

DSR-250N/1000AC L2TP/IPSec VPN + Windows 10 Client

- ⇒ The DSR is already fully configured and has internet access
- ⇒ DSR has already the latest available Firmware installed
 - <ftp://ftp.dlink.de/dsr/>

1.) Create L2TP User

a. Create (ADD) new Group for L2TP

The screenshot displays the 'Groups List' page in the D-Link web interface. The page title is 'Security > Authentication > Internal User Database > Groups'. There are tabs for 'Get User DB', 'Groups', and 'Users'. A note states: 'This page shows the list of added groups to the router. The user can add, delete and edit the groups also. The Login policies, Browser Policies and IP Policies can only be configured for groups having admin and sslvpn privileges.'

The 'Groups List' table shows the following data:

Group Name	Description
ADMIN	Admin Group
GUEST	Guest Group

Below the table, it says 'Showing 1 to 2 of 2 entries'. There are navigation buttons: 'First', 'Previous', '1', 'Next', 'Last'.

A 'Group Configuration' dialog box is open, showing the configuration for a new group named 'L2TP'. The 'Description' is also 'L2TP'. Under 'User Type', the 'Network' radio button is selected. Other options include 'Admin' and 'Guest'. There are checkboxes for 'PPTP User', 'L2TP User', 'Xauth User', 'OpenVPN User', and 'SSLVPN User'. The 'L2TP User' checkbox is checked. The 'Idle Timeout' is set to '10' minutes, with a note '[Default: 10, Range: 1 - 999] Minutes'. A 'Save' button is at the bottom right of the dialog.

Below the dialog, the 'Groups List' page is shown again, now with three entries:

Group Name	Description
ADMIN	Admin Group
GUEST	Guest Group
L2TP	L2TP

It now says 'Showing 1 to 3 of 3 entries'.

b. Create User for L2TP

The screenshot shows the 'Users List' interface with a table of existing users:

User Name	Group Name	Login Status
admin	ADMIN	Enabled (LAN) Enabled (WAN)
guest	GUEST	Disabled (LAN) Disabled (WAN)

The 'User Configuration' dialog box is open, showing the following fields:

- User Name: L2TPUser
- First Name: L2TPUser
- Last Name: L2TPUser
- Select Group: L2TP (highlighted with a red box)
- Password: [masked]
- Confirm Password: [masked]

Define Username, First Name and Last Name to your liking.

Select the previously created L2TP Group and enter the Users password

⇒ This are the User credentials you later need to enter into Windows 10 while connecting

The screenshot shows the 'Users List' interface after successful user creation. A green message box at the top indicates 'Operation Succeeded'. The 'Users List' table now includes the newly created user:

User Name	Group Name	Login Status
admin	ADMIN	Enabled (LAN) Enabled (WAN)
guest	GUEST	Disabled (LAN) Disabled (WAN)
L2TPUser	L2TP	Enabled (LAN) Enabled (WAN)

2.) Enable L2TP Server

VPN » L2TP VPN » L2TP Server

L2TP allows an external user to connect to your router through the Internet, forming a VPN. This section allows you to enable/disable L2TP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.).

L2TP Server

Server Setup

Enable L2TP Server:

Operation Succeeded

L2TP allows an external user to connect to your router through the internet, forming a VPN. This section allows you to enable/disable L2TP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.).

L2TP Server

Server Setup

Enable L2TP Server:

L2TP Routing Mode: NAT Classical

Range of IP Addresses (Allocated to L2TP Clients)

Starting IP Address:

Ending IP Address:

Authentication Database

Authentication:

Authentication Supported

PAP: OFF

CHAP: OFF

MS-CHAP: ON

MS-CHAPv2: ON

Encryption

Secret Key: OFF

User Time-out

Idle Timeout: [Range: 300 - 1800] Seconds

Enable the L2TP IPv4 Server

Define the Routing Mode to your requirements.

Define an IP Range of maximum 20 IP Addresses outside your LAN Range.

Define the Security Authentication your device supports. (If you want to connect several different operating system (OS) you may need to add unsecure Methods like PAP or CHAP, depending on your OS

Define the IDLE Timeout.

3.) Create IPSec Policy

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.
Note: Policy with "" represents a Client Policy.

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
No data available in table								

Showing 0 to 0 of 0 entries

[Add New IPSec Policy](#)

IPSec Policy Configuration

General

Policy Name: VPN

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: OFF

[Save](#)

IPSec Policy Configuration

Enable Mode Config: OFF

Enable RollOver: OFF

Protocol: ESP

Enable Keepalive: OFF

Phase1(IKE SA Parameters)

Exchange Mode: Main

Direction / Type: Both

Nat Traversal: ON

NAT Keep Alive Frequency: 20 Seconds

Local Identifier Type: Local Wan IP

Remote Identifier Type: FQDN

Remote Identifier: 0.0.0.0

[Save](#)

IPSec Policy Configuration

Remote Identifier: 0.0.0.0

Encryption Algorithm

DES: OFF

AES-128: ON

AES-256: OFF

BLOWFISH: OFF

CAST128: OFF

3DES: ON

AES-192: OFF

Authentication Algorithm

MD5: OFF

SHA2-256: OFF

SHA2-512: OFF

SHA-1: ON

SHA2-384: OFF

Authentication Method: Pre-Shared Key

[Save](#)

IPSec Policy Configuration

Authentication Method:

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

Diffie-Hellman (DH) Group:

SA-Lifetime: [Range: 300 - 604800] Seconds

Enable Dead Peer Detection: OFF

Extended Authentication:

Phase2 (Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm

DES: OFF None OFF

3DES: ON AES-128 ON

AES-192: OFF AES-256: OFF

TWOFISH (128): OFF TWOFISH (192): OFF

TWOFISH (256): OFF

BLOWFISH: OFF

CAST128: OFF

Integrity Algorithm

MDS: OFF SHA-1: ON

SHA2-224: OFF SHA2-256: OFF

SHA2-384: OFF SHA2-512: OFF

PFS Key Group: OFF

IPSec Policy Configuration

DES: OFF None: OFF

3DES: ON AES-128: ON

AES-192: OFF AES-256: OFF

TWOFISH (128): OFF TWOFISH (192): OFF

TWOFISH (256): OFF

BLOWFISH: OFF

CAST128: OFF

Integrity Algorithm

MDS: OFF SHA-1: ON

SHA2-224: OFF SHA2-256: OFF

SHA2-384: OFF SHA2-512: OFF

PFS Key Group: OFF

IPSec Policies List

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

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	VPN*	None	Auto Policy	Transport Mode	Any	Any	SHA1	3DES AES-128

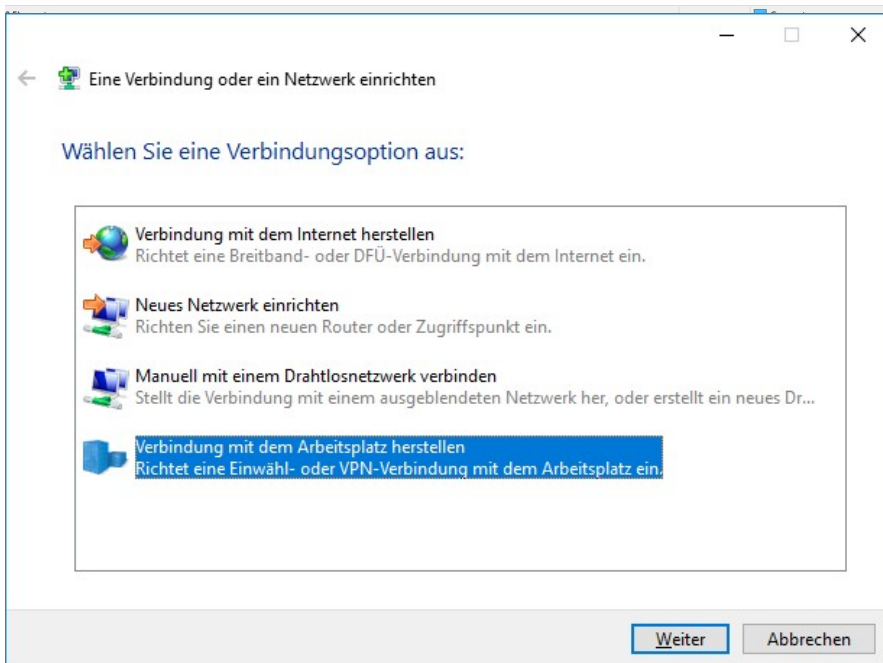
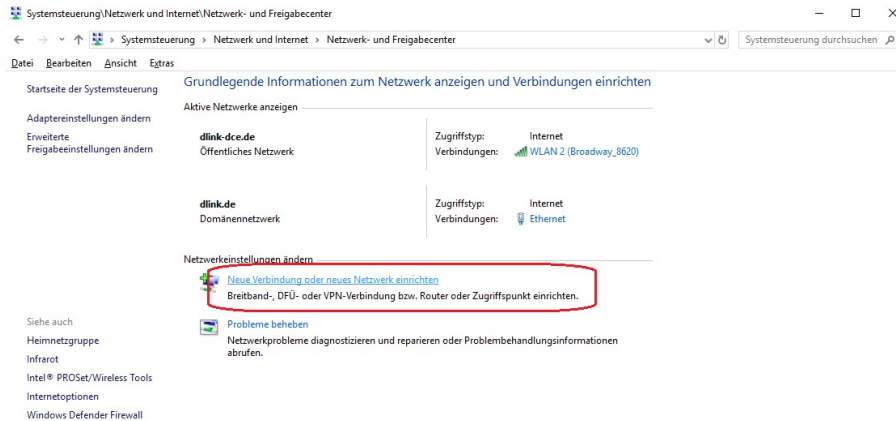
Showing 1 to 1 of 1 entries

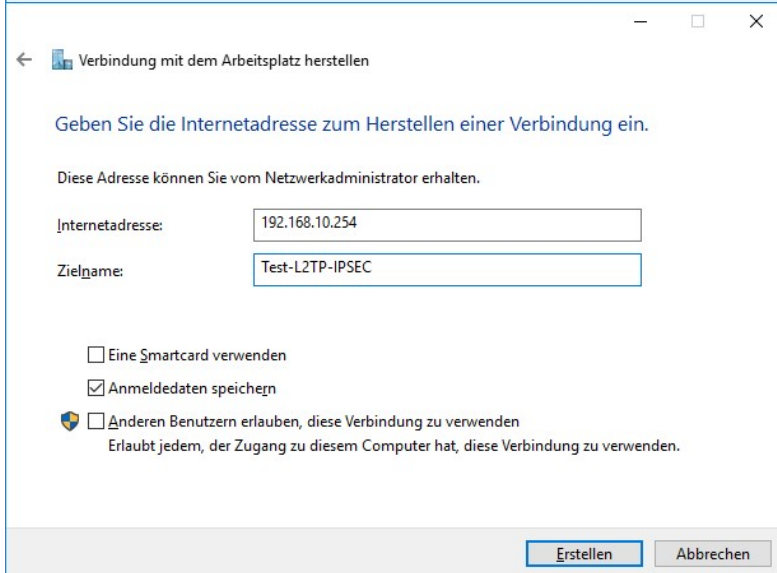
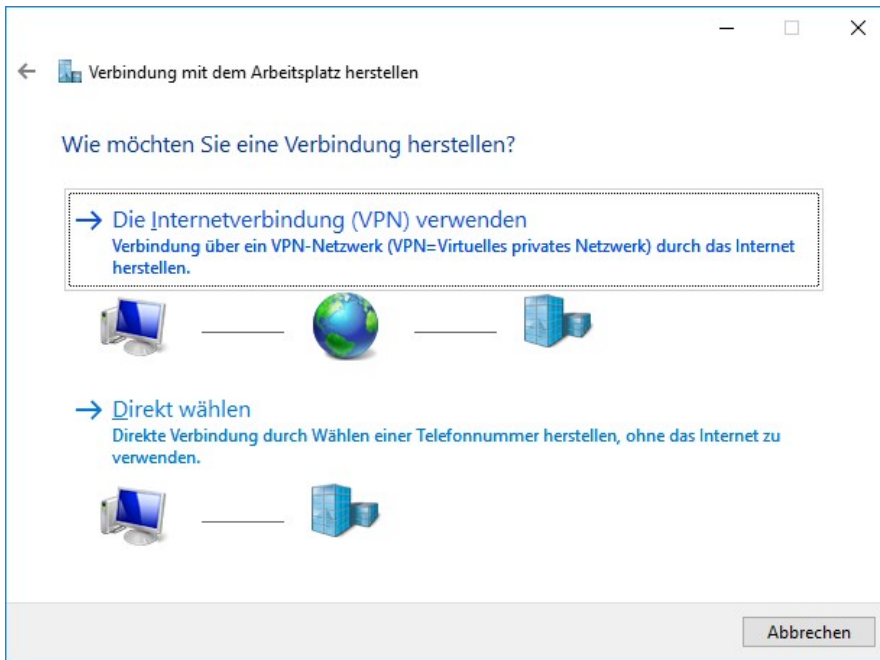
1

The Pre-Shared Key you later need to enter at Windows 10 VPN creation site.

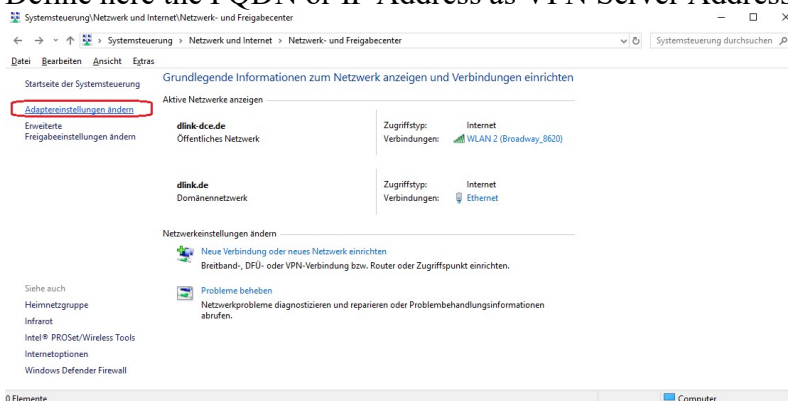
4.) Setup Windows 10

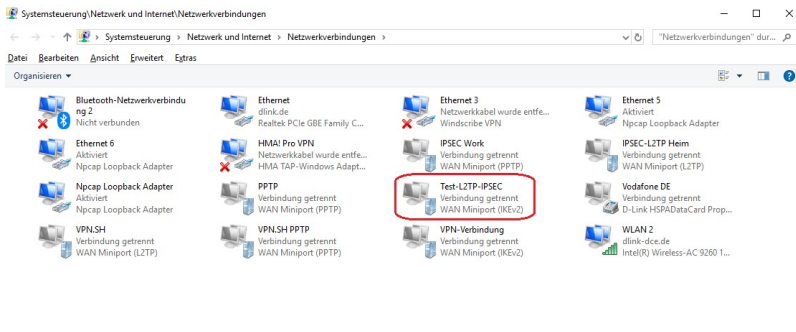
a. Go to Network settings and create a new connection



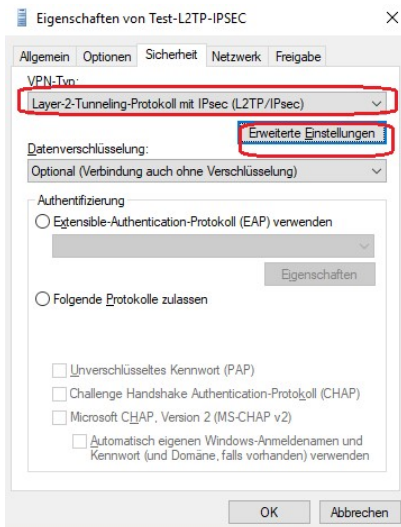
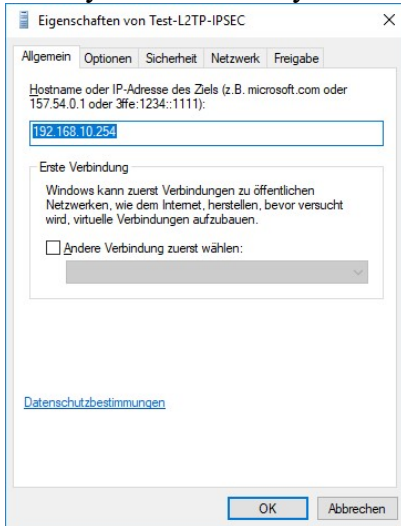


Define here the FQDN or IP Address as VPN Server Address

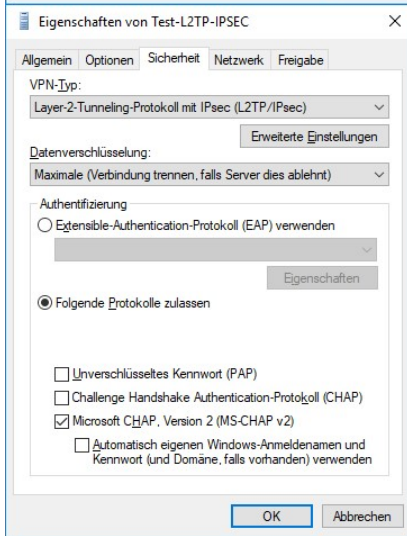
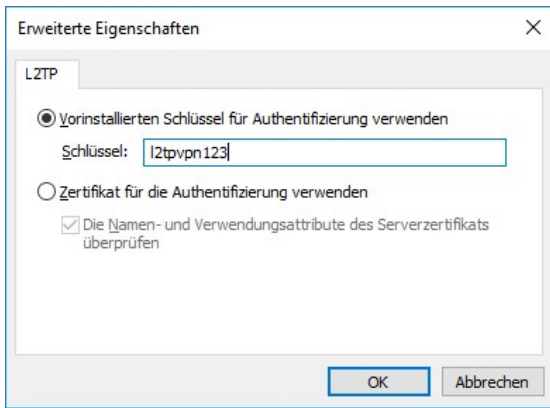




Modify now the freshly created VPN, since it's currently on auto and not L2TP/IPSec.



Change the existing “auto” value to L2TP with IPsec and then modify/enter within the extended settings the previously created IPsec Policy Sectet.



5.) Connect client

