	1 View	

- 4 -



- f. kopieren Sie den Inhalt des Feldes "Data to supply to CA"g. schließen Sie das Fenster anschließend mir klick auf "x"

Certificate Details		×
System Name Hash Algorithm Signature Algorithm Key length Data to supply to CA	C=DE, ST=Germany, L=Eschborn, O=D-Link, OU=DEUR, CN=marcus.dlink-dce.de SHA1 RSA 2048 BEemr CERTIFICATE REQUEST WKDA0BANVBAgTB0dicm1hbnixkTAP BgNVBACTCEV72hBJJMQ&WDQVDQQKE WZALUxpbmsxDTALBgNVBASTBERPVVIx HDA6BgNVBATE21thcmN1cy5kbGluay1kT2U HDA6BgNVBATE21thcmN1cy5kbGluay1kT2U	



## [Erstellen eines Zertifikates aus dem CSR]

1. greifen Sie nun erneut auf Ihren Zertifikasserver zu um aus dem CSR ein Zertifikat zu erstellen.

Microsoft-Active Directory-Zertifikatdienste -- dlink-dce-WIN2K12R2RADIUS-CA-2

## Willkommen

Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Pr kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sich

Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Ze

Weitere Informationen zu Active Directory-Zertifikatdienste erhalten Sie unter Active Directory-

### Wählen Sie eine Aufgabe:

Ein Zertifikat anfordern

*Microsoft*-Active Directory-Zertifikatdienste -- dlink-dce-WIN2K12R2RADIUS-CA-2

## Zertifikat anfordern

Wählen Sie den Zertifikattyp: Benutzerzertifikat

oder senden Sie eine erweiterte Zertifikatanforderung ein.

#### Microsoft-Active Directory-Zertifikatdienste -- dlink-dce-WI

Erweiterte Zertifikatanforderung

-Die Richtlinie der Zertifizierungsstelle legt fest, welche Zertifikattypen angefordert werden können. Klicken Sie auf ein der folgenden Optionen:

Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen

Renchen Sie eine Zertifikatanforderung ein. die eine Base64-codierte CMD- oder PKCS10-Datel verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datel verwendet, ein

- a. kopieren Sie die Daten des CSR in das Feld (achten Sie darauf, dass keine Leerzeichen am Ende des Requests mit eingetragen sind)
- b. Wählen die gglfs.die entstprechende Zertifikatsvorlage (IPSEC oder Webserver, ..) aus
- c. Drücken Sie einsenden um ein Zertifikat zu erhalten



## Microsoft-Active Directory-Zertifikatdienste -- dlink-dce-WIN2K12R2RADIUS-CA-2

## Zertifikat- oder Erneuerungsanforderung einreichen

Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanford∉ Anforderung" ein, um eine gespeicherte Anforderung bei der Zertifizierur

Gespeicherte Anford	derung:
Base-64-codierte Lertifikatanforderung CMC oder PKCS #10 oder PKCS #7):	wgPHmh+/UfKOGrHsKfSEvKqmesIcao6zLuPzNrmE Q4xzL29gVzQb5fvN+q28QEJTxNUWikzk4xLDMEA51 1SpY2DBHmQqyX9eYvNcYqFPGcZ3r2PdnUh2n1FZkl o3kt19jrfRui9Oyi/cbW7fLvcN0jEgwnfVXJoox/1 lr6XZriMnZskdLY= END CERTIFICATE REQUEST
Zertifikatvorlage:	
<	Webserver
Zusätzliche Attribut	e:
Attribute:	< >>
	Einsenden

Je nach Vorgabe muss dieses Zertifikat noch durch den Zertifikatsverantwortlichen freigegeben werden.

d. Laden Sie das soeben erstellte Zertifikat herunter

*Microsoft*-Active Directory-Zertifikatdienste -- dlink-dce-WIN2K12R2RADIUS-CA-2

## Zertifikat wurde ausgestellt

Das angeforderte Zertifikat wurde ausgestellt.

ODER-codiert oder 

Download des Zertifikats

Download der Zertifikatkette



# [Hochladen des Zertifikates auf den DSR-1000AC]

- 1. greifen Sie auf Ihren DSR-1000AC zu
  - a. gehen Sie auf "VPN > Certificates > Active Self Certificares"
  - b. wählen Sie "Upload New Self Certificate" um das soeben erstellte Zertifikat auf den DSR-1000AC zu laden

VPN » IPSec VPN » Certificates » Active Self Certifi	cates					? •
•	Operation	Succeede	d			
Trusted Certificates Active Self Certificate	Self Certificate Requ	iests				
This table lists the certificates issued to you by trus IKE server validates this router using these certifica	ted Certification Authoriti tes. For each certificate,	es (CAs), an the following	d available for present g data is displayed:	ation to r	remote IKE servers. T	he remote
Active Self Certificates List						
Show 10 • entries [Right click on record to get m	ore options]					
Name 🖸 Subject Name 🗧	Serial Number	⇔	Issuer Name	⇔	Expiry Time	⇔
	No data availa	ble in table				
Showing 0 to 0 of 0 entries				First	I Previous Next >	Last 刘
Upload New Self Certificate						

e. wählen Sie das soeben erstellte Zertifikat aus und laden es mittels "Upload" auf den DSR-1000AC

Upload Active Self Certificate		$\bigotimes$
Certificate File	Durchsuchen certnew.cer	
		Upload



2. nach dem Upload sehen Sie die Daten Ihres gerade installierten Zertifikates

VPN » IP	PSec VPN » Certificates » Active Se	f Certificates				?	9
	•	Operation Succee	ded				
Trust	ted Certificates Active Self Cer	tificates Self Certificate Requests					_
This table IKE server	e lists the certificates issued to you r validates this router using these c	by trusted Certification Authorities (CAs), ertificates. For each certificate, the follow	and available ring data is d	for presentation isplayed:	to remote IKE s	ervers. The rem	ote
Show 10	Self Certificates List	e get more options					
Name	Subject Name	Serial Number	θ	Issuer Name		⊖ Expiry Time	8
LAB	C=DE, ST=Germany, L=Eschborn, O=D-Link, OU=DEUR, CN=marcus.dlink- dce.de	1e:00:00:00:07:20:ee:61:10:d5:0a:92:6f:00:0	0:00:00:00:07	DC=de, DC=dlink-c dce-WIN2K12R2R4	lce, CN=dlink- NIUS-CA-2	Jun 17 08:21:41 201 GMT	8
Showing 1	1 to T of 4 entries			K First	t Previous 1	Now / Last )	4
Uploa	d New Self Certificate						

3. unter dem Menüpunkt Self Certificate Requests sehen Sie, dass Ihr Zertifikat aus dem CSR heraufgeladen wurde

VPN » IPSec VPN » Certificates » Self Certificate Requests	0 0				
Trusted Certificates Active Self Certificates Self Certificate Requests					
The Self Certificate Requests table displays a list of all the certificate requests made.					
Self Certificate Requests List					
Show 10  • entries [Right click on record to get more options]					
Name 🕜 Status	⇔				
LAB Active Self Certificate Uploaded					
Showing 1 to 1 of 1 entries	First Previous 1 Next > Last >				
New Self Certificate					



# [Aktivieren des Zertifikates auf den DSR-1000AC]

- 1. greifen Sie auf Ihren DSR-1000AC zu
  - a. gehen Sie auf "VPN > Certificates > Active Self Certificares"
  - b. klicken Sie mit der rechten Mausaste auf das Zertifikat und setzen dies als "Default", damit es aktiv ist

VPN » IP	PSec VPN » Certificates » Active Self	Certificates		? 🥑		
certificate has been changed please wait for 60 seconds						
Trusted Certificates Active Self Certificates Self Certificate Requests						
This table lists the certificates issued to you by trusted Certification Authorities (CAs), and available for presentation to remote IKE servers. The remote IKE server validates this router using these certificates. For each certificate, the following data is displayed: Active Self Certificates List						
Show 10 • entries [Right click on record to get more options]						
Nam	Subject Name ⊖	Serial Number $\ominus$	Issuer Name 😔	Expiry Time ↔		
LAB	C=DE, ST=Germany, L=Eschborn, O=D-Link, OU=DEUR, CN=marcus.dlink- dce.de	1e:00:00:00:07:20:ee:61:10:d5:0a:92:6f:00:00:00:00:00:07	DC=de, DC=dlink-dce, CN=dlink- dce-WIN2K12R2RADIUS-CA-2	Jun 17 08:21:41 2018 GMT		
Showing	1 to 1 of 1 entries		First Previous 1	lext 🔪 Last 刘		
Upload New Self Certificate						

# Zertifikat vor der Aktivierung:

https://192.168.10.241/scgi-bin/platform.cgi	🔎 – 😢 Zertifikatfehler 🕐
Datei Bearbeiten Ansicht Favoriten Extras ? ↓ Vorgeschlagene Sites ▼ Ø JDE Intern Ø httpsrv-049-41-pbvweb Http://www	entportal 2.0 📓 Free Internet Radio Statio 📓 Free Internet Radio Sta
Zertifikat	SR-1000AC ease login to access D-Link Unified Services Router (DSR-1000AC vice. pgin
rusgestellt für:       dsr.dlink.com.tw         Ausgestellt von:       dsr.dlink.com.tw         cijltig ab       30. 03. 2016 bis       28. 03. 2026         Zertifikat installieren       Ausstellererklärung         Weitere Informationen über Zertifikate	Username Password Login



# Zertifikat nach der Aktivierung:



Anschließend müssen sie das Zertifikat und ggfls. das CA-Stammzertifikat bei Ihren Clients installieren.