Home > VPN Settings > Tunnel > Manual

Home	Advanced	Tools	Status	Hel
VPN Setting	s - Tunnel 1			
	Item		Setting	
Tunnel Name				
Aggressive M	ode	Enable		
Local Subnet		0.0.0.0		
Local Netmas	ik.	0.0.0.0		
Remote Subr	et	0.0.0.0		
Remote Netr	lask	0.0.0.0		
Remote Gate	way	0.0.0.0		
Method		MANUAL		
Local SPI		0x 0000		
Remote SPI		0000 x0		
Encapsulatio	n Protocol	ESP 🛩		
Encryption Alg	jorithm	3DES 😽		
Encryption Ke	y a			
(FOI ESP OIII)	y		(for 3DES ONLY)	
100000			(for 3DES ONLY)	
Authentication	Algorithm	NONE 🛩		
Authentication	i Key			
Life Time		0		
Life Time Uni		Second 🐱		

Current tunnel name.
Enabling this mode will accelerate establishing tunnel, but the device will have less security.
The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Local netmask combined with local subnet to form a subnet domain.
The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
The WAN IP address of remote VPN gateway.
The set of rules applied when connecting to the VPN gateway.
The value of the local SPI should be set in hex format.
The value of the remote SPI should be set in hex format.

Home > VPN Settings > Tunnel > Manual Continued...

Home	Advanced	Tools	Status	Hel
VPN Settings	Tunnel 1			
1	Item		Setting	
Tunnel Name				
Aggressive Mod	le	Enable		
Local Subnet		0.0.0.0		
Local Netmask		0.0.0.0		
Remote Subnet		0.0.0.0		
Remote Netma	sk	0.0.0.0		
Remote Gatewa	ay	0.0.0.0		
Method		MANUAL		
Local SPI		0x 0000		
Remote SPI		0x 0000		
Encapsulation I	Protocol	ESP 💌		
Encryption Algo	rithm	3DES 🛰		
Encryption Key (For ESP Only)				
(FOLEOF ONLY)			(for 3DES ONLY)	
1000			(for 3DES ONLY)	
Authentication A	lgorithm	NONE Y		1
Authentication F	(ey			1
Life Time		0		
Life Time Unit		Second 🛩		

Encapsulation Protocol	There are two protocols that can be selected: ESP and AH.
Encryption Algorithm	There are two algorithms that can be selected: 3DES and DES.
Encryption Key	For DES, the encryption key is 8 bytes (16 Char.). For 3DES, the encryption key is 24 bytes (48 Char.).
Authentication Algorithm	There are two algorithms that can be selected: SHA1 and MD5.
Authentication Key	For MD5, the authentication algorithm is16 bytes (32 Char.). For SHA1, the authentication algorithm is 20 bytes.(40 Char.).
Life Time	Enter in the life time value.
Life Time Unit	There are two units that can be selected: Second and KB.

Using the Configuration Menu Home > VPN Settings > Dynamic VPN Tunnel

Ho	me Advance	ed Tools	Status	Help
VPN Se	ttings - Dynamic VPN	Tunnel		
-	Item		Setting	
Tunnel N	lame			
Dynamic	: VPN	🔲 Enable		
Local Su	Ibnet	0.0.0.0		
Local Ne	etmask	0.0.0.0		
Preshan	е Кеу			
IKE Prop	iosal index	Select IKE Propose	al	
IPSec Pr	roposal index	Select IPSec Prop	osal	

VPN Settings - IKE There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: basic setup, IKE proposal setup, and IPSec proposal setup. Basic setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from the previous page of VPN setting. IKE proposal setup includes the setting of a set of frequent-used IKE proposals and selecting from the set of IKE proposals.

Tunnel Name Current tunnel name.

Dynamic VPN This feature works with a VPN software client so the DI-824VUP does not need to know the IP address of the remote clients.

Aggressive Mode Enabling this mode will accelerate establishing the tunnel, but the device will have less security.

Local Subnet The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.

Local Netmask The netmask of the VPN gateway's local network.

Home > VPN Settings > Dynamic VPN Tunnel Continued...

Home	Advanced	Tools	Status	Hel
VPN Settings -	Dynamic VPN Tunn	el		
	Item		Setting	
Tunnel Name	[
Dynamic VPN		🔲 Enable		
Local Subnet	[0.0.0		
Local Netmask	[0.0.0.0		
Preshare Key	[
IKE Proposal in	dex (Select IKE Propos	al	
IPSec Proposal	index	Select IPSec Pro	oosal	

Preshared Key The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be the same for both endpoint gateways.

IKE Proposal index Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the dedicated tunnel.

IPSec ProposalClick the button to setup a set of frequent-used IPSec
proposals and select from the set of IKE proposals for the
dedicated tunnel.

Using the Configuration Menu Home > VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal

D-Link Building Networks for People	High-Speed 2.4GHz Wireless Router
DI-824VUP	Home Advanced Tools Status Help
R	VPN Settings - Dynamic VPN Tunnel - Set IKE Proposal
- Contraction of the second	Item Setting
Wizard	- Empty -
	Remove
Wireless	ID Proposal Name DH Group Encrypt algorithm Auth algorithm Life Time Life Time Unit
WAN	1 Group 1 V 3DES V SHA1 V 0 Sec. V
(management	3 Group 1 V 3DES V SHA1 V 0 Sec. V
LAN	4 Group 1 💙 3DES 💙 SHA1 💙 0 Sec. 💙
DHCP	5 Group 1 V 3DES V SHA1 V 0 Sec. V
Constant of the second	6 Group 1 V 3DES V SHA1 V 0 Sec. V
VPN	7 Group 1 V 3DES V SHA1 V U Sec. V
	9 Group 1 V 3DES V SHA1 V 0 Sec. V
	10 Group 1 V 3DES V SHA1 V 0 Sec. V
	Proposal ID select one 💙 🛛 Add to 🕽 Proposal index
	G Ø 20 C Back Apply Cancel Help
IKE Proposal index	A list of selected proposal indexes from the IKE propose pool listed below.
Proposal Name	It indicates which IKE proposal to be focused.
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encrypt algorithm	There are two algorithms that can be selected: 3DES an DES.
Auth algorithm	There are two algorithms that can be selected: SHA1 an MD5.

Home > VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal Continued...

Home	Advanced	l Tools	Stat	us	Help
VPN Settings	s - Dynamic VPN Tu	nnel - Set IKE F	Proposal		
	ltem		Setting	1	
IKE Proposal i	index	- Empty -			
		6	Remove		
			(emove		
ID Proposal N	Name DH Group E	ncrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	Group 1 🛩	3DES 🛩	SHA1 💌	0	Sec. 🛩
2	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
3	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
4	Group 1 💌	3DES 💙	SHA1 💌	0	Sec. 💌
5	Group 1 💌	3DES 🛩	SHA1 🗸	0	Sec. 🛩
6	Group 1 💌	3DES 💙	SHA1 💌	0	Sec. 💙
7	Group 1 💌	3DES 👻	SHA1 🔽	0	Sec. 💙
8	Group 1 💌	3DES 🗸	SHA1 💌	0	Sec. 💙
9	Group 1 💌	3DES 🛩	SHA1 💌	0	Sec. 💙
10	Group 1 💌	3DES 💙	SHA1 🛩	0	Sec. 🗸
10	Group 1 💌	3DES 🛩	SHA1 💌	0	Sec. 💙

Life TimeEnter in the life time value.Life Time UnitThere are two units that can be selected: second and KB.Proposal IDThe identifier of IKE proposal can be chosen for adding the
corresponding proposal to the dedicated tunnel.Add toClick it to add the chosen proposal indicated by proposal ID
to IKE Proposal index list.

Home > VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal

Home	Advanc	ed	Tools	Statu		Hel
VPN Setting	s - Dynamic VPN	l Tunnel -	Set IPSEC Pr	oposal		
	Item			Setting		
IPSec Propos	ai index	- Em	Remo	ve		
ID Proposal Name	DH Group	Encap protocol	Encrypt	Auth algorithm	Life Time	Life Tir Unit
1	None 💌	ESP 💌	3DES 🗸	None 💌	0	Sec.
2	None 🗸	ESP 🗸	3DES 🗸	None 💌	0	Sec.
3	None 💙	ESP 💌	3DES 💌	None 💌	0	Sec.
4	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.
5	None 💌	ESP 💌	3DES 🐱	None 💌	0	Sec.
6	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.
7	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.
8	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.
9	None 👻	ESP 🐱	3DES 🐱	None 💌	0	Sec.
10	None 💌	ESP 💌	3DES 💙	None 💌	0	Sec.
	Proposal ID	select on	e 💉 🗛 Add to	Proposal ind	lex	

IPSec Proposal index	A list of selected proposal indexes from the IPSec proposal pool listed below.
Proposal Name	This is the name used to classify the IPSec proposal.
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encap protocol	There are two protocols that can be selected: ESP and AH.
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are two algorithms that can be selected: SHA1 and MD5.

Home > VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal Continued...

Home	Advan	ced	Tools	Statu	5	Help
VPN Setting	s - Dynamic VP	N Tunnel -	Set IPSEC P	roposal		
	Item			Setting		
IPSec Propos	al index	- Emj	pty -			
1			Remo	ve		
		<u>r</u>				
ID Proposal	DH Group	Encap	Encrypt	Auth	Life	Life Tim
1	None 🗸	ESP 🗸	3DES 🗸	None V	0	Sec.
2	None	ESP 🗸	3DES 💙	None 💙	0	Sec.
3	None 👻	ESP 🛩	3DES 💌	None 💌	0	Sec.
4	None	ESP 💌	3DES 💌	None 💌	0	Sec.
5	None	ESP 💌	3DES 🛩	None 💌	0	Sec.
6	None	ESP 🛩	3DES 🛩	None 💙	0	Sec.
7	None	ESP 💌	3DES 💌	None 🔽	0	Sec.
8	None	ESP 💌	3DES 💌	None 💌	0	Sec.
9	None 🗸	ESP 🛩	3DES 🛩	None 👻	0	Sec.
			0050	Mana in	0	Sec S

Life Time Enter in a life time value.

Life Time Unit There are two units that can be selected: second and KB.

Proposal ID The identifier of IPSec proposal can be chosen for adding the corresponding proposal to the dedicated tunnel.

Add to Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list.

Using the Configuration Menu Home > VPN Settings > L2TP Server Setting

Home	Advance	d) Tools) Status	Holp
Home	Auvance	Turna Turna	Status	neip
L2TP Serve	r			
	Item		Setting	
L2TP Server		🗌 Enable		
Virtual IP of L	2TP Server	10 0	.1 .1	
Authenticatio	n Protocol	● PAP ○ CI	HAP OMSCHAP	
		Tunnel Settir	Ig	
Tunnel Name	9			
User Name				
Password				
	12 million		(3) Ø	0 0
			Back Apple	
			васк арріу	Cancel Help
Tunnel Name	UserN	ame Passwo	rd	

Enable L2TP Server	Click to enable the L2TP Server function.
Virtual IP of L2TP Server	Enter your Virtual IP address to access the L2PT server.
Authentication Protocol	Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.
Tunnel Name	Current tunnel name.
User Name	Enter in the username for the L2TP account.
Password	Enter in the password for the L2TP account.

Using the Configuration Menu Home > VPN Settings > PPTP Server Setting

1		night opeca				
Home	Advanced	Tools	St	atus	1	leip
PPTP Server						
t It	em		Se	tting		
PPTP Server		Enable				
Virtual IP of PPTP	Server	100	.0	1		
Authentication Pro	itocol		P OMSC	HAP		
		Tunnel Setting				
Tunnel Name						
User Name						
Password						
			0		52	0
			9	-		U

Click to enable the PPTP Server function.

Enter your Virtual IP address to access the PPPT server.

Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.

Tunnel NameCurrent tunnel name.

Enable PPTP

Virtual IP of PPTP Server

Authentication

Server

Protocol

User Name Enter in the username for the PPTP account.

Password Enter in the password for the PPTP account.

Advanced > Virtual Server

	Home	Advan	iced 📄	Fools S	Status		lelp
	Virtual Server Virtual Server is u	sed to allow i	Internet users	access to LAN ser	vices.		
		O Enable	d ODisable	d			
erver	Name						
<u> </u>	Private IP	192.168.0.					
on	Protocol Type	TCP 💌					
	Private Port						
	Public Port						
	Schedule	O Always					
		O From	Time 00	✓ 00 ✓ To 00 ▲	00 🗸		
			day Sun	🛩 to Sun 🖌			
P					0	63	0
					Apply	Cancel	Help
					Аррту	cancer	пец
	Virtual Server	List					
	Name	CTD.	Private IP	Protocol TOP 31 (31	Schedule		1
1	Virtual Server	HTTP	0.0.0.0	TCP 80 (80	always		
	Virtual Server	HTTPS	0.0.0.0	TCP 443 (443	always		
1	Virtual Server	DNS	0.0.0.0	UDP 53 / 53	always		
	Virtual Server	SMTP	0.0.0.0	TCP 25/25	alwavs		

The DI-824VUP can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DI-824VUP firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DI-824VUP are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling *Virtual Server*. Depending on the requested service, the DI-824VUP redirects the external service request to the appropriate server within the LAN network.

Name	The name referencing the virtual service.
Private IP	The server computer in the LAN network that will be providing the virtual services.
Protocol Type	The protocol used for the virtual service.
Private Port	The port number of the service used by the Private IP computer.
Public Port	The port number on the WAN side that will be used to access the virtual service.
Schedule	Select Always , or choose From and enter the time period dur- ing which the virtual service will be available.

Advanced > Application

		Н	igh-Speed 2	2.4GHz Wireles	ss Route
Но	me A	dvanced	Tools	Status	Help
Special Special	I Application Application is	1 used to run applica	ations that require	multiple connections	e.
10 A	C) Enabled 🔘 Dis	abled		
Name					
Trigger	Port	-			
Trigger	Туре	CP 💌			
Public F					
	ons				
Public	Fype T	CP 💌			3 6
Public 1 Specia	Type T	1 List	Dublis Davi	Ø (Apply Ca	3 G
Public 1	Fype T	CP V 1 List Trigger 6112	Public Port 6112	Apply Ca	3 G
Public 1	Fype Tr Fype Tr I Application me ttle.net	CP V List Trigger 6112 7175	Public Port 6112 51200-512		S G
Public 1 Specia Na Bal Dia Clu	Type T Type T me ttle.net J l	CP V List Trigger 6112 7175 2019	Public Port 6112 51200-512 2000-2035 2051,2069	Apply Ca 101,51210 1,2085.001-3030	3 G Incel Hel
Public 1 Specia Na Bat Dia COL Zor	Type T Type T Me the.net alpad J II N Gaming ne	CP v List Trigger 6112 7175 2019 47624	Public Port 6112 2000-2038 2051,2069 2300-2400	Apply Ca 201,51210 3,2050- 1,2085,3010-3030 0,28800-29000	3 G Incel Hel
Public 1 Specia Na Bal Dia Col Score PC	Type T Application me ttle.net JII N Gaming ne -to-Phone	CP v 1 List Trigger 6112 7175 2019 47624 12053	Public Port 6112 51200-512 2000-2035 2051,2069 2300-2400 12120,121	Apply Ca 201,51210 3,2050- 1,2085,3010-3030 0,28800-29000 22,24150-24220	Contraction of the second seco
Public 1 Specia Na Bal Dis Cor S Zor P C Q Qu	Type T Type T Me ttle.net Up I N Gaming ne -to-Phone ick Time	List Trigger 6112 7175 2019 47624 12053 554	Public Port 6112 51200-512 2000-2036 2300-2400 12120,121 6970-6995	201,51210 3,2050- 1,2085,3010-3030 0,28800-29000 2,22,4150-24220	e fi

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). *Special Applications* makes some of these applications work with the DI-824VUP. If you need to run applications that require multiple connections, specify the port normally associated with an application in the **Trigger** field, then enter the public ports associated with the trigger port into the **Incoming Ports** field.

At the bottom of the screen, there are already defined special applications. To use them, select one from the drop down list and select an ID number you want to use. Then click the "Copy to" button and the router will fill in the appropriate information to the list. You will then need to enable the service. If the mechanism of Special Applications fails to make an application work, try using DMZ host instead.

Note! Only one PC can use each Special Application tunnel.

- Enabled Select to activate the policy.
- **Trigger Port** This is the port used to trigger the application. It can be either a single port or a range of ports.
- Public Ports This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Using the Configuration Menu Advanced > Filter > IP Filter

Use IP (Internet Protocol) filters to allow or deny computers access to the Internet based on their IP address.



IP Filter

Use IP Filters to deny LAN IP addresses access to the internet.

Enabled or Disabled

Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy. (You can reactivate the policy later.)

IP Address

Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Port Range

Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Protocol

Select the protocol type to allow or deny certain types of IP addresses.

Schedule

Select **Always**, or choose **From** and enter the time period during which the IP filter policy will be in effect.

Advanced > Filter > MAC Filters

Home	Advanced	Tools	Status	Help
Filter	to allow or deny LAN use	re from accessin	a the Internet	
O IP Filters	OURI Blocking		g the memory	
MAC Filters	O Domain Blocking			
	o bonnan bioonning			
MAC Filters				
Use MAC addres	s to allow or deny comp	uters access to th	ie network.	
Disabled M	IAC Filters			
Only allow	computers with MAC add	trace listed heles	v to accord the notive	-
O Only allow	computers with MAC add	ress listed below	to access the netwo	in la
U Only deny	computers with who add	iless listed below	to access the networ	R.
Name				
MáC áddress			T	
DUOD OK				
DHCP Client	- select one		Jone	
			- V (9 G
			Apply Ca	ncel Hel
MAC Filter List		2		
Name	MAC Addres	S		

MAC (Media Access Control) Filters are used to allow or deny LAN (Local Area Network) computers from accessing the Internet and network by their MAC address.

At the bottom of the screen, there is a list of MAC addresses from the DHCP client computers connected to the DI-824VUP. To use them, select one from the drop down list. Then click the "Apply" button and the DI-824VUP will fill in the appropriate information to the list.

Disabled MAC Filter

Select this option if you do not want to use MAC filters.

Only allow computers with MAC address listed below to access the network Select this option to only allow computers that are in the list to access the network and Internet. All other computers will be denied access to the network and Internet.

Only deny computers with MAC address listed below to access the network

Select this option to only deny computers that are in the list to access the network and Internet. All other computers will be allowed access to the network and Internet.

MAC Address

Enter the **MAC Address** of the client that will be filtered.

Using the Configuration Menu Advanced > Filter > URL Blocking



Use URL Blocking to deny LAN computers from accessing specific web sites by its URL. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display.

Disabled URL Blocking

Select this option if you do not want to use URL Blocking.

Using the Configuration Menu Advanced > Filter > Domain Blocking



Use Domain Blocking to allow or deny computers access to specific Internet domains whether it is through www, ftp, snmp, etc.

Disabled Domain Blocking

Select this option if you do not want to use Domain Blocking.

Allow users to access all domains except "Blocked Domains"

Select this option to allow users to access the specified Internet domains listed below. Users will be denied access to all other Internet domains.

Deny users to access all domains except "Permitted Domains"

Select this option to deny users to access the specified Internet domains listed below. Users will be allowed access to all other Internet domains.

Using the Configuration Menu Advanced > Firewall

VUP	Home	Advance	ed Too	ls Stat	us	Help
	Firewall Rules	can be used to allo	w or deny traffic t	rom passing throug	gh the DI-824VU	JP.
	Name	O Enabled O Di	sabled			
intual Server	Action					
		Interface IP Start	IP Er	id Protoc	ol Port Rang	10
pplication	Source	* 🗸			and here and	
Eller	Destination	* ~		TCP	~	
MILLER	Schedule	O Alwaye		di china		
-		O From	Time 00 👽 00	V To 00 V 00	~	
Irewaii			ot V nuC yeh	Sun 🗸		
SNMP						0
					0 🕗	•
DDNS				A	oply Cancel	Help
	Firewall Rule	es List				
Routing	Action Nam	ne	Source	Destination	Protocol	
	Allow Allov	v to Ping WAN port	WAN,*	LAN,192.168.0.	1 ICMP,*	
and the second se	Deny Defa	iult	7,7	LAN,- 192.168.0.1	*,*	2
DMZ						

Firewall Rules is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

Enabled or Disabled

Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy (You can reactivate the policy later).

Name

Enter the name of the Firewall Rule.

Action

Select Allow or Deny to allow or deny traffic to pass through the DI-824VUP.

Source

Choose between a LAN or WAN source. An asterisk signifies the selection of both sources.

IP Start

The starting IP address for the filter policy. Leaving the field blank selects all IPs.

IP End

The ending IP address for the filter policy. Leaving the field blank sleects all IPs.

Destination

Choose between a LAN or WAN destination. An asterisk signifies the selection of both destinations.

Using the Configuration Menu Advanced > Firewall Continued

nome	Advance	ed Tool	s Status	i Help
Firewall Rule	i les is can be used to allo	w or deny traffic fr	om passing through t	ne DI-824VUP.
	O Enabled O Di	sabled		
Name				
Action	O Allow O Deny			
on	Interface IP Start	IP End	Protocol	Port Range
Source	· ·			
Destination	*		TCP 💌	
Schedule	O Always			
	O From	Time 00 🖌 : 00	✓ To 00 ✓ :00 ✓	
-	1000	day Sun 💌 to S	Sun 💌	
P				0 0
			Appl	v Cancel Hein
			- Abbr	y cuncer new
Firewall R	iles List			
Action N	ame low to Ping WAN port	Source WANT*	LAN 192 169 0 1 IC	MP *
	ow to ring twat port	***	LAN,- +.	·····, ⊡u
Deny D	aaut	Y	192.168.0.1	

IP Address

Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Protocol

Select one of the following protocols: TCP, UDP, or ICMP.

Port Range

Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Schedule

Select **Always**, or choose **From** and enter the time period during which the virtual service will be available.

Using the Configuration Menu Advanced > SNMP

/UP Home A	dvanced Tools	Status	Help
SNMP Use Simple Network I	danagement Protocol(SNMP) for DI-	824VUP managemen	t purposes.
SNMP Local	Enabled ODisable	i	
SNMP Remote	O Enabled 💿 Disable	ł	
Get Community	public		
cation Set Community	private		
IP1			
IP 2			
IP 3			
IP 4			
SNMP Version	O V1 O V2c		
MP			-
s		V	90
		Apply Ca	ncel Hel

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DI-824VUP. The DI-824VUP supports SNMP v1 or v2c.

Enable SNMP	(Simple Network Management Protocol.)
Local	LAN (Local Area Network).
Remote	WAN (Wide Area Network).
Get Community	Enter the password public in this field to allow "Read only" access to network administration using SNMP. You can view the network, but no configuration is possible wth this setting.
Set Community	Enter the password private in this field to gain "Read and Write" access to the network using SNMP software. The administrator can configure the network with this setting.
SNMP v1	Simple Network Management Protocol (SNMP) is an applica- tion layer protocol that facilitates the exchange of management information between nework devices.
SNMP v2	Enhanced version of SNMP v1 with additional protocol opera- tions such as UDP, IP, CLNS, DDP, and IPX.

Advanced > DDNS



DDNS (Dynamic Domain Name System) keeps dynamic IP addresses (*e.g.*, IP addresses assigned by a DHCP capable router or server) linked to a domain name. Users who have a Dynamic DNS account may use this feature on the DI-824VUP.

DDNS	When an IP address is automatically assigned by a DHCP server, DDNS automatically updates the DNS server. Select Disabled or Enabled .
Provider	Select from the pull-down menu.
Host Name	Enter the Host name.
Username/Email	Enter the username or email address.
Password/Key	Enter the password or key.

Using the Configuration Menu Advanced > Routing

Static routes can be added if you require specific routes within your internal network. These routes will not apply to the WAN (Internet) network.

P Rout	ome Adv	anced	ools	Status	Help
Use ti	e Routing Table for	routing purposes v	vithin your local ne	twork.	
Dyna	mic Routing 💿 Dis	able 🔿 RIPv1 🔿	RIPv2		
ver ID	Destination	Subnet Mask	Gateway	Нор	Enable
1					
2					
3					
4					
5					
6					
7					
8					
				-	
				V	9 6
				Annly C	ancel He

Dynamic Routing	Dynamic Routing Settings allow the VPN Router to route IP packets to another network automatically. The RIP protocol is applied, and broadcasts the routing information to other routers on the network regularly.
	By default, it is set to disable. Check to enable (RIPv1 / RIPv2) protocol.
RIP v1	Protocol in which the IP address is routed through the internet.
RIP v2	Enhanced version of RIP v1with added features such as Au- thentication, Routing Domain, Next Hop Fowarding, and Subnet- mask Exchange.
Destination	Enter in the IP of the specified network that you want to access using the static route.
Subnet Mask	Enter in the subnet mask to be used for the specified net work.
Gateway	Enter in the gateway IP address to the specified network.
Нор	Enter in the amount of hops it will take to the specified network.
Enable	Select this option for the specified static route to take effect.

Hop Count - In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

Advanced > DMZ

D-Link unding Networks for People		H	Ais igh-Speed	Plus (TREME 2.4GHz Wireles	G+ s Router
824VUP	Home	Advanced	Tools	Status	Help
	DMZ DMZ(Demilitariz the Internet.	ed Zone) is used to al	ow a single com	puter on the LAN to b	e exposed to
Virtual Server	IP Address	© Enabled ® Disa 192.168.0.	abled		
Application				0	3 🗘
Filter				Apply Ca	ncel Help
Firewall					
SNMP					
DDNS					
Routing					
DMZ					
Performance					

If you have a computer that cannot run Internet applications properly from behind the DI-824VUP, then you can allow that computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

Advanced > Performance

4VUP	Home	Advanced	Tools	Status	Help
	Wireless Perform These are the Wirel	iance ess Performance fea	atures for the AP(Access Point) portion.	
	Beacon Interval	100 (msec	;, range:1~1000,	default: 100)	
intual Server	DTIM Interval	3 (rang	e: 1~65535, defa	ult 3)	
	TX Rates	Auto 👻 (Mbps)			
plication	Wireless Mode	💿 mixed mode	O G mode		
	Authentication Type	• Open Syster	n 🔿 Shared Key	🕐 💿 Both	
Filter	SSID broadcast	🖲 Enable 🔘 🛛	Disable		
Firewall	8X	💿 Enable 🔘	Disable		
SNMP				Ø (3 0
DDNS				Apply C	ancel Help
louting					

- **Beacon Interval** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. **100** is the default setting and is recommended.
- **DTIM interval** (Delivery Traffic Indication Message) **3** is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **TX Rates** Select the data rate. Default is **1-2-5.5-11-22-54Mbps**.
- Wireless Mode Select either mix mode or G mode.
 - **Mixed Mode** The DI-824VUP will use either B or G mode depending on which mode has a stronger frequency.
 - **G Mode** The DI-824VUP will only use G mode.

Advanced > Performance (Continued)



Authentication Select Open system, Shared Key or Both.

Open System	The DI-824VUP will be visible to all devices on the network. This is
	the default setting.

Shared Key In this mode, in order to access the DI-824VUP on the network, the device must be listed in the MAC Address Control List.

Both In this mode, all devices on the network can access the DI-824VUP.

SSID Broadcast Enable is the default setting. Choose Enable to broadcast the SSID across the network. All devices on a network must share the same SSID (Service Set Identifier) to establish communication. Choose Disable if you do not wish to broadcast the SSID over the network.

8x Enable 8X Mode on the wireless client and the DI-824VUP to increase data transmission speed. 8X Mode will only work with wireless devices that also support 8X Mode.