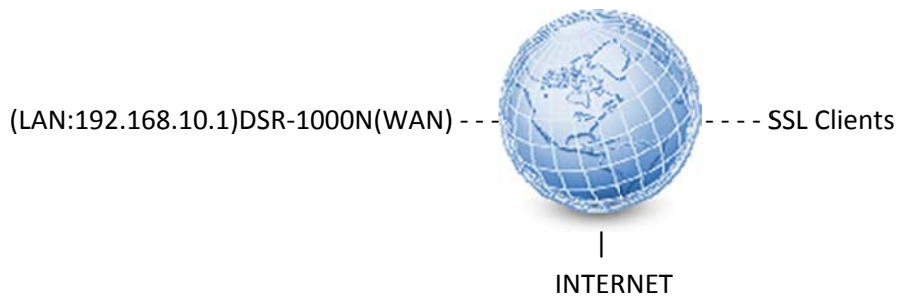


# SSL VPN Split Tunnel



Here we are trying to build a SSL VPN server on the DSR-1000N for users who are able to remotely connect into the resource of a company network.

In this scenario the traffic of the SSL client sending data to 192.168.10.0/24 will be forwarded via SSL VPN tunnel. Normal internet traffic will be sent through their local ISP, this setup is called “split tunnel” in VPN terminology.

## DSR-1000N Setup

**Step 1)** Go to SETUP > VPN Settings > SSL VPN server > Portal Layouts.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B50

**D-Link**

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard	<b>INTERNET CONNECTION</b> LOGOUT				<b>Helpful Hints...</b> If you are new to networking and have never configured a router before, click on Internet Connection Setup Wizard and the router will run you through a few simple steps to get your network up and running. If you consider yourself an Advanced user and have configured a router before, click Manual Internet Connection Setup to input all the settings manually. <a href="#">More...</a>
Internet Settings	This page will guide you through common configuration tasks such as changing the password, timezone and setting up of your internet connection.				
Wireless Settings	<b>Internet Connection Setup Wizard</b>				
Network Settings	IPsec	our easy to use Web-based Wizards to assist you in connecting your new D-Link internet, click on the button below.		<input type="button" value="Internet Connection Setup Wizard"/>	
DMZ Setup	PPTP				
VPN Settings	L2TP				
USB Settings	SSL VPN Server	Portal Layouts	are you have followed all steps outlined in the Quick		
VLAN Settings	SSL VPN Client	SSL VPN Policies			
	Manual Internet Con	Resources			
	If you would like to config the button below.	Port forwarding	your new D-Link Systems Router manually, then click on		

Step 2) Click "Add" to add a Portal.

**PORTAL LAYOUTS** LOGOUT

The table lists the SSL portal layouts configured for this device and allows several operations on the portal layouts.

**List of of Layouts**

<input type="checkbox"/>	Layout Name	Use Count	Portal URL
<input type="checkbox"/>	SSLVPN*	1	https://0.0.0.0/portal/SSLVPN
<input type="checkbox"/>	fortest	1	https://0.0.0.0/portal/fortest
<input type="checkbox"/>	test2	1	https://0.0.0.0/portal/test2

Under Portal configuration enter information into the following:

- Portal Layout Name: Enter in a name for the Portal
- Portal Site Title: Enter in a Title, this can be left blank
- Banner Message: Enter in a Message, this can be left blank

Next make sure all of the boxes have been selected then click "Save Settings".

**PORTAL LAYOUT CONFIGURATION** LOGOUT

This page allows you to add a new portal layout or edit the configuration of an existing portal layout. The details will then be displayed in the List of Portal Layouts table on the SSL VPN Server > Portal Layouts page under the VPN menu.

**Portal Layout and Theme Name**

**Portal Layout Name:**

**Portal Site Title (Optional) :**

**Banner Title (Optional) :**

**Banner Message (Optional) :**

**Display banner message on login page:**

**HTTP meta tags for cache control (recommended):**

**ActiveX web cache cleaner:**

**SSL VPN Portal Pages to Display**

**VPN Tunnel page:**

**Port Forwarding:**

Step 3) Go to ADVANCE > Users > Domains.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01650

# D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▾

Website Filter ▾ APPLICATION RULES LOGOUT

Firewall Settings ▾

Wireless Settings ▾

Advanced Network ▾

Routing ▾

Certificates

Users ▾ Get Users DB

IP/MAC Binding Domains

IPv6 ▾ Groups

Radius Settings Users

Power Saving

**APPLICATION RULES** LOGOUT

The table lists all the available port triggering rules and allows several operations on the rules.

**List of Available Application Rules**

<input type="checkbox"/>	Name	Enable	Protocol	Interface	Outgoing Ports		Incoming Ports	
					Start Port	End Port	Start Port	End Port
<input type="checkbox"/>								

Edit Delete Add

**Helpful Hints...**

Application rules are also referred to as port forwarding rules. Devices on the LAN or DMZ can send a request to the Internet along one of the defined outgoing ports, and then the configured rule will open the corresponding incoming port for the specified type of traffic coming from the WAN.

Note that port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.

More...

Click "Add" to create a domain object.

## DOMAINS LOGOUT

This page shows the list of added domains to the router. The user can add, delete and edit the domains also.

**List of Domains**

<input type="checkbox"/>	Domain Name	Authentication Type	Portal Layout Name
<input type="checkbox"/>	SSLVPN *	Local User Database	SSLVPN
<input type="checkbox"/>	fortest	Local User Database	fortest
<input type="checkbox"/>	fortest2	Local User Database	test2

Edit Delete Add

Under Domain enter in the following:

- Domain Name: Enter in a name for the Domain
- Authentication Type: Select Local User Database
- Select Portal: Select the name of the Portal that was added before
- Time out: Set to 360

Click **“Save Settings”** once done.

**DOMAINS** LOGOUT

This page allows a user to add a new domain.

---

**Domains Configuration**

<b>Domain Name:</b>	<input type="text" value="Domain_for_test_custom_portal"/>
<b>Authentication Type:</b>	<input style="border: 1px solid #ccc;" type="text" value="Local User Database"/>
<b>Select Portal:</b>	<input style="border: 1px solid #ccc;" type="text" value="test_custom_portal"/>
<b>Authentication Server 1:</b>	<input type="text"/>
<b>Authentication Server 2:</b>	<input type="text"/> (Optional)
<b>Authentication Server 3:</b>	<input type="text"/> (Optional)
<b>Timeout:</b>	<input type="text" value="360"/> (Seconds)
<b>Retries:</b>	<input type="text" value="5"/>
<b>Authentication Secret:</b>	<input type="text"/>
<b>Authentication Secret2:</b>	<input type="text"/>
<b>Workgroup:</b>	<input type="text"/>
<b>Second Workgroup:</b>	<input type="text"/> (Optional)
<b>LDAP Base DN:</b>	<input type="text"/>
<b>Second LDAP Base DN</b>	<input type="text"/> (Optional)
<b>Active Directory Domain:</b>	<input type="text"/>
<b>Second Active Directory Domain</b>	<input type="text"/> (Optional)

Step 4) Go to ADVANCED > Users > Users

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B50

# 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 Power Saving

## USERS LOGOUT

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

### List of Users

<input type="checkbox"/>	User Name	Group	Type	Authentication Domain	Login Status
<input type="checkbox"/>	admin *	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	Get Users DB	VPN	Guest	Local User Database	Disabled
<input type="checkbox"/>	Domains	VPN	Local User	Local User Database	Enabled (LAN and WAN)

Logn Policies Policies By Browsers Policies By IP

Helpful Hints... Authentication of the users (IPsec, SSL VPN, or GUI) is done by the router using either a local database on the router or external authentication servers (i.e. LDAP or RADIUS). User level policies can be specified by browser, IP address of the host, and whether the user can login to the router's GUI in addition to the SSL VPN portal. More...

Click on "Add"

## USERS LOGOUT

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

### List of Users

<input type="checkbox"/>	User Name	Group	Type	Authentication Domain	Login Status
<input type="checkbox"/>	admin *	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	guest *	SSLVPN	Guest	Local User Database	Disabled
<input type="checkbox"/>	test1	fortest	SSL VPN User	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	dlink	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	test2	fortest2	SSL VPN User	Local User Database	Enabled (LAN and WAN)

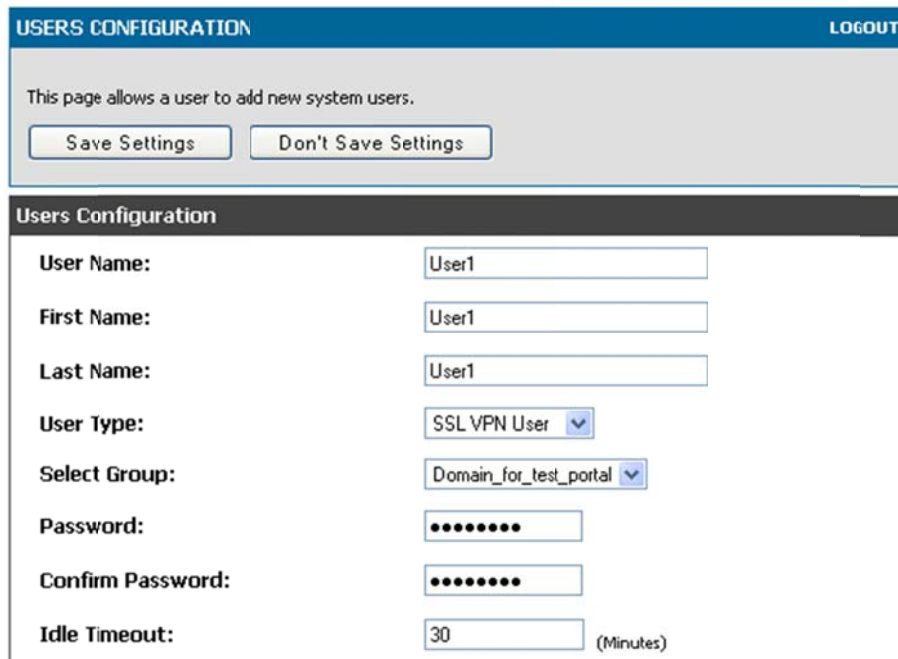
Edit Delete Add

Login Policies Policies By Browsers Policies By IP

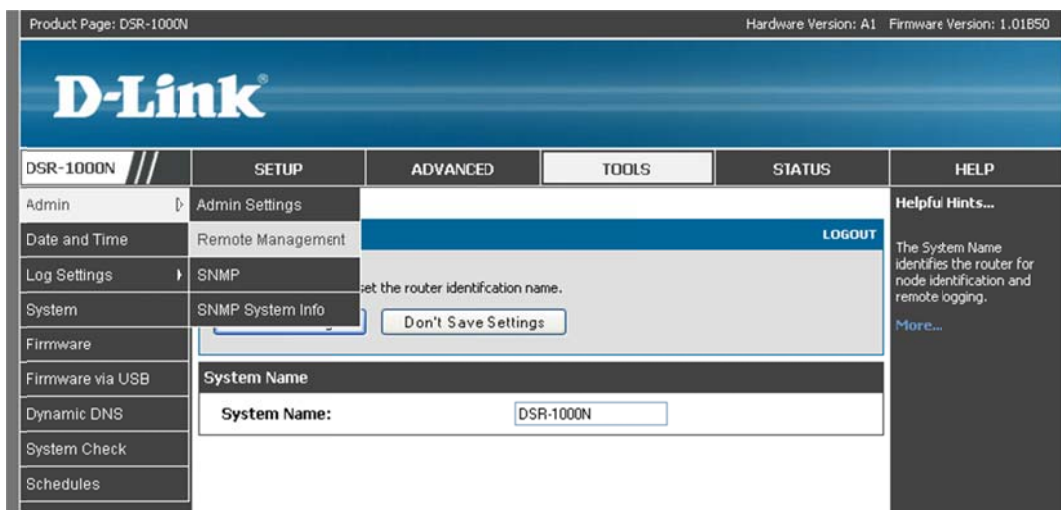
Under User Configuration enter in the following:

- User Name: A name for the use(this is used when the user logs in).
- First Name: First name of user
- Last Name: The last name
- User Type: Leave as is (SSL VPN User)
- Select Group: Enter in the name of the Portal that was added in step 2.

Once done select **“Save Settings”**



**Step 5)** Go to TOOLS > Admin > Remote Management



Select **“Enable Remote Management”**, then click **“Save Settings”**.

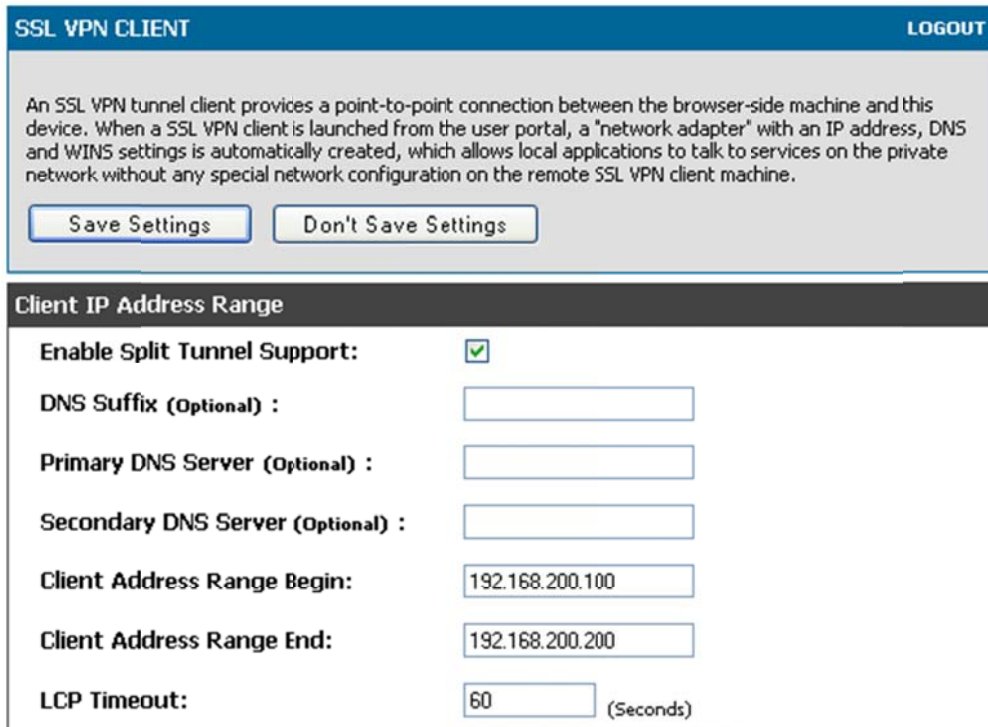
The screenshot shows the 'REMOTE MANAGEMENT' configuration page. At the top, there is a 'LOGOUT' link. Below the title, a text box explains that users can configure remote management from the WAN side. Two buttons, 'Save Settings' and 'Don't Save Settings', are provided. The main configuration area is titled 'Remote Management Enable' and includes the following settings:

- Enable Remote Management:** A checked checkbox.
- Access Type:** A dropdown menu set to 'All IP Addresses'.
- From:** An empty text input field.
- To:** An empty text input field.
- IP Address:** An empty text input field.
- Port Number:** A text input field containing the value '443'.
- Enable Remote SNMP:** An unchecked checkbox.

**Step 6)** Go to **SETUP > VPN Settings > SSL VPN Client > SSL VPN Client**

The screenshot displays the D-Link router's web interface for a DSR-1000N model. The top navigation bar includes 'DSR-1000N', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'VPN Settings' menu is expanded, showing options for 'IPsec', 'PPTP', 'L2TP', 'SSL VPN Server', and 'SSL VPN Client'. The 'SSL VPN Client' option is selected, and its sub-menu is visible, containing 'Manual Internet Connection Setup', 'Configured Client Routes', and 'SSL VPN Client Portal'. The 'Manual Internet Connection Setup' option is highlighted with a button. A 'Helpful Hints...' section on the right provides guidance for new users and advanced users. The D-Link logo is prominently displayed at the top left of the interface.

Select **“Enable Split Tunnel Support”**.



**SSL VPN CLIENT** LOGOUT

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this device. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.

**Client IP Address Range**

**Enable Split Tunnel Support:**

**DNS Suffix (Optional) :**

**Primary DNS Server (Optional) :**

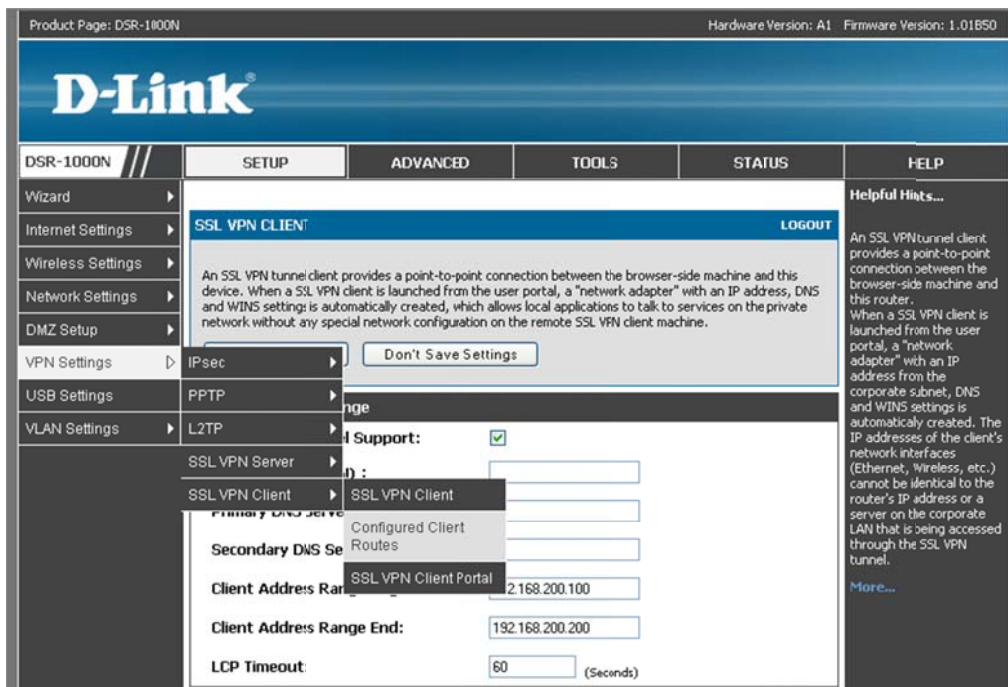
**Secondary DNS Server (Optional) :**

**Client Address Range Begin:**

**Client Address Range End:**

**LCP Timeout:**  (Seconds)

**Step 7)** Go to **ADVANCED > VPN Settings > SSL VPN Client > Configured Client Routes**.



Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01850

**D-Link**

DSR-1000N // **SETUP** **ADVANCED** **TOOLS** **STATUS** **HELP**

Wizard  
Internet Settings  
Wireless Settings  
Network Settings  
DMZ Setup  
VPN Settings > IPsec > **Configured Client Routes**  
USB Settings > PPTP  
VLAN Settings > L2TP

**SSL VPN CLIENT** LOGOUT

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this device. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.

**Enable Split Tunnel Support:**

**DNS Suffix (Optional) :**

**Primary DNS Server (Optional) :**

**Secondary DNS Server (Optional) :**

**Client Address Range Begin:**

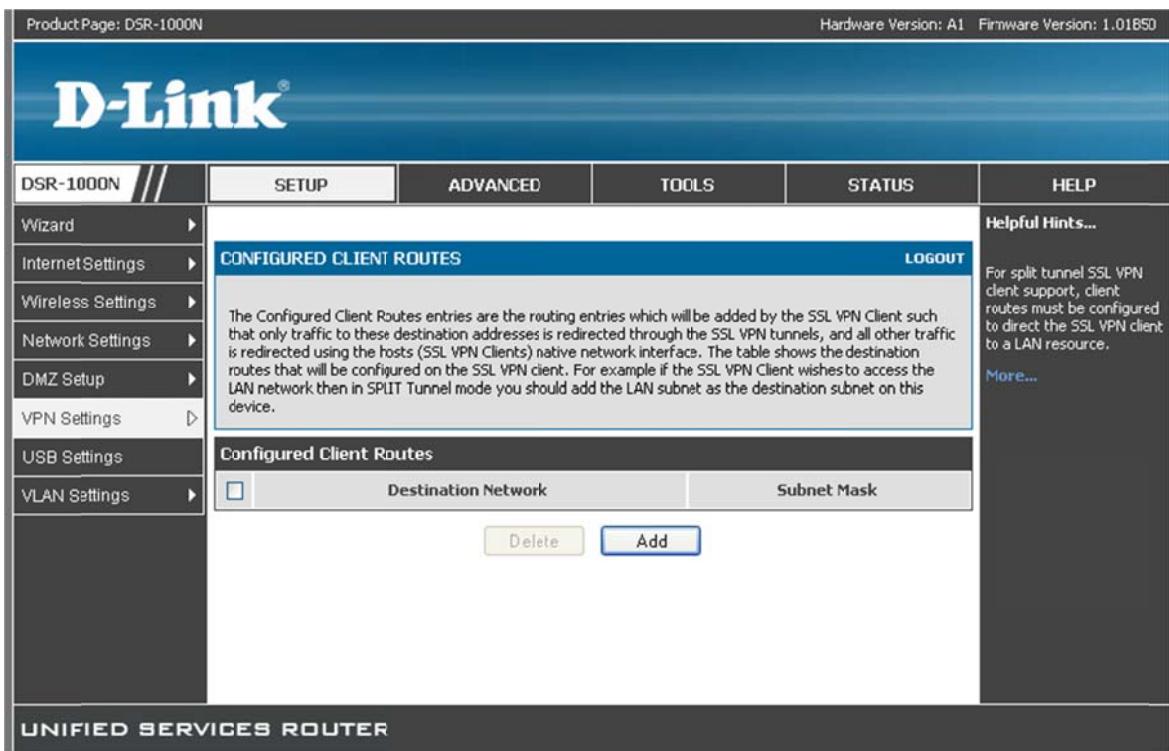
**Client Address Range End:**

**LCP Timeout:**  (Seconds)

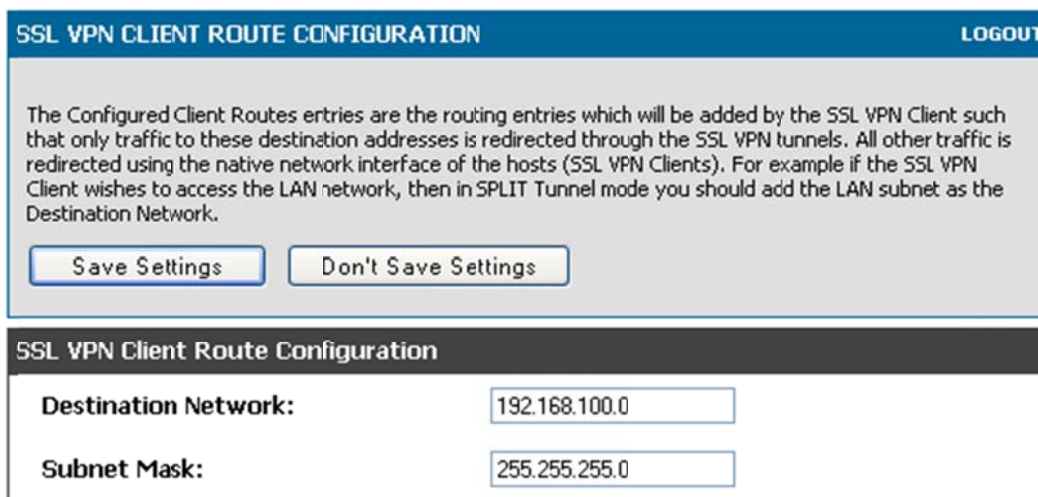
**Helpful Hints...**  
An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this router. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address from the corporate subnet, DNS and WINS settings is automatically created. The IP addresses of the client's network interfaces (Ethernet, Wireless, etc.) cannot be identical to the router's IP address or a server on the corporate LAN that is being accessed through the SSL VPN tunnel.  
[More...](#)



Under Configured Client routes click "Add".



Under Destination Network enter in the LAN network then under Subnet mask the local Subnet.



Once done click "Save Settings", this is the last step on the DSR-1000N.

## Client test / setup.

**Step 1)** Access VPN Settings > SSL VPN Server > Portal Layouts.

The screenshot shows the D-Link web interface for a DSR-1000N router. The top navigation bar includes 'DSR-1000N', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar menu is expanded to 'VPN Settings', which is further expanded to 'SSL VPN Server'. Under 'SSL VPN Server', the 'Portal Layouts' option is selected and highlighted. The main content area shows the 'Internet Connection Setup Wizard' and 'Manual Internet Connection Setup' options. A 'Helpful Hints...' section on the right provides guidance for new users and advanced users.

Under Portal Layouts you will see the entry that you added before, next to it a URL, write down this address.

NOTE: if the IP seen is a private IP (as seen below) you need to find out what the public IP is, the public IP will go in the place of the private IP.

The screenshot shows the 'PORTAL LAYOUTS' section of the D-Link web interface. It includes a 'LOGOUT' button in the top right corner. Below the title, there is a descriptive text: 'The table lists the SSL portal layouts configured for this device and allows several operations on the portal layouts.' Below this is a table titled 'List of of Layouts' with the following data:

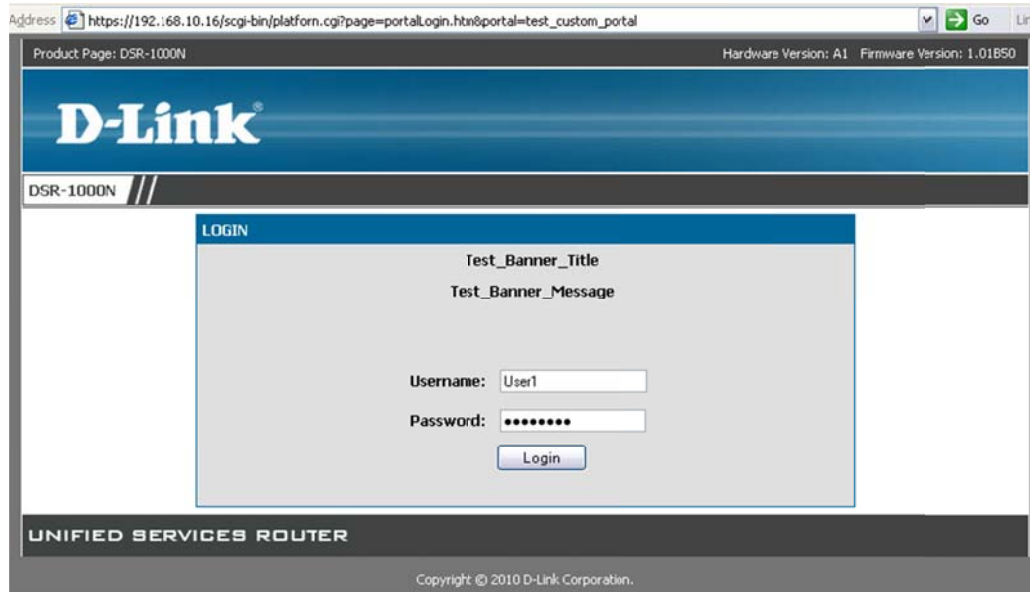
<input type="checkbox"/>	Layout Name	Use Count	Portal URL
<input type="checkbox"/>	SSLVPN*	1	https://192.168.10.16/portal/SSLVPN
<input type="checkbox"/>	test_custom_portal	1	https://192.168.10.16/portal/test_custom_portal

Below the table are four buttons: 'Edit', 'Delete', 'Set Default', and 'Add'.

**Step 2)** From the Client PC enter in the Portal URL (as seen in step 1).

In our example its **https://192.168.10.16/portal/test\_custom\_portal**

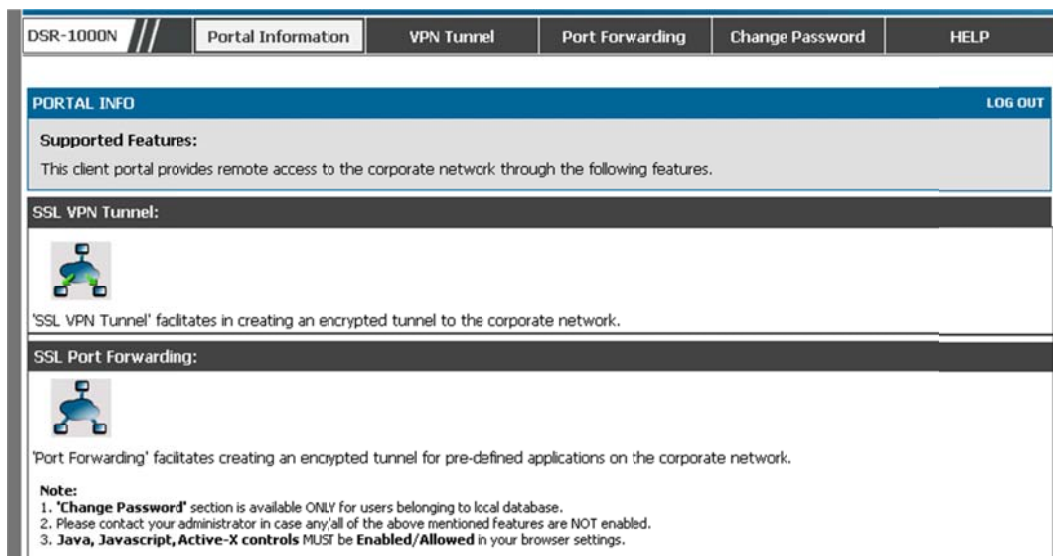
This will bring up a page asking for a Username / password, enter in the Username / Password that you entered in on **page 5** of the guide.



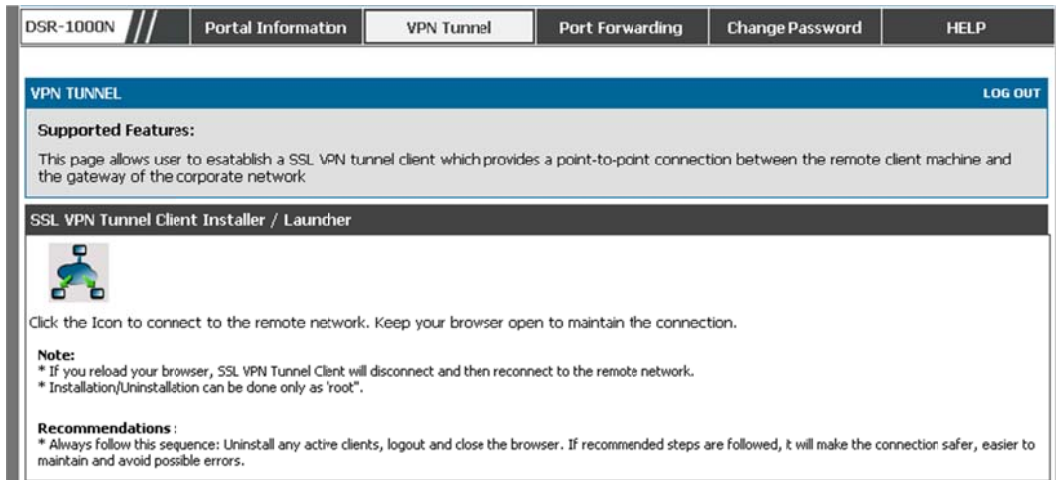
The first page that you will see after logging in explains the different services available.

SSL VPN Tunnel: Used to all full access to the remote site.

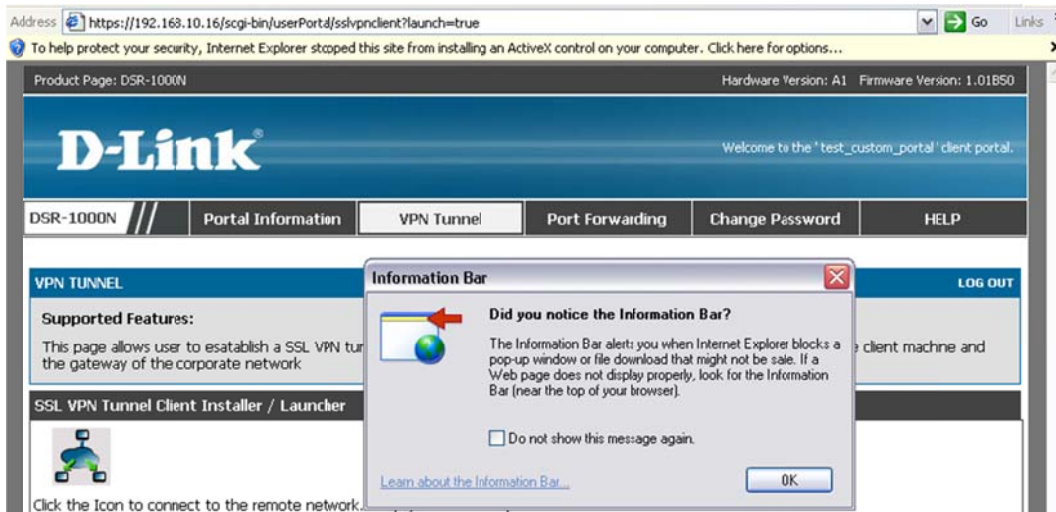
SSL Port Forwarding: Creates a SSL tunnel to the remote site but allow allows access to certain services (set on the DSR-1000N)



**Step 3)** Select VPN Tunnel tab at the top of the page



Then **click** on “SSL VPN Tunnel”, this will pop up a box at the top of the page and a warning (as seen below).



**Click** on “OK” to close the Information bar.

Next **click** on the bar at the top of the page and select “Install ActiveX Control”.



You will see a Security Warning, [Click “OK”](#)



Under Digital Signature Details, [Click “View Certificate”](#)



You should see a new screen (Certificate), Click **“Install Certificate”** (found at the bottom of the pop up).



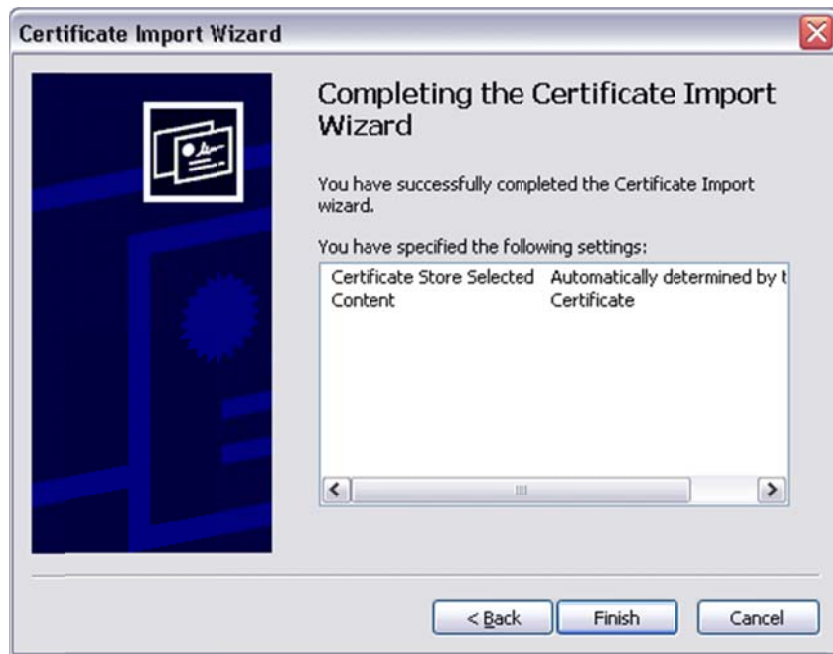
Step 4) You should now see the **“Certificate Import Wizard”**, Click **“Next”**.



Leave the top option selected then **Click “Next”**.



Then **Click “Finish”**.



Click “Yes” on the Security Warning.



Then Click “OK”

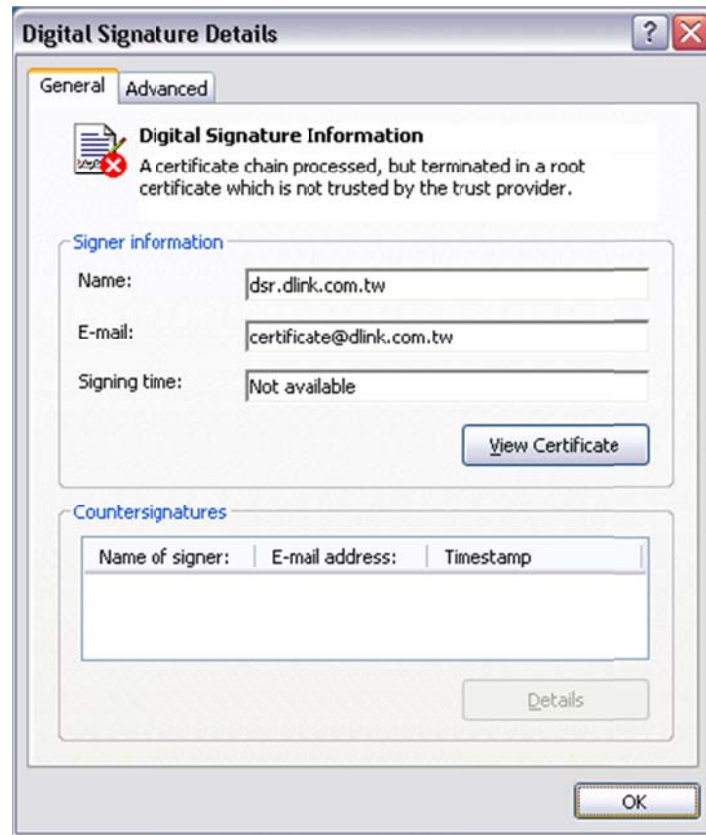


You need to Click on “Install Certificate” a seconds time.





Once done **Click “OK”**.



If you get a Security Warning **Click on “OK”**



Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B50

---

D-Link Welcome to the "test\_custom\_portal" client portal.

---


DSR-1000N // 
 Portal Information
VPN Tunnel
Port Forwarding
Change Password
HELP

---

VPN TUNNEL
LOG OUT

**Supported Features:**  
 This page allows user to establish a SSL VPN tunnel client which provides a point-to-point connection between the remote client machine and the gateway of the corporate network.

**SSL VPN Tunnel Client Installer / Launcher**



Click the Icon to connect to the remote network. Keep your browser open to maintain the connection.

**Note:**  
 \* If you reload your browser, SSL VPN Tunnel Client will disconnect and then reconnect to the remote network.  
 \* Installation/Uninstallation can be done only as "root".

**Recommendations :**  
 \* Always follow this sequence: Uninstall any activeclients, logout and close the browser. If recommended steps are followed, it will make the connection safer, easier to maintain and avoid possible errors.

**UNIFIED SERVICES ROUTER**

Copyright © 2010 D-Link Corporation.

**D-link-SSLVPN-Tunnel:Connection Status**
X


 Uninstall On Browser Exit

**Connection**

Status	Connected
Duration	00:00:51

**Interfaces**

IP Address	192.168.200.101
Server IP	192.168.10.16

**Activity**

Bytes Sent	4366
Bytes Received	578

**Status Message**


D-link-SSLVPN-Tunnel:Connected

Disconnect
Close

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\TechLaptop>ping 192.168.100.5

Pinging 192.168.100.5 with 32 bytes of data:

Reply from 192.168.100.5: bytes=32 time=2ms TTL=64
Reply from 192.168.100.5: bytes=32 time=1ms TTL=64
Reply from 192.168.100.5: bytes=32 time=1ms TTL=64
Reply from 192.168.100.5: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\TechLaptop>_
```

## Port forward

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B50


**D-Link** Welcome to the 'test\_custom\_portal' client portal.

DSR-1000N // Portal Information VPN Tunnel **Port Forwarding** Change Password HELP

**PORT FORWARDING** LOG OUT

**Supported Features:**  
This page allows user to establish a Port Forwarding tunnel which is a light weight tunnel with port based encryption.

**SSL VPN Port Forwarding Client Installer / Launcher**



Click the Icon to connect to the remote servers.

**Note:**  
\* The active connections can still persist even when browser is closed without uninstalling the Port Forwarding client

**Recommendations :**  
\* Always follow this sequence: Uninstall any active clients, logout and close the browser. If recommended steps are followed, it will make the connection safer, easier to maintain and avoid possible errors.

Address <https://192.168.10.16/cgi-bin/userPortal/portforwarding?launch=true> Go Links

This site might require the following ActiveX control: 'MenloLSP.cab' from 'dsr.dlink.com.tw'. Click here to install...

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B50

# D-Link


Welcome to the 'test\_custom\_portal' client portal.

DSR-1000N // Portal Information VPN Tunnel Port Forwarding Change Password HELP

## PORT FORWARDING

**Supported Features:**  
This page allows user to establish a Port Forwarding...

SSL VPN Port forwarding Client Installer / Lau




Click the Icon to connect to the remote servers.

**Note:**  
\* The active connections can still persist even when browser is closed without uninstalling the Port Forwarding client

**Recommendations :**  
\* Always follow this sequence: Uninstall any active clients, logout and close the browser. If recommended steps are followed, it will make the connection safer, easier to maintain and avoid possible errors.

**Information Bar**



**Did you notice the Information Bar?**

The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser).

Do not show this message again.

[Learn about the Information Bar...](#) OK

## Internet Explorer - Security Warning

**Do you want to install this software?**

 Name: MenloLSP.cab  
Publisher: [dsr.dlink.com.tw](http://dsr.dlink.com.tw)

More options Install Don't Install

 While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. [What's the risk?](#)

