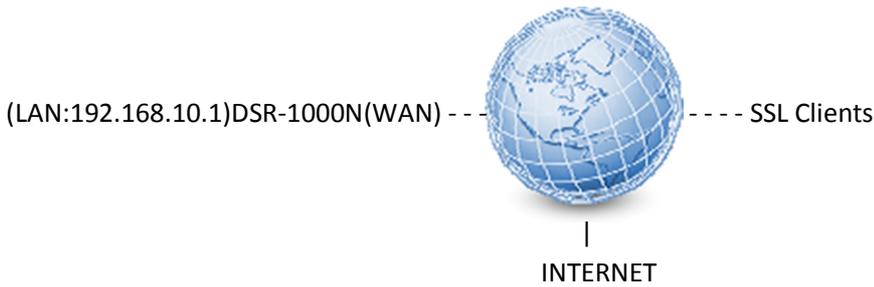


SSL VPN Split Tunnel



Here we're trying to build a SSL VPN server on the DSR-1000N for users are able to remotely connect into the resource of 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	INTERNET CONNECTION LOGOUT				Helpful Hints... 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. More...
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	Internet Connection Setup Wizard				
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.			
DMZ Setup	PPTP	<input type="button" value="Internet Connection Setup Wizard"/>			
VPN Settings	L2TP	are you have followed all steps outlined in the Quick			
USB Settings	SSL VPN Server	Portal Layouts			
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		
	<input type="button" value="Manual Internet Connection Setup"/>				

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 in 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.

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

IPsec ▾

Mobile Settings

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

	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 listening 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

	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

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

Step 4) Go to ADVANCED > Users > Users

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

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

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)

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.

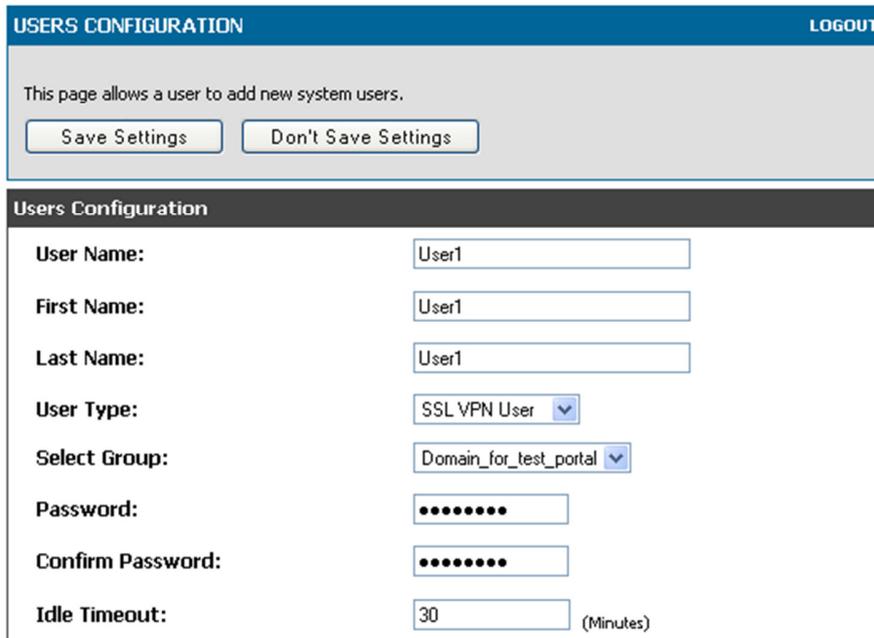
List of Users

<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)

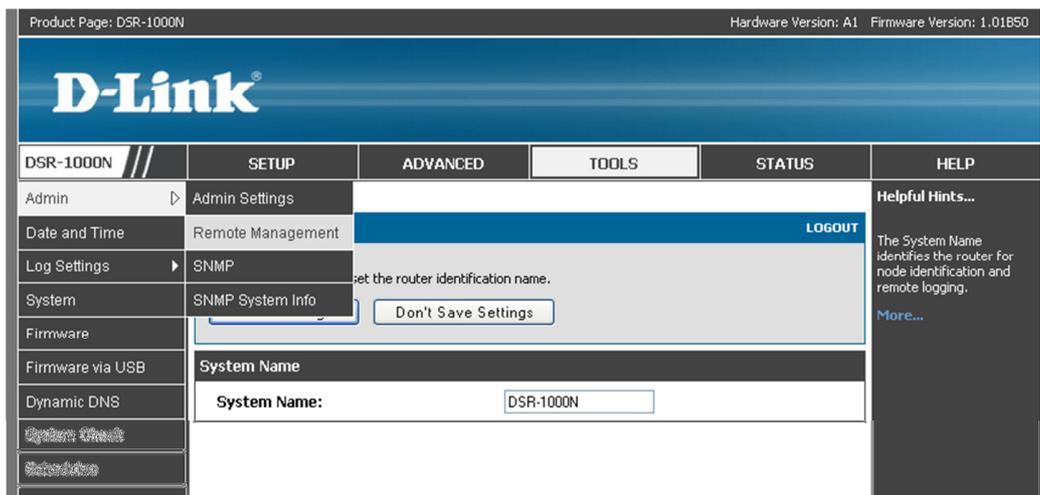
Under User Configuration enter in the following:

- 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”**.

REMOTE MANAGEMENT LOGOUT

From this page a user can configure the remote management feature. This feature can be used to manage the box remotely from WAN side.

Remote Management Enable

Enable Remote Management:

Access Type: All IP Addresses

From:

To:

IP Address:

Port Number: 443

Enable Remote SNMP:

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

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

USB Settings

VLAN Settings

Internet Connection Setup Wizard

IPsec

PPTP

L2TP

SSL VPN Server

SSL VPN Client

Manual Internet Connection Setup

Configured Client Routes

SSL VPN Client Portal

Manual Internet Connection Setup

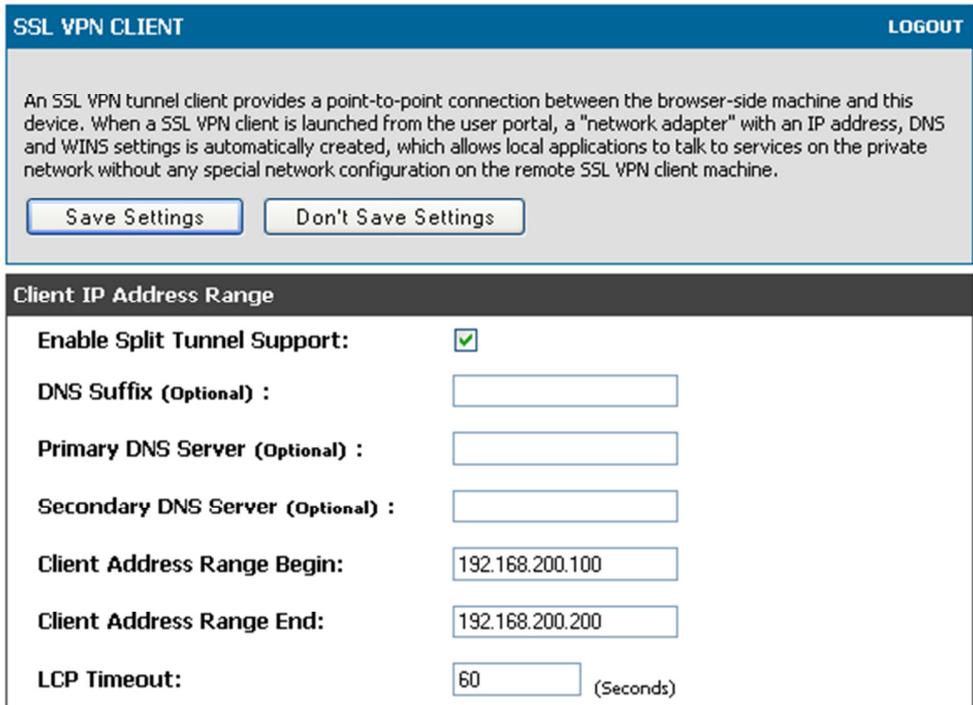
Helpful Hints...

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.

[More...](#)

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) :

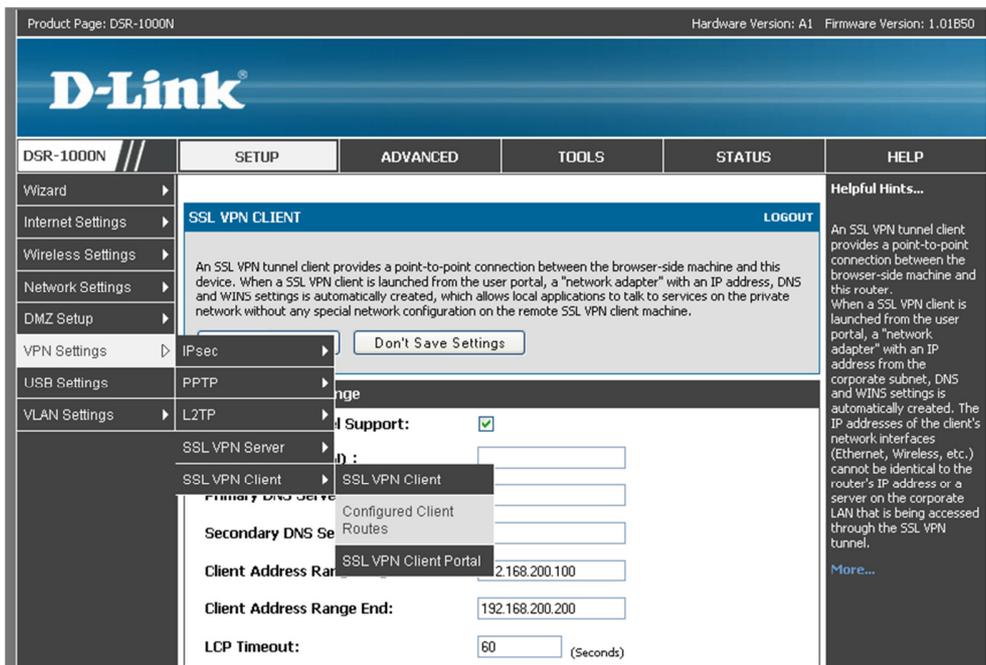
Secondary DNS Server (Optional) :

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: 1.01B50

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".

The screenshot shows the D-Link DSR-1000N web interface. At the top, it displays 'Product Page: DSR-1000N', 'Hardware Version: A1', and 'Firmware Version: 1.01850'. The D-Link logo is prominent. Below the logo is a navigation menu with tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'SETUP' tab is selected, and a sidebar on the left lists various settings like Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled 'CONFIGURED CLIENT ROUTES' and includes a 'LOGOUT' link. A text block explains that these routes are added by the SSL VPN Client and that traffic to these destinations is redirected through the VPN tunnels. Below this is a table with columns for 'Destination Network' and 'Subnet Mask'. There are 'Delete' and 'Add' buttons below the table. A 'Helpful Hints...' section on the right provides additional information about split tunnel SSL VPN client support.

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

The screenshot shows the 'SSL VPN CLIENT ROUTE CONFIGURATION' dialog box. It has a title bar with 'SSL VPN CLIENT ROUTE CONFIGURATION' and a 'LOGOUT' button. The main text explains that the configured client routes are added by the SSL VPN Client and that traffic to these destinations is redirected through the VPN tunnels. Below the text are two buttons: 'Save Settings' and 'Don't Save Settings'. At the bottom, there is a section titled 'SSL VPN Client Route Configuration' with two input fields: 'Destination Network' with the value '192.168.100.0' and 'Subnet Mask' with the value '255.255.255.0'.

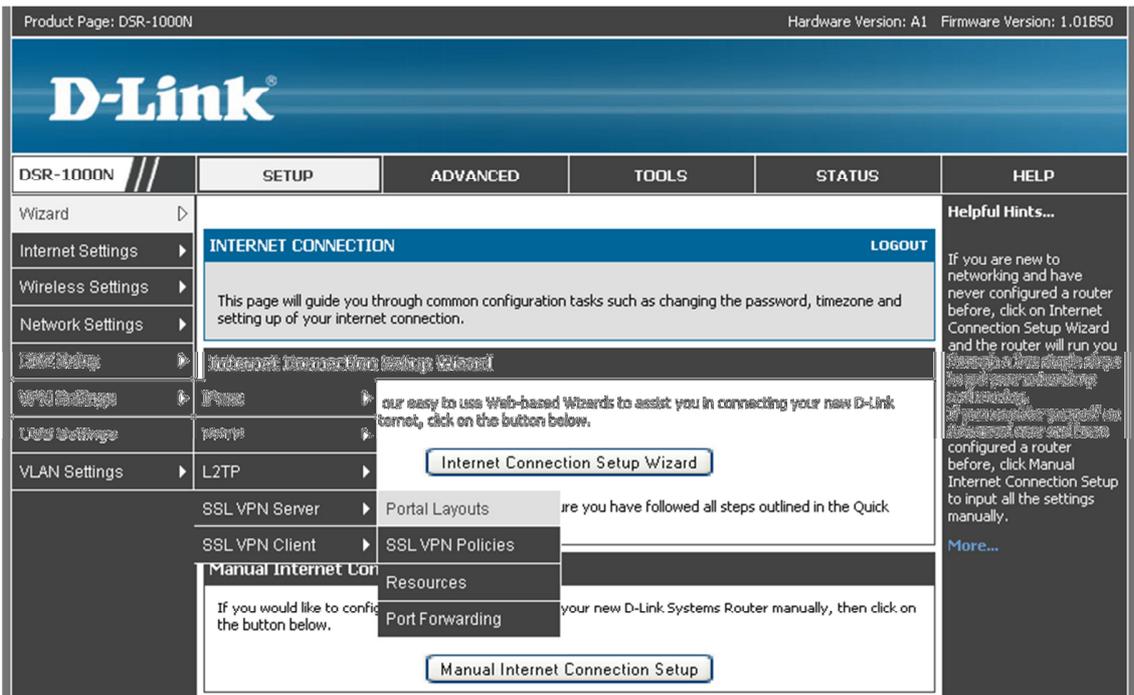
Once done click "Save Settings", this is the last step on the DSR-1000N.

Client test / setup.

NOTE: Windows 7 64bit users please download the below file to allow full support.

http://www.microsoft.com/downloads/en/details.aspx?familyid=90548130-4468-4BBC-9673-D6ACABD5D13B&displaylang=en

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



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.

PORTAL LAYOUTS
LOGOUT

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

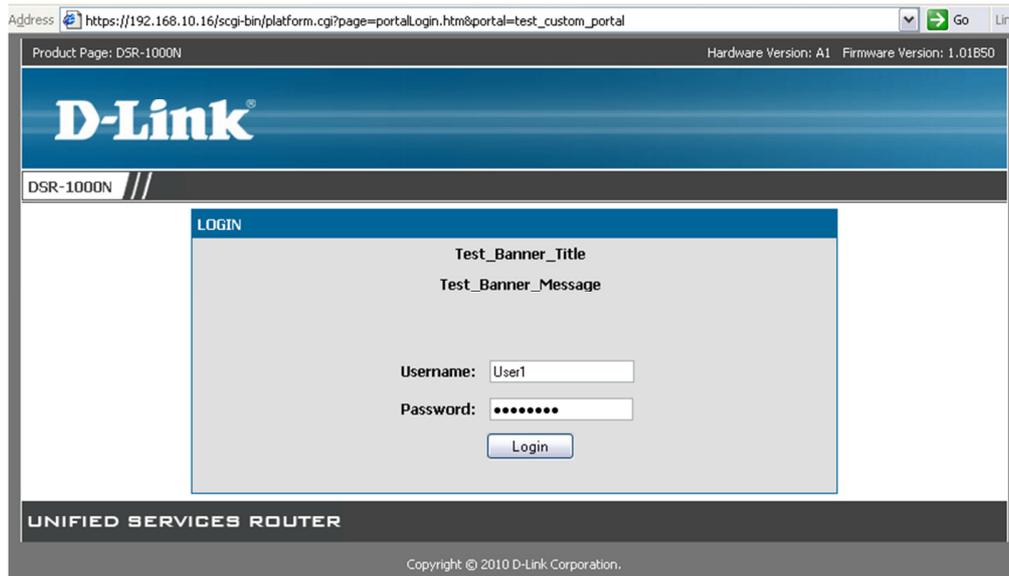
List of of Layouts

	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

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**

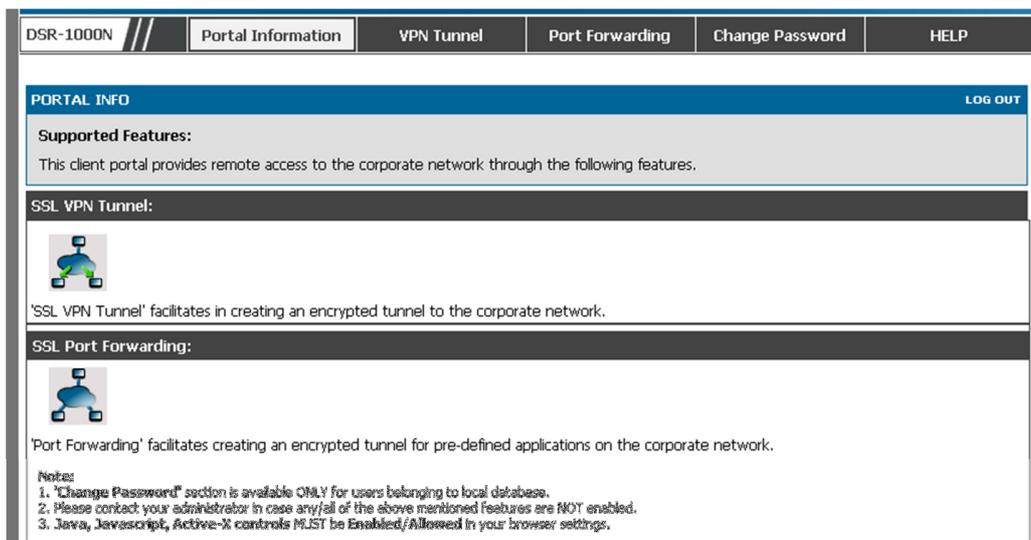
This will bring up a page asking for a Username / password, enter in the Username / Password that you entered in on **page 5** of the guide.



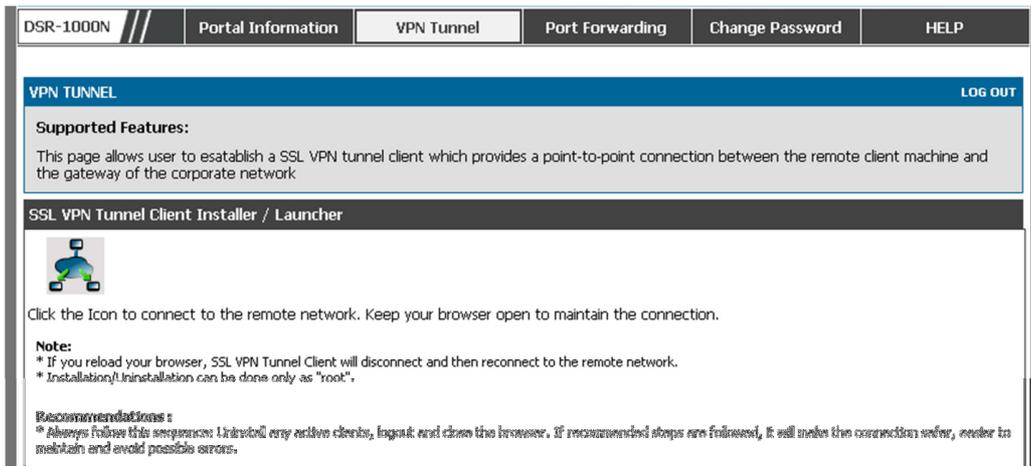
The first page that you will see after logging in explains the different services available.

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

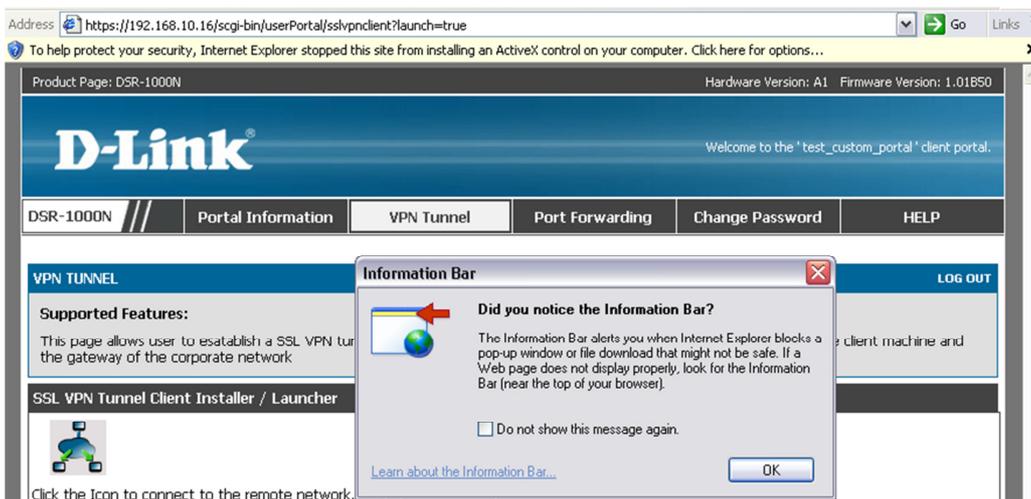
SSL Port Forwarding: Creates a SSL tunnel to the remote site but allow allows access to certain services (set on the DSR-1000N)



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

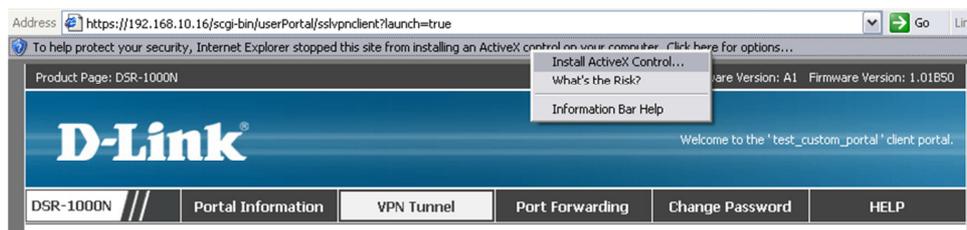


Then **click** on **“SSL VPN Tunnel”**, this will pop up a box at the top of the page and a warning (as seen below).



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

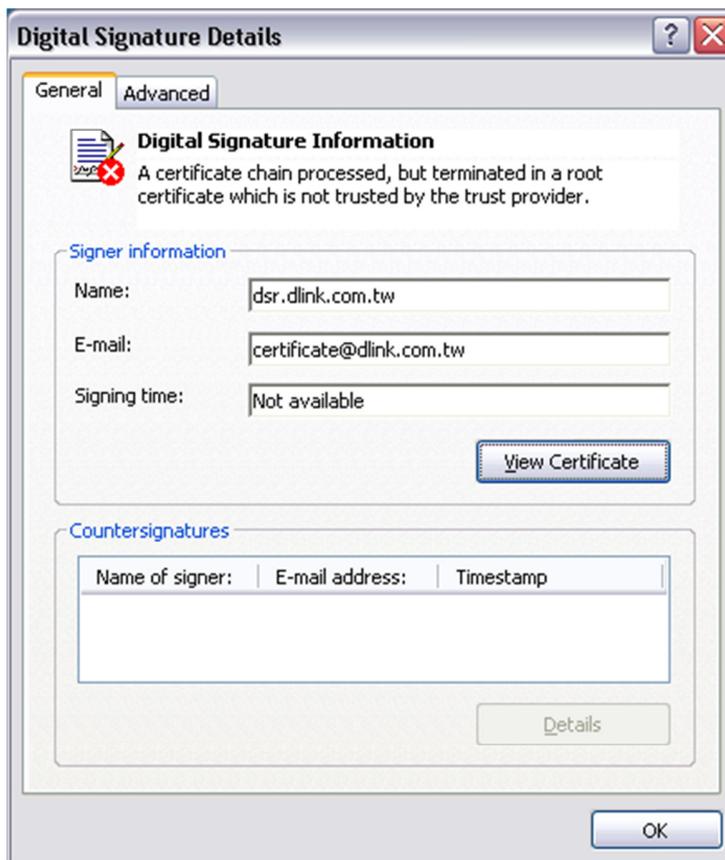
Next **click** on the bar at the top of the page and select **“Install ActiveX Control”**.



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.



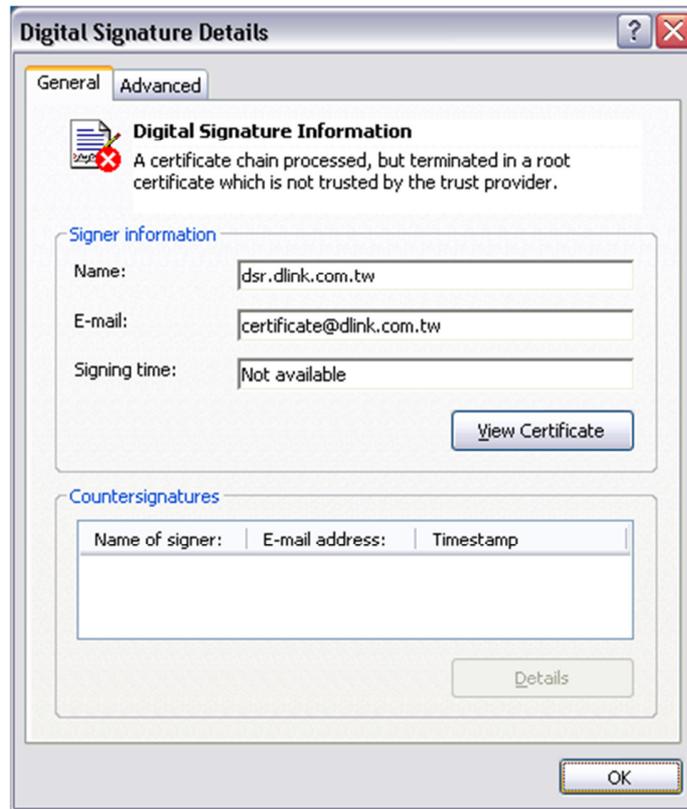
Then Click “OK”



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.

Notes
 * 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 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.

UNIFIED SERVICES ROUTER

Copyright © 2010 D-Link Corporation.

D-link-SSLVPN-Tunnel:Connection Status ✖

 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/scgi-bin/userPortal/portforwarding?launch=true>

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 **LOG OUT**

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

SSL VPN Port Forwarding Client Installer / Lau

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**

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.

Internet Explorer - Security Warning

Do you want to install this software?

Name: MenloLSP.cab
Publisher: 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?](#)

