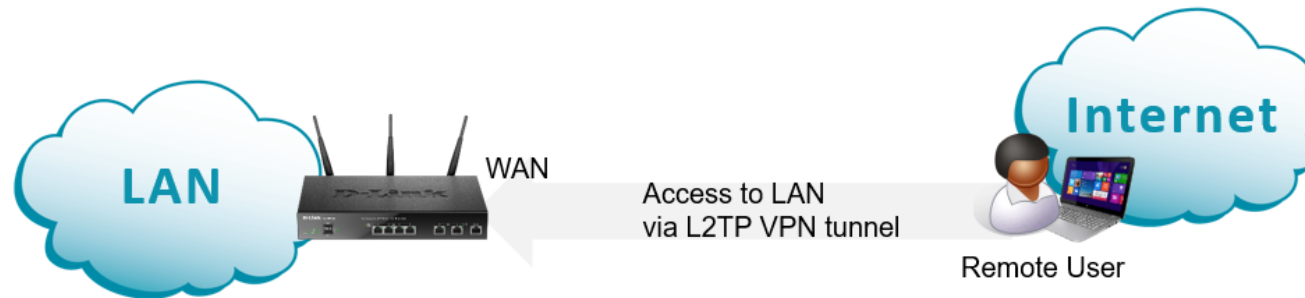


# L2TP VPN Service Setup Guide

## DSR-1000AC / DSR-500AC

Firmware 3.08B302C



Remote users can connect to the router using VPN client software and securely access LAN resources.

### Configuration Steps:

- Create VPN Policy.
- Enable L2TP Server.
- Add user database.

Step 1. Go to *VPN > IPSec VPN > Policies*.

Create a new IPSec Policy. Use the below example as a guide.

**IPSec Policy Configuration**

*General*

Policy Name	VPNtest
Policy Type	Auto Policy ▼
IP Protocol Version	IPv4 ▼
IKE Version	IKEv1 ▼
L2TP Mode	Gateway ▼
IPSec Mode	Transport Mode
Select Local Gateway	Dedicated WAN ▼
Remote Endpoint	FQDN ▼
IP Address / FQDN	0.0.0.0
Enable Mode Config	<input type="checkbox"/> OFF
Enable RollOver	<input type="checkbox"/> OFF
Protocol	ESP ▼
Enable Keepalive	<input type="checkbox"/> OFF

*Phase 1 (IKE SA Parameters)*

Exchange Mode	Main ▼
Direction / Type	Both ▼
Nat Traversal	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
NAT Keep Alive Frequency	20 Seconds
Local Identifier Type	Local Wan IP ▼
Remote Identifier Type	FQDN ▼
Remote Identifier	0.0.0.0

**Encryption Algorithm**

DES	<input type="checkbox"/> OFF	3DES	<input checked="" type="checkbox"/> ON
AES-128	<input type="checkbox"/> OFF	AES-192	<input type="checkbox"/> OFF
AES-256	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

**Authentication Algorithm**

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-256	<input type="checkbox"/> OFF	SHA2-384	<input type="checkbox"/> OFF
SHA2-512	<input type="checkbox"/> OFF		

Authentication Method:

Pre-Shared Key:  [Length: 8 - 49]

Diffie-Hellman (DH) Group:

SA-Lifetime:  [Default: 28800, Range: 300 - 2147483647] Seconds

Enable Dead Peer Detection:  OFF

Extended Authentication:

**Phase2-(Auto Policy Parameters)**

SA Lifetime:

**Encryption Algorithm**

DES	<input type="checkbox"/> OFF	NONE	<input type="checkbox"/> OFF
3DES	<input checked="" type="checkbox"/> ON	AES-128	<input type="checkbox"/> OFF
AES-192	<input type="checkbox"/> OFF	AES-256	<input type="checkbox"/> OFF
TWOFISH (128)	<input type="checkbox"/> OFF	TWOFISH (192)	<input type="checkbox"/> OFF
TWOFISH (256)	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

**Integrity Algorithm**

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-224	<input type="checkbox"/> OFF	SHA2-256	<input type="checkbox"/> OFF
SHA2-384	<input type="checkbox"/> OFF	SHA2-512	<input type="checkbox"/> OFF
PFS Key Group	<input type="checkbox"/> OFF		

Your new VPN Policy should look similar to this:

The screenshot shows the D-Link Unified Services Router (DSR-1000AC) web interface. The top navigation bar includes links for Status, Wireless, Network, VPN, Security, and Maintenance. The current page is titled "IPSec VPN Policies" and provides instructions on how to manage policies. Below the instructions is a table listing the configured policies.

VPN » IPSec VPN » Policies

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.

### IPSec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	VPNtest*	None	Auto Policy	Transport Mode	Any	Any	SHA1	3DES

Showing 1 to 1 of 1 entries

Navigation: First, Previous, 1, Next, Last

Step 2. Go to VPN > L2TP VPN > Server

Enable L2TP Server.

Specify the range of IP addresses you want to assign to the connecting clients (this range should be different from your LAN subnet).

As Authentication Database we are using "Local User Database" in this example.

**L2TP Server**

**Server Setup**

Enable L2TP Server: Enable IPv4

L2TP Routing Mode:  Nat  Classical

**Range of IP Addresses (Allocated to L2TP Clients)**

Starting IP Address: 192.168.3.1

Ending IP Address: 192.168.3.10

**Authentication Database**

Authentication: Local User Database

**Authentication Supported**

PAP: ON

CHAP: ON

MS-CHAP: ON

MS-CHAPv2: ON

**Encryption**

Secret Key: OFF

**User Time-out**

Idle TimeOut: 300 [Range: 300 - 1800] Seconds

Save Cancel

Step 3. Go to *Security > Authentication > User Database > Groups*

Add a new L2TP group.

Set User Type as "Network" and "L2TP".

**Group Configuration**

Group Name: l2tp

Description: l2tp

**User Type**

User Type:  Admin  Network  Guest

PPTP User:  OFF

L2TP User:  ON

Xauth User:  OFF

OpenVPN User:  OFF

SSLVPN User:  OFF

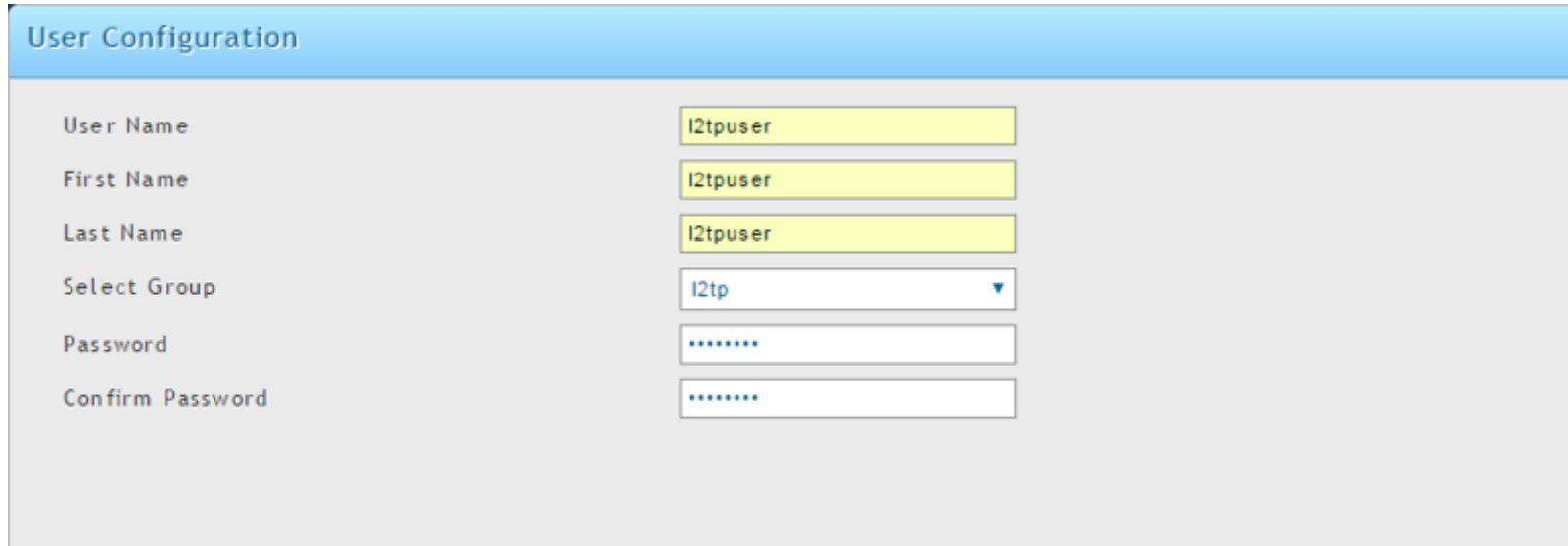
Captive Portal User:  OFF

Idle Timeout: 10 [Default: 10, Range: 1 - 999] Minutes

Step 4. Go to *Security > Authentication > User Database > Users*

Add new users for the group that you created in the previous step.

Specify the usernames and passwords.



The screenshot displays the 'User Configuration' web interface. It features a light blue header with the title 'User Configuration'. Below the header, there are six rows of configuration fields:

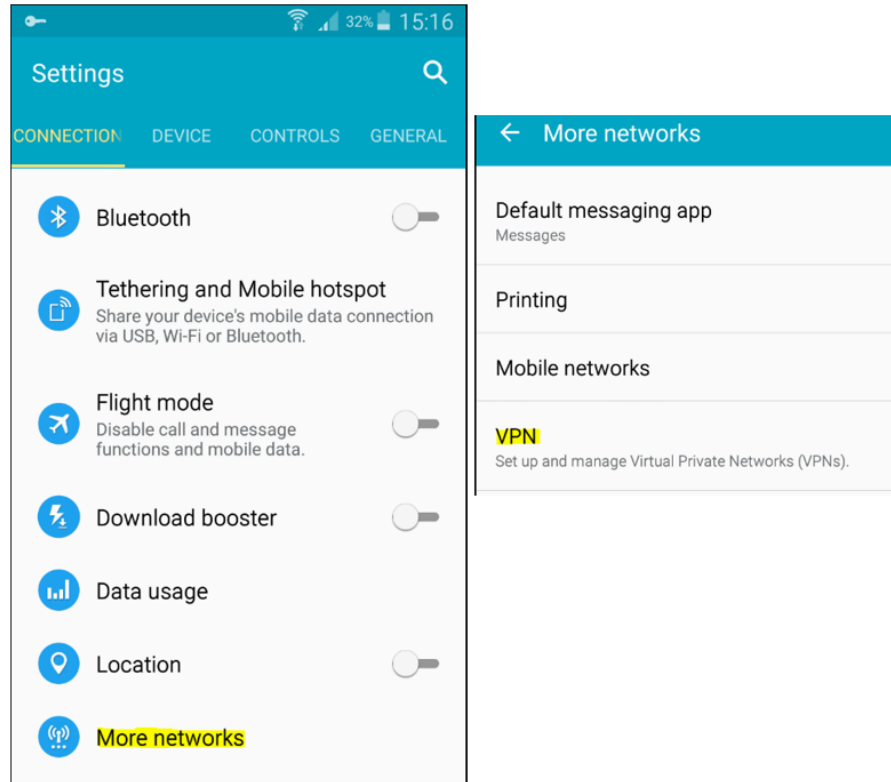
- User Name:** A text input field containing 'l2tpuser'.
- First Name:** A text input field containing 'l2tpuser'.
- Last Name:** A text input field containing 'l2tpuser'.
- Select Group:** A dropdown menu with 'l2tp' selected and a downward arrow.
- Password:** A text input field with seven dots representing a masked password.
- Confirm Password:** A text input field with seven dots representing a masked password.

Remote users should now be able to connect to the router and local network with their generic L2TP client.

## Remote Client Setup Example

The below example shows setup and connection process on an Android phone (Samsung Galaxy Note 3, Android ver. 5.0).

Go to Settings > Connections > More Networks > VPN.





Add a new L2TP/IPSec PSK Profile and enter the L2TP server settings:

*Server address* – the public IP address on the WAN port of your DSR-series router

*Pre-Shared Key* – the key you set in the router's IPSec Policy in Step 1.

**Add VPN**

Name  
DSR-1000AC

Type  
L2TP/IPSec PSK

Server address  
123.123.123.123

L2TP secret  
Not used

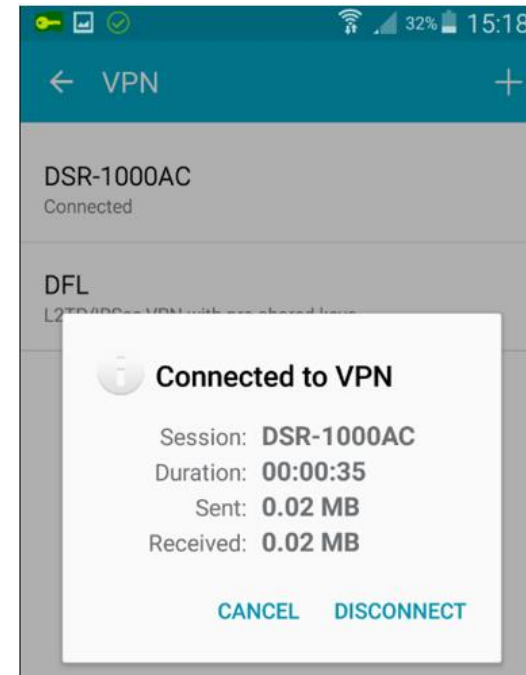
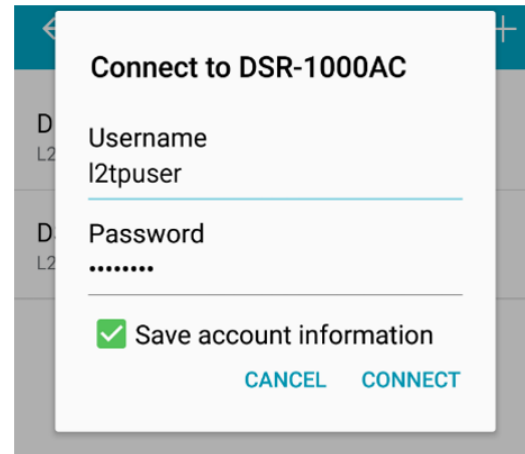
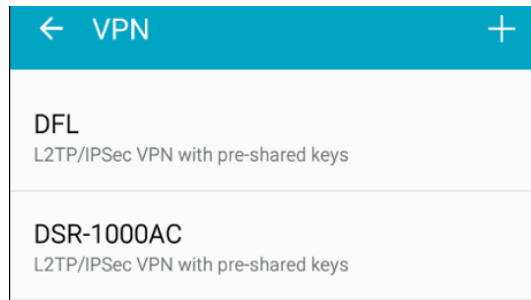
IPSec identifier  
Not used

IPSec pre-shared key  
.....

Show advanced options

CANCEL SAVE

Press the L2TP/IPSec Profile that you added. Enter the L2TP username and password (the user you added into the router's database in Step 4). Once connected, you should see a Key icon in the top left corner indicating successful secure connection.



End of Document