

How to request a test certificate from Windows Server 2008

1. Browse to Advanced/Certificate and press 'New Self Certificate' button

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_WW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Selected Self Certificates Deleted

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="button" value="Upload"/> <input type="button" value="Delete"/>			

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input type="button" value="Upload"/> <input type="button" value="Delete"/>					

Self Certificate Requests

<input type="checkbox"/>	Name	Status	Action
<input type="button" value="New Self Certificate"/> <input type="button" value="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...](#)

2. Fill in Self Certificate Request with the format below then pressing 'Save Settings':

Name: <test>(type whatever in <>)

Subject: C=<TW>, ST=<Taiwan>, L=<Taipei>, O=<D-Link>, OU=<TSS2>, CN=<DIR1000N>

Hash Algorithm: MD5 or SHA

Signature Key Length: 512/1024/2048

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_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

Helpful Hints... More...

GENERATE SELF CERTIFICATE REQUEST LOGOUT

This page allows user to generate a self certificate using a custom configuration.

Generate Self Certificate Request

Name:	<input type="text" value="test"/>
Subject:	<input type="text" value="U=TSS2, CN=DIR1000N"/>
Hash Algorithm:	<input type="text" value="SHA1"/>
Signature Key Length:	<input type="text" value="2048"/>
IP Address (Optional) :	<input type="text"/>
Domain Name (Optional) :	<input type="text"/>
Email Address (Optional) :	<input type="text"/>

UNIFIED SERVICES ROUTER

3. Press 'View' on Self Certificate Requests field

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_WW



DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP																												
<ul style="list-style-type: none"> 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 	<p style="color: red;">Operation succeeded</p> <p>CERTIFICATES LOGOUT</p> <p>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.</p> <p>Trusted Certificates (CA Certificate)</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>CA Identity (Subject Name)</th> <th>Issuer Name</th> <th>Expiry Time</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center;"> <input type="button" value="Upload"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table> <p>Active Self Certificates</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Subject Name</th> <th>Serial Number</th> <th>Issuer Name</th> <th>Expiry Time</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;"> <input type="button" value="Upload"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table> <p>Self Certificate Requests</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Status</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>test</td> <td>Active Self Certificate Not Uploaded</td> <td style="text-align: center;"><input type="button" value="View"/></td> </tr> </tbody> </table>				<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time	<input type="button" value="Upload"/> <input type="button" value="Delete"/>				<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time	<input type="button" value="Upload"/> <input type="button" value="Delete"/>						<input type="checkbox"/>	Name	Status	Action	<input type="checkbox"/>	test	Active Self Certificate Not Uploaded	<input type="button" value="View"/>	<p>Helpful Hints...</p> <p>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.</p> <p>More...</p>
<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time																														
<input type="button" value="Upload"/> <input type="button" value="Delete"/>																																	
<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time																												
<input type="button" value="Upload"/> <input type="button" value="Delete"/>																																	
<input type="checkbox"/>	Name	Status	Action																														
<input type="checkbox"/>	test	Active Self Certificate Not Uploaded	<input type="button" value="View"/>																														

4. Copy all the encrypted data in Data to supply to CA field

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: L03874_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 ▶

[LOGOUT](#)

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

Certificate Details

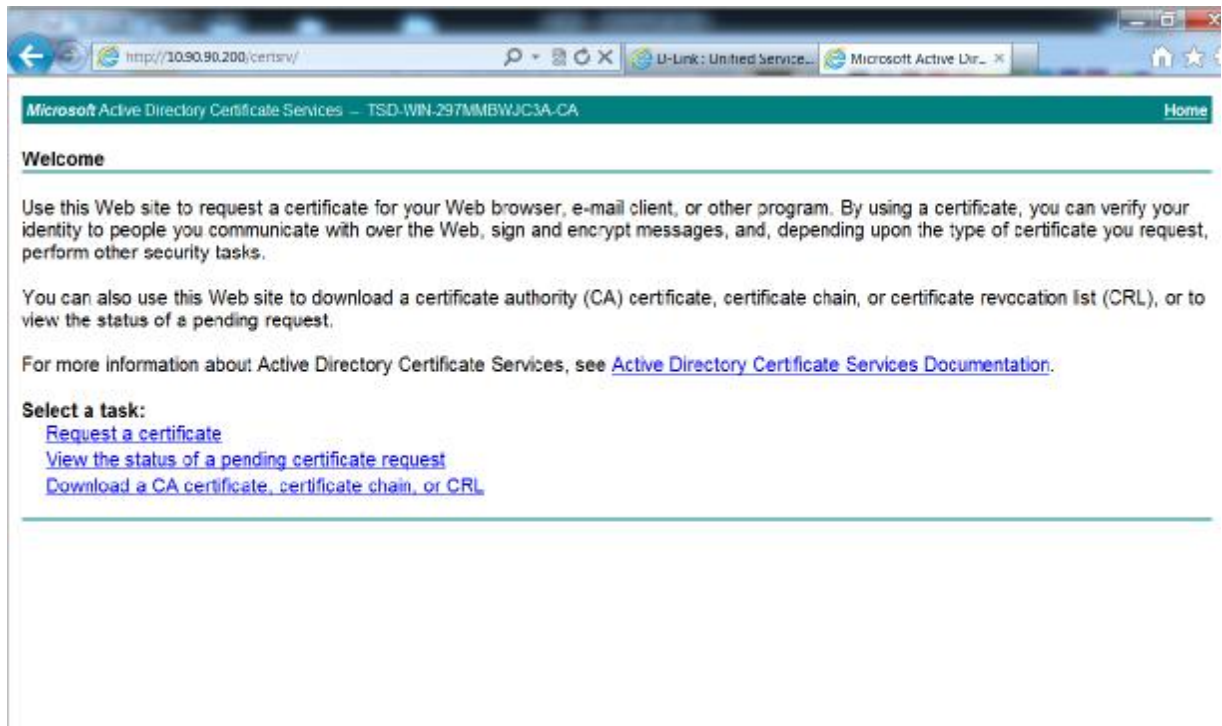
System Name:	C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DIR1000N
Hash Algorithm:	SHA1
Signature Algorithm:	RSA
Key length:	2048

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----
MIICPCAQsCAQAwTjEwMGAUUEBhMCVFEaDzANBgNVBAQgTDR1b3RhaXk6bGJE
RlE0EStkMmVpY299p08w0QYD99qKw2ELExpbm90ZALBqWVBAaTDFX
T0z1a
BgNVBAMTCER1b3RhaXk6bGJEb290b3RhaXk6bGJEb290b3RhaXk6bGJE
b290b3RhaXk6bGJEb290b3RhaXk6bGJEb290b3RhaXk6bGJEb290b3R
hah
ljYRnSExrPWVBIjUWpjjL79oB3A0d4kkPc9yOuteaq2Tg3No6nrugjFPrOo
aeFDqD4Yp9Y7ic//+B1Qec9ha3bp4wGHI+CkYce8Lc2a2404eez6e8g7pm9
B1kLE640y8qg/CXK6CJ38aaFlmayRgpSL68peK412gbybzMACDge24y9p28C
1S71oc2R18f709c/3X77avY891actHoKadTagELa194a0jFPgt120166jRE
vrexLdha31Tolj28ca2w0vIDAGAs0AkwqY3Ro2Thve3Rq2P9aDqg2BAPM/
```

Helpful Hints...
 You can use the data shown to generate the CA.
[More...](#)

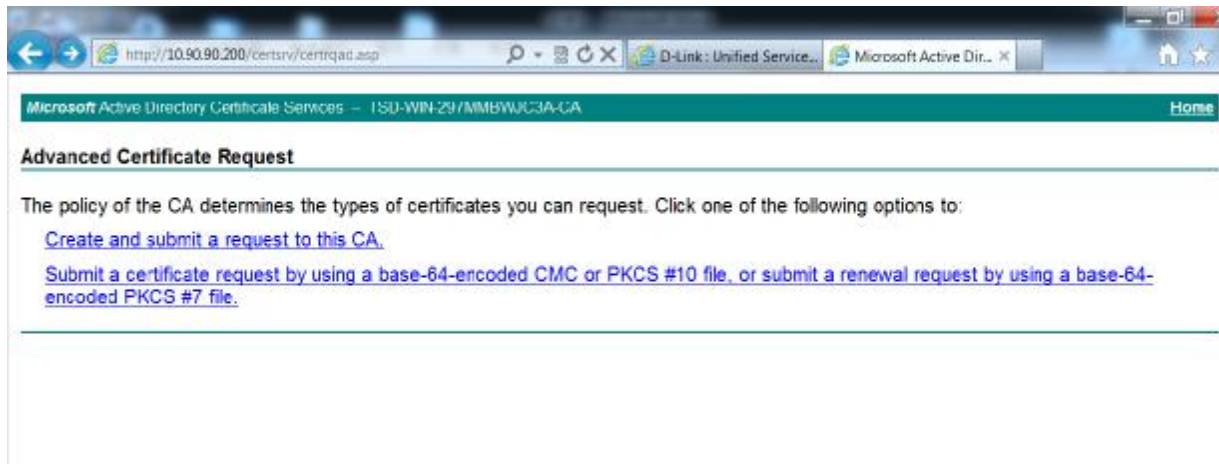
5. Request a certificate from Server 2008



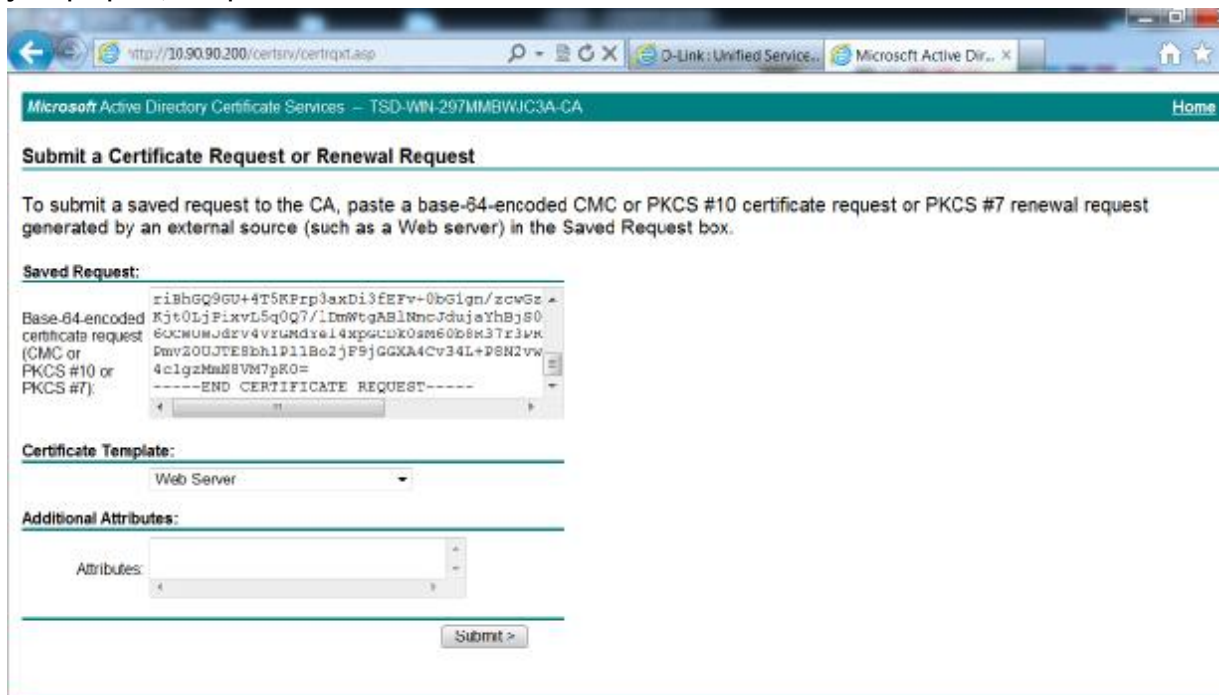
6. Choose 'advanced certificate request'



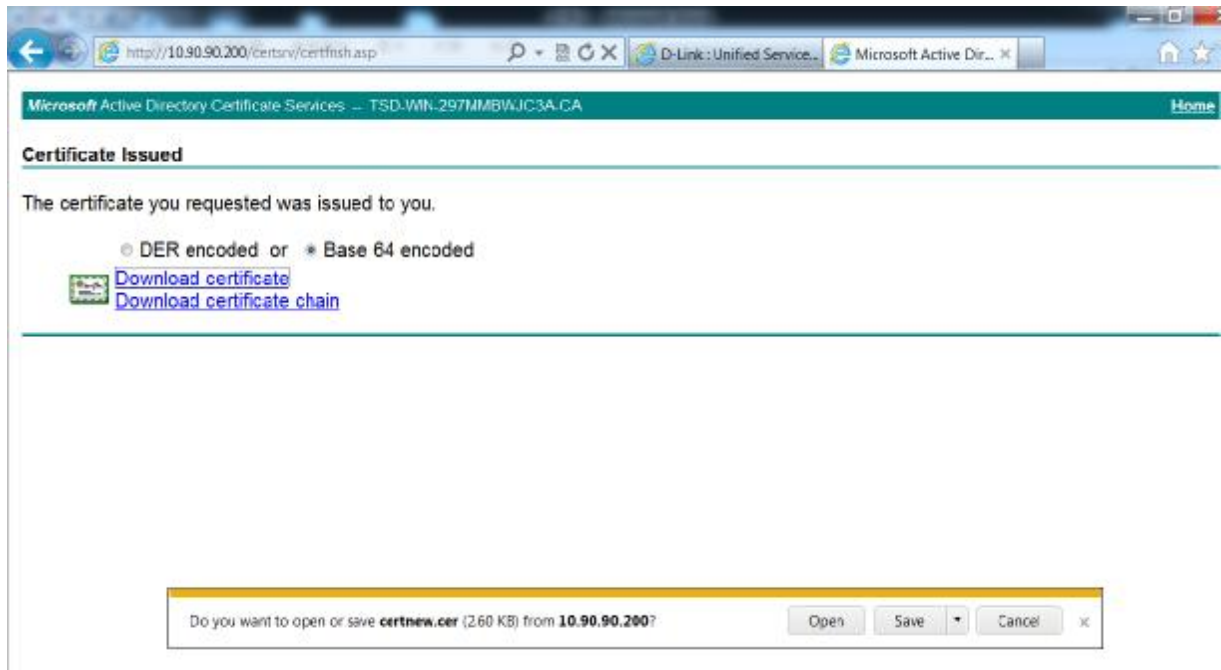
7. Choose 'Submit a certificate



8. Paste the copied encrypted data in the Saved Request field, choose certificate template(depend on your purpose) and press 'Submit'

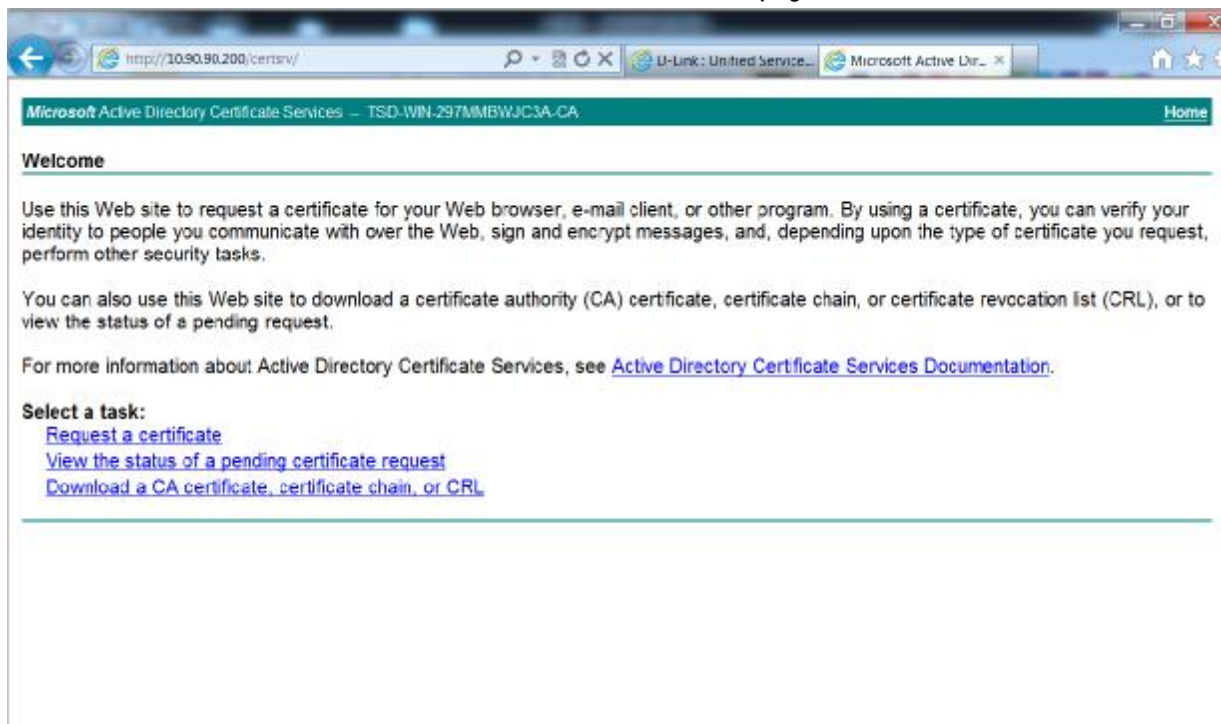


9. Choose the Base 64 encoded(DSR only supports Base 64 format), and click 'Download certificate'



The screenshot shows a web browser window with the address bar displaying <http://10.90.90.200/certsrv/certifish.asp>. The page title is "Microsoft Active Directory Certificate Services - TSD-WIN-297MMBWJC3A-CA". The main content area is titled "Certificate Issued" and contains the text: "The certificate you requested was issued to you." Below this text, there are two radio buttons: "DER encoded" (unselected) and "Base 64 encoded" (selected). Underneath, there are two blue links: "Download certificate" and "Download certificate chain". At the bottom of the browser window, a yellow download dialog box is open, asking "Do you want to open or save certnew.cer (2.60 KB) from 10.90.90.200?". The dialog box has "Open", "Save", and "Cancel" buttons.

10. Download a CA certificate from the certificate service Home page



The screenshot shows the Microsoft Active Directory Certificate Services Home page. The address bar displays <http://10.90.90.200/certsrv/>. The page title is "Microsoft Active Directory Certificate Services - TSD-WIN-297MMBWJC3A-CA". The main content area is titled "Welcome" and contains the following text: "Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks." Below this, it says: "You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request." At the bottom, it says: "For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#)." Under the heading "Select a task:", there are three blue links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

11. Press Upload button on Trusted Certificate field

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_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 ▾

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="button" value="Upload"/> <input type="button" value="Delete"/>			

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input type="button" value="Upload"/> <input type="button" value="Delete"/>					

Self Certificate Requests

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

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...](#)

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_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 ▾

CERTIFICATES LOGOUT

This page allows user to upload a trusted certificate to the router.

Upload Trusted Certificate

Certificate File: C:\Users\Administrator\Desktop\D-Track C:

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

UNIFIED SERVICES ROUTER

12. Press Upload button on Active Self Certificate field

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_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

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, Thawite 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 checked="" type="checkbox"/>	DC=local, DC=dlink, DC=TSD, CN=TSD-WIN-297MMBWJCSA-CA	DC=local, DC=dlink, DC=TSD, CN=TSD-WIN-297MMBWJCSA-CA	Aug 11 10:05:50 2015 GMT

Upload Delete

Active Self Certificates

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

Upload Delete

Self Certificate Requests

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...

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B74_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

CERTIFICATES LOGOUT

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

Upload Active Self Certificate

Certificate File: C:\Users\Administrator\Desktop\certnew_te [Browse]

Upload

Helpful Hints...
Please locate the certificate on your secondary storage of your computer and press Upload.
More...

13. You should see both CA certificate and Self certificate on the list.

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

Added Active Self 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"/>	DC=local, DC=dlink, DC=TSD, CN=TSD-WIN-297MMBWJC3A-CA	DC=local, DC=dlink, DC=TSD, CN=TSD-WIN-297MMBWJC3A-CA	Aug 11 10:05:50 2015 GMT

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input type="checkbox"/>		C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DIR1000N	61:5c:96:95:00:00:00:00:25	DC=local, DC=dlink, DC=TSD, CN=TSD-WIN-297MMBWJC3A-CA	Oct 5 04:03:00 2013 GMT

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...](#)

End of Document