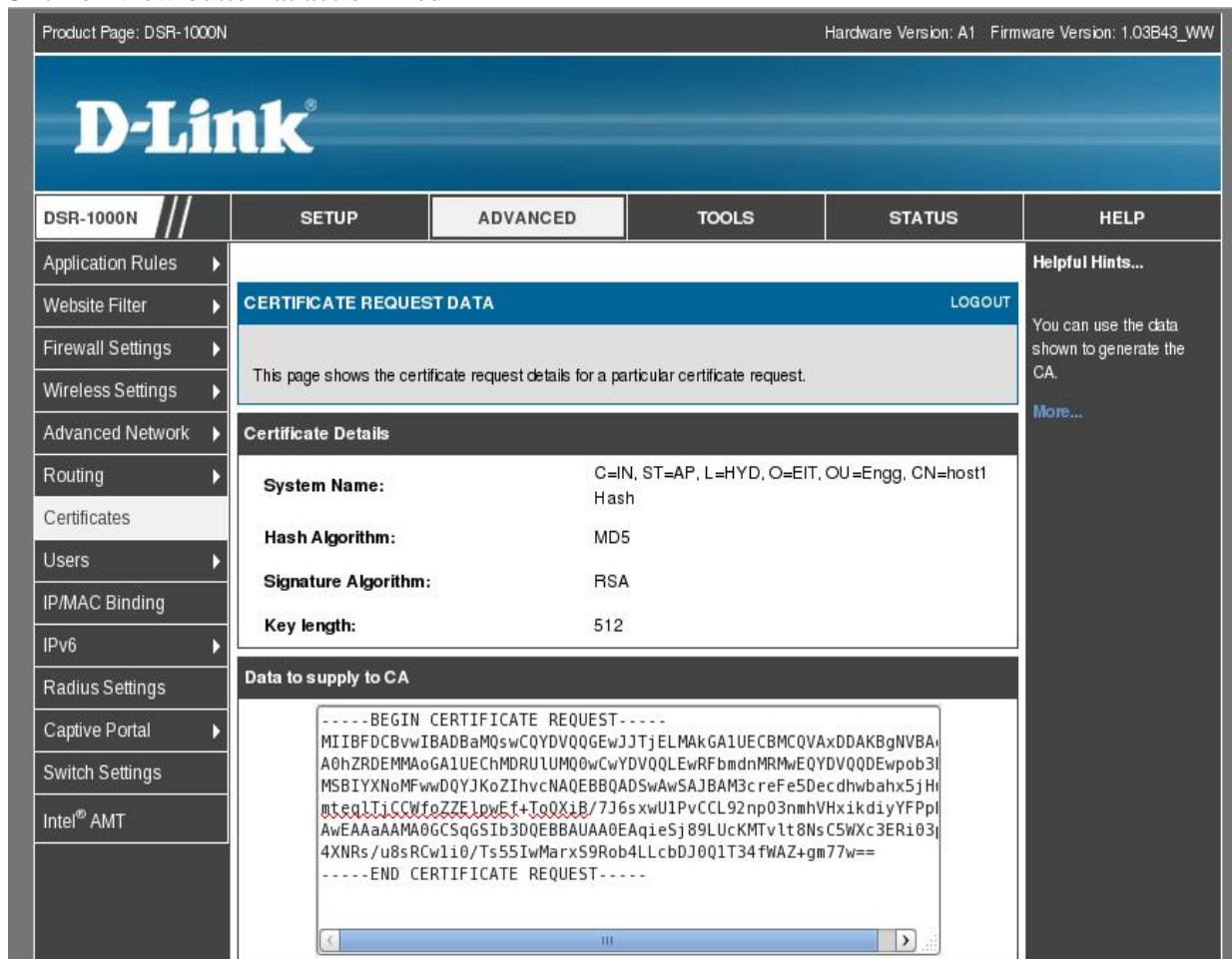


How to request certificates from openssl server

1. Go to Advanced → Certificates → Self Certificates
2. Click on New Self Certificate , Configure as follow
 - a. Name : host1
 - b. Subject : C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1 (Must follow this format for subject)
 - c. Hash Algorithm : MD5
 - d. Signature Key Length: 512
3. Click on Save Settings.
4. Click on view button at action filed



Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B43_WW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules Website Filter Firewall Settings Wireless Settings Advanced Network Routing Certificates Users IP/MAC Binding IPv6 Radius Settings Captive Portal Switch Settings Intel® AMT

CERTIFICATE REQUEST DATA LOGOUT

This page shows the certificate request details for a particular certificate request.

Certificate Details

System Name:	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1
Hash Algorithm:	MD5
Signature Algorithm:	RSA
Key length:	512

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBFDCBvwIBADBaMQswCQYDVQQGEwJJtjELMAkGA1UECBMCQVxDDAKBgNVBA
A0hZRDEMMMAoGA1UEChMURU1UMQ0wCwYDVQQLEwRFRmndnMRMwEQYDVQQDEwpob3I
MSBIYXNoMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAM3creFe5Decdhwbahx5jH
tsgLtiCCWfoZZE1pwEf+To0XiB/7J6sXwU1PvCCL92np03nmhVHxikdiyYFPp
AwEAAaAAMA0GCSqGSIb3DQEBAUAA0EAqieSj89LUcKMTvlt8NsC5Wxc3ERi03j
4XNRs/u8sRCw1i0/Ts55IwMarxS9Rob4LLcbDJ0Q1T34fWAZ+gm77w==
-----END CERTIFICATE REQUEST-----
```

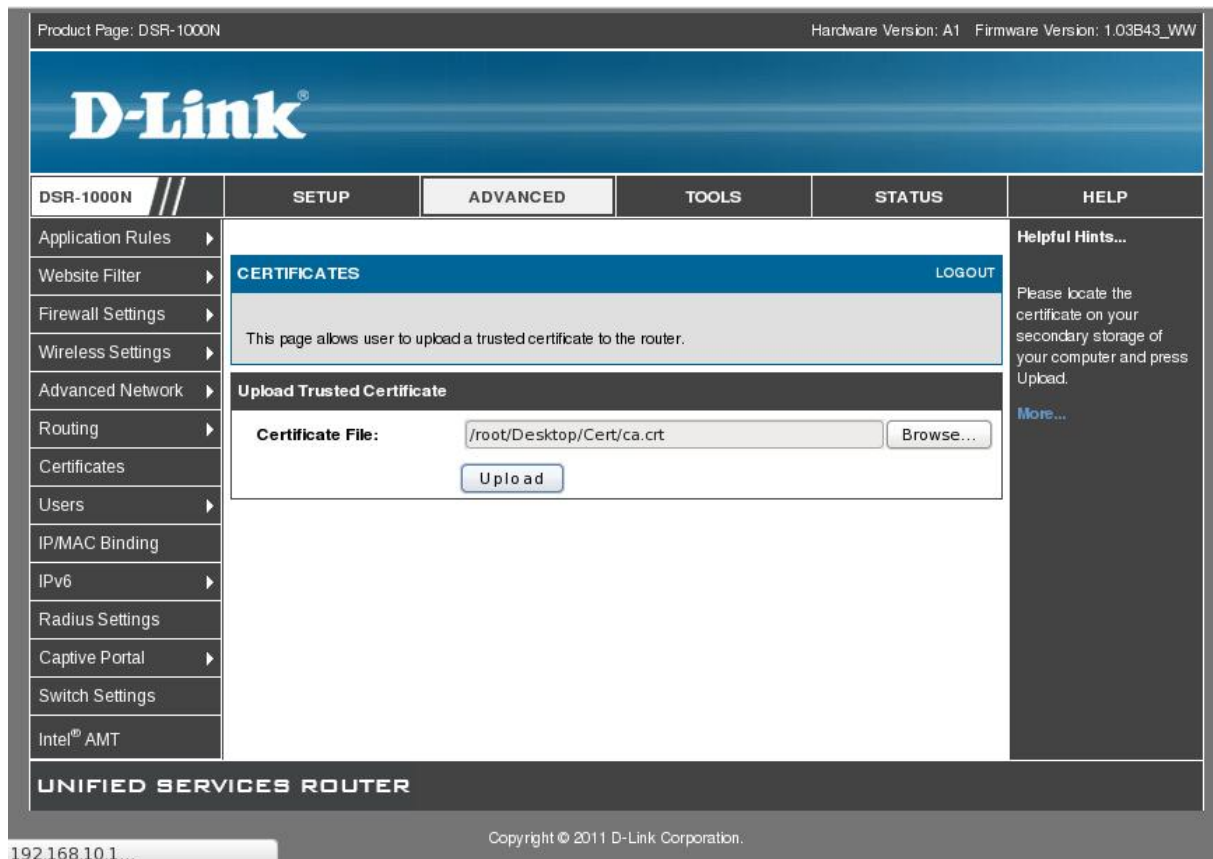
5. Copy the Content in Data to Supply to CA into host1.csr
(NOTE: while copying and modifying data, mode is changed to 777 on all files using the command “`chmod 777 *`”for changing mode for access privileges)

6. The two commands below are used for creating CA certificate(ca.crt)
 - a. openssl genrsa -des3 -out ca.key 512 (key is entered for validation purpose)
 - b. openssl req -new -x509 -days 365 -key ca.key -out ca.crt (data is entered as per the data used in Subject Name)

7. The two commands below are used for creating certificate files(.crt) for corresponding hosts.
 - a. openssl x509 -req -days 182 -in host1.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out host1.crt
 - b. openssl x509 -req -days 182 -in host2.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out host2.crt(if scenario is SSL VPN, more than 1 .crt certificate needed)

8. Browse to Advanced/Certificates page, click on Upload button for Trusted Certificate(CA Certificate)

9. Browse for ca.crt (which was created at step 6.b) and click on Upload



DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules Website Filter Firewall Settings Wireless Settings Advanced Network Routing Certificates Users IP/MAC Binding IPv6 Radius Settings Captive Portal Switch Settings Intel® AMT

Added Trusted Certificate

CERTIFICATES LOGOUT

Digital Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CA) such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities.

Trusted Certificates (CA Certificate)

<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time
<input type="checkbox"/>	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1	Jul 26 09:08:27 2012 GMT

Upload Delete

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input type="checkbox"/>					

Upload Delete

Self Certificate Requests

<input type="checkbox"/>	Name	Status	Action
<input type="checkbox"/>	host1	Active Self Certificate Not Uploaded	View

New Self Certificate Delete

Helpful Hints...
IPsec VPN, SSL VPN, and management over HTTPS use digital certificates. The router has a default self-signed certificate, and this can be replaced by one signed by a known Certificate Authority if needed. Note that a CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.
[More...](#)

10. Then click on Upload button for Active Self Certificate

11. Browse for host1.crt (Which was created at Step 7.a) and click on upload.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B43_VW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules Website Filter Firewall Settings Wireless Settings Advanced Network Routing Certificates Users IP/MAC Binding IPv6 Radius Settings Captive Portal Switch Settings Intel® AMT

CERTIFICATES LOGOUT

This page allows user to upload a active self certificate to the router.

Upload Active Self Certificate

Certificate File: /root/Desktop/Cert/host1.crt

Upload

Upload

Helpful Hints...
Please locate the certificate on your secondary storage of your computer and press Upload.
[More...](#)

UNIFIED SERVICES ROUTER

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules Website Filter Firewall Settings Wireless Settings Advanced Network Routing Certificates Users IP/MAC Binding IPv6 Radius Settings Captive Portal Switch Settings Intel[®] AMT

Added Active Self Certificate

CERTIFICATES [LOGOUT](#)

Digital Certificates (also known as X.509 Certificates) are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CA) such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities.

Trusted Certificates (CA Certificate)

<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time
<input type="checkbox"/>	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1	Jul 26 09:08:27 2012 GMT

[Upload](#) [Delete](#)

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input type="checkbox"/>		C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1 Hash	df87:38:69:20:7aa7.x00	C=IN, ST=AP, L=HYD, O=EIT, OU=Engg, CN=host1	Jan 25 09:08:49 2012 GMT

[Upload](#) [Delete](#)

Self Certificate Requests

<input type="checkbox"/>	Name	Status	Action
<input type="checkbox"/>	host1	Active Self Certificate Uploaded	View

[New Self Certificate](#) [Delete](#)

UNIFIED SERVICES ROUTER

Helpful Hints ...
IPsec VPN, SSL VPN, and management over HTTPS use digital certificates. The router has a default self-signed certificate, and this can be replaced by one signed by a known Certificate Authority if needed. Note that a CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.
[More...](#)

Note:

1. Note: Make sure that Device and LAN Host are in the same time Zone, or the requested certificates may not be usable.
2. The self certificate will activate after adding the Trusted certificate. The status of the Self Certificate Requests shown as "Active Self Certificate Uploaded"