

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 Zertifikatsausstellung 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 Downloa

Zertifizierungsstellenzertifikat:

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

Codierungsmethode:

- DER
 Base 64

[Download des Zertifizierungsstellenzertifikats](#)

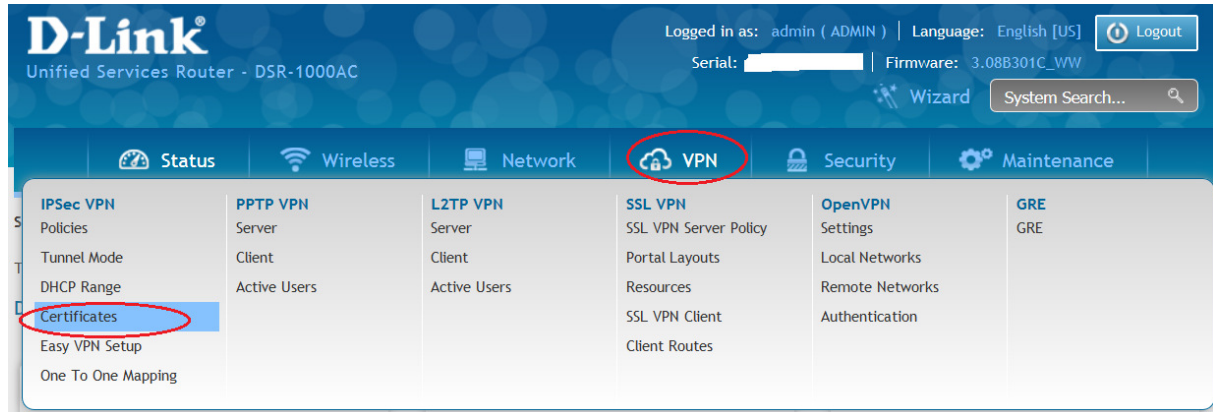
[Download der Zertifizierungsstellen-Zertifikatkette](#)

[Download der aktuellen Basissperrliste](#)

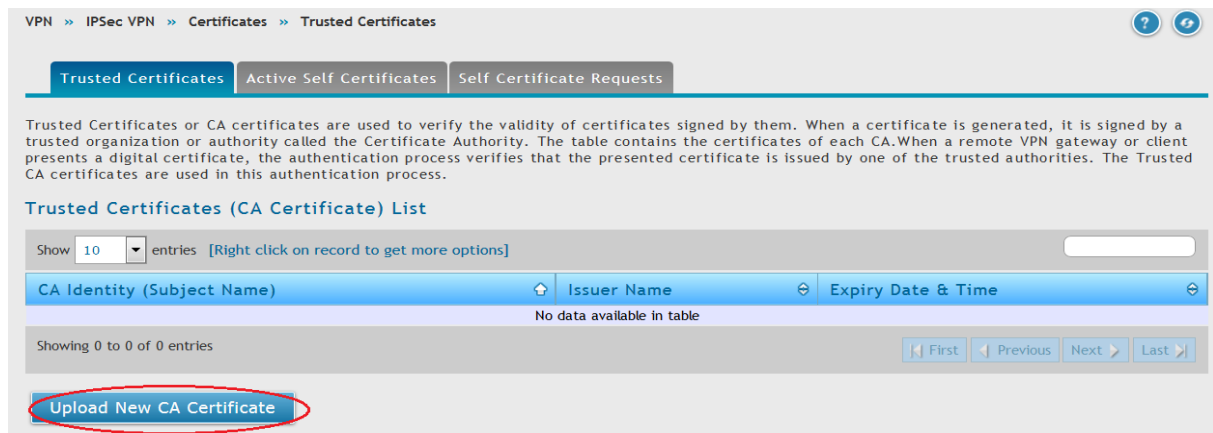
[Download der aktuellen Deltasperrliste](#)

[Installation des CA-Stammzertifikates]

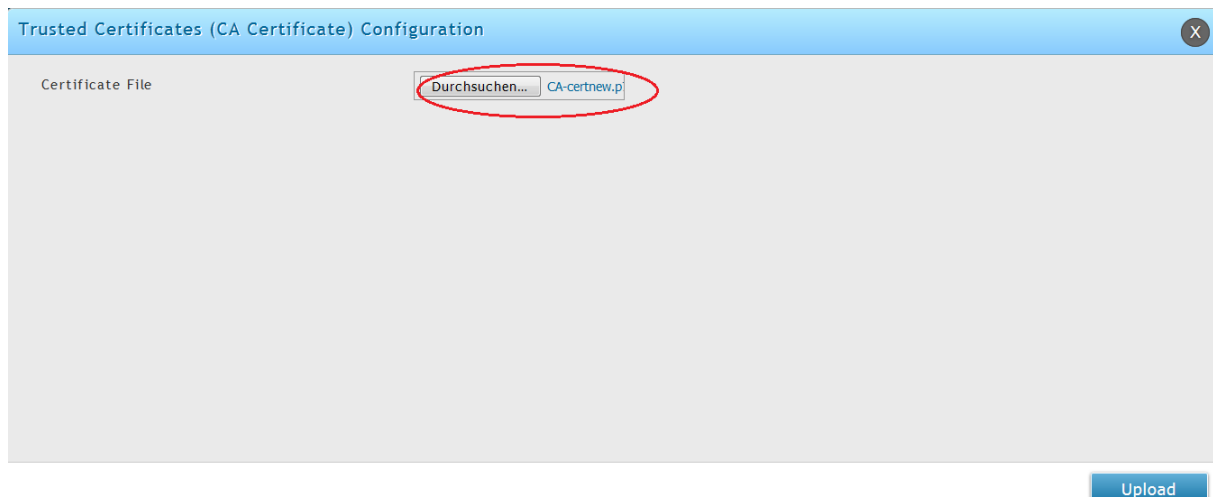
1. greifen Sie auf Ihren DSR-1000AC zu
 - a. gehen Sie auf „VPN > Certificates“



- b. wählen Sie “Upload New CA Zertifikat” um ein neues Stammzertifikat auf den DSR-1000AC hochzuladen



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



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

VPN » IPsec VPN » Certificates » Trusted Certificates

Operation Succeeded

Trusted Certificates Active Self Certificates Self Certificate Requests

Trusted Certificates or CA certificates are used to verify the validity of certificates signed by them. When a certificate is generated, it is signed by a trusted organization or authority called the Certificate Authority. The table contains the certificates of each CA. When a remote VPN gateway or client presents a digital certificate, the authentication process verifies that the presented certificate is issued by one of the trusted authorities. The Trusted CA certificates are used in this authentication process.

Trusted Certificates (CA Certificate) List

Show 10 entries [Right click on record to get more options]

CA Identity (Subject Name)	Issuer Name	Expiry Date & Time
DC=de, DC=dlink-dce, CN=dlink-dce-WIN2K12R2RADIUS-CA-2	DC=de, DC=dlink-dce, CN=dlink-dce-WIN2K12R2RADIUS-CA-2	Jun 14 16:02:29 2021 GMT

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Upload New CA Certificate

[Erstellen eines CSR (Certificate Self Request)]

- greifen Sie auf Ihren DSR-1000AC zu
 - gehen Sie auf „VPN > Certificates > Self Certificate Requests“
 - wählen Sie “New Self Certificate” zur Erstellung eines neuen CSR aus

VPN » IPsec VPN » Certificates » Self Certificate Requests

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
No data available in table	

Showing 0 to 0 of 0 entries

First Previous Next Last

New Self Certificate

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

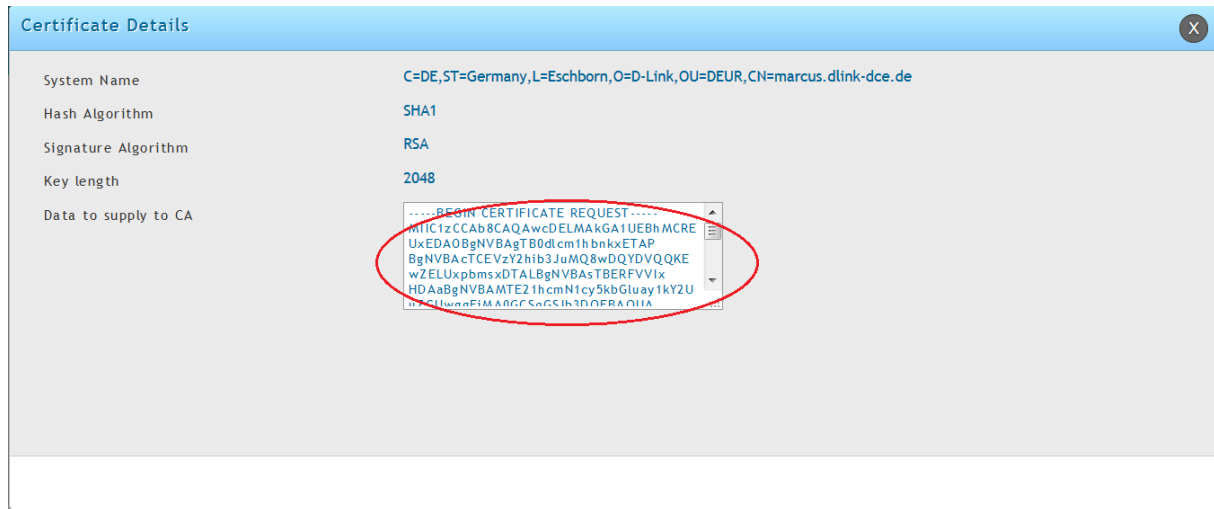
In diesem Beispiel wurden folgende Daten verwendet:

”
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

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



[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 Programme kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Schritte durchführen.

Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatsvorlage oder einer Zertifikatsanforderung verwenden.

Weitere Informationen zu Active Directory-Zertifikatdiensten 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-WIN2K12R2RADIUS-CA-2

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](#)

[Reichen Sie eine Zertifikatanforderung ein, die eine Base64-codierte CMD- oder PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei 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 ggfs. die entsprechende Zertifikatsvorlage (IPSEC oder Webserver, ..) aus
- c. Drücken Sie einsenden um ein Zertifikat zu erhalten

Zertifikat- oder Erneuerungsanforderung einreichen

Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanforderung ein, um eine gespeicherte Anforderung bei der Zertifizierung

Gespeicherte Anforderung:

Base-64-codierte Zertifikatanforderung CMC oder PKCS #10 oder PKCS #7):

```
wqPHmh+/UfKOGrHsKfSEvKqmesIcao6zLuPzNrmE:  
Q4xzL29gVzQb5fvN+q28QEJTxNUWikzk4xLDMEA5!  
1SpY2DBHmQqyX9eYvNcYqFPGcZ3rZPdnUh2n1FZkl  
o3kt19jrfRui9Oyi/cbW7fLvcN0jEgwnfVXJoox/i  
lr6XZriMnZskdLY=  
-----END CERTIFICATE REQUEST-----
```

Zertifikatvorlage:

Webserver

Zusätzliche Attribute:

Attribute:

Einsenden

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

- d. Laden Sie das soeben erstellte Zertifikat herunter

Zertifikat wurde ausgestellt

Das angeforderte Zertifikat wurde ausgestellt.

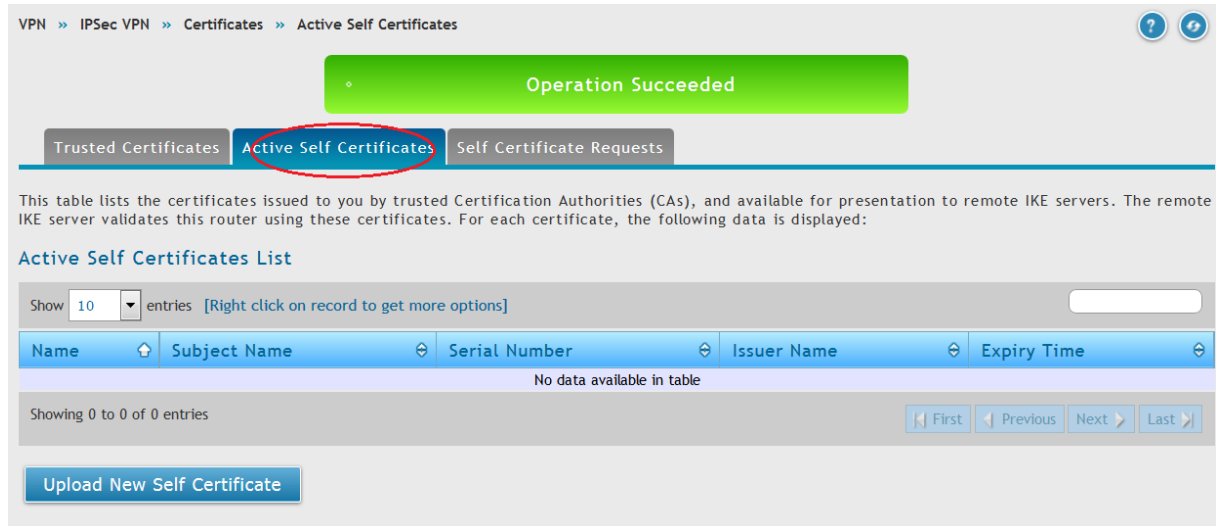
DER-codiert oder Base-64-codiert



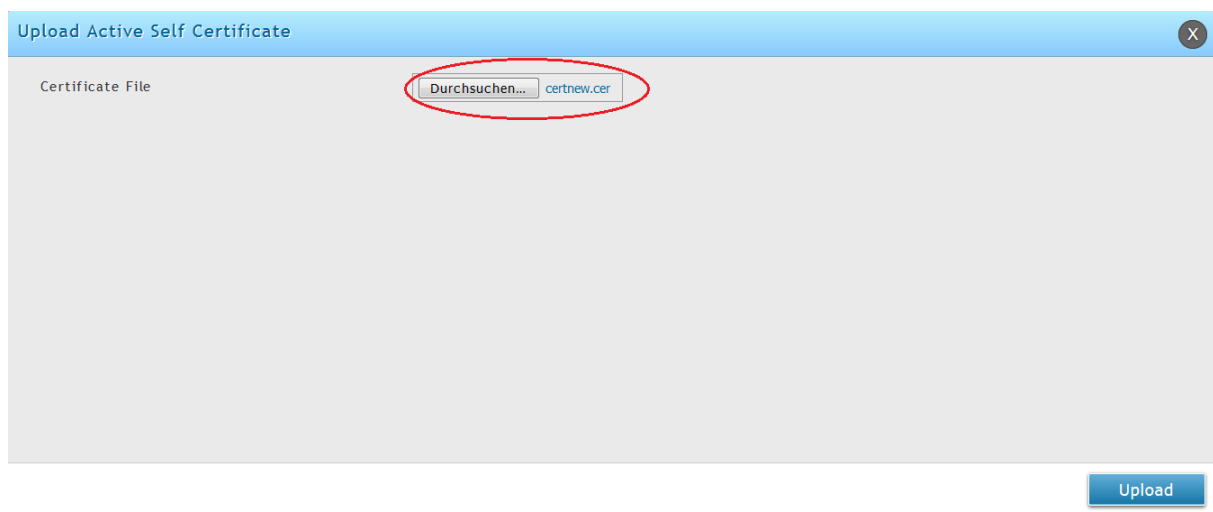
[Download des Zertifikats](#)
[Download der Zertifikatkette](#)

[Hochladen des Zertifikates auf den DSR-1000AC]

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



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



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

VPN » IPsec VPN » Certificates » Active Self Certificates

Operation Succeeded

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]

Name	Subject Name	Serial Number	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:00:00:00:00:07	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

Upload 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

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

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 Certificates“
 - b. klicken Sie mit der rechten Mausaste auf das Zertifikat und setzen dies als “Default”, damit es aktiv ist

VPN >> IPSec 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]

Name	Subject Name	Serial Number	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:00:00:00:00:07	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

Upload New Self Certificate

Zertifikat vor der Aktivierung:

https://192.168.10.241/scgi-bin/platform.cgi

Zertifikatfehler

Vorgeschlagene Sites

JDE Intern

Agentportal 2.0

Free Internet Radio Statio...

Free Internet Radio Sta

Zertifikat

Allgemein | Details | Zertifizierungspfad

Zertifikatsinformationen

Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.

Ausgestellt für: dsr.dlink.com.tw

Ausgestellt von: dsr.dlink.com.tw

Gültig ab 30. 03. 2016 bis 28. 03. 2026

Zertifikat installieren... Ausstellererklärung

Weitere Informationen über [Zertifikate](#)

SR-1000AC

Please login to access D-Link Unified Services Router (DSR-1000AC) device.

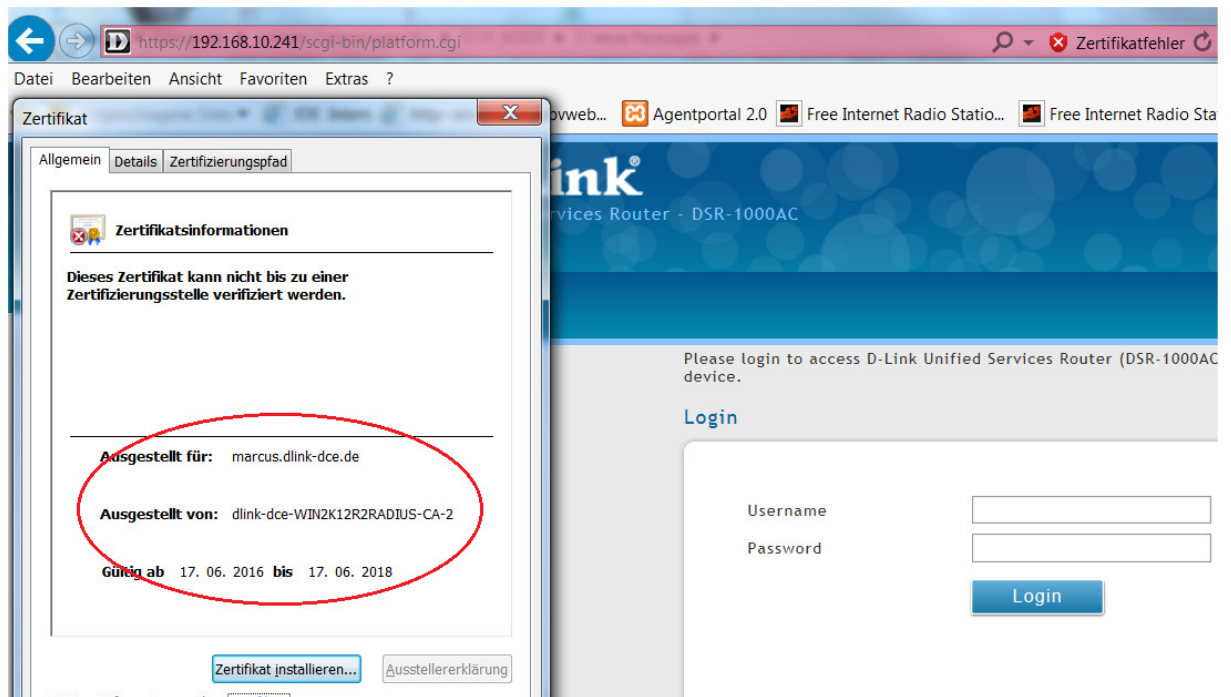
login

Username

Password

Login

Zertifikat nach der Aktivierung:



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