

# L2PT VPN on RV345 for Windows 10

This Manual is based in Windows 10 version 20H2 and Image version 1.0.03.21 on the router.

1. (optional) Create a group for users who are going to use VPN

The screenshot displays the 'User Groups' configuration page in a web interface. The left sidebar contains navigation options: Getting Started, Status and Statistics, Administration, System Configuration (highlighted), System, Time, Log, Email, User Accounts, and User Groups (highlighted).

The main content area is titled 'User Groups' and features an 'Apply' button and a 'Cancel' button. Below the title is a 'User Groups Table' with a '+' icon for adding a new group and a trash icon for deleting. The table lists existing groups and their configurations:

<input type="checkbox"/>	Group	Web Login/NETCONF/RESTCONF	S2S-VPN	EzVPN/3rd Party	SSL VPN	PPT
<input type="checkbox"/>	admin	Admin	Disabled	Disabled	SSLVPND...	Eni
<input type="checkbox"/>	guest	Disabled	Disabled	Disabled	Disabled	Dis

Below the table is an 'Overview' section for a new group. The 'Group Name' field is set to 'VPN\_Users'. Below this is a 'Local User Membership List' table:

#	Join	User Name	Joined Groups *
1	<input type="checkbox"/>	cisco	admin
2	<input type="checkbox"/>	guest	guest

- (optional) Create one or more user(s) for that group.

**User Accounts** [Apply] [Cancel]

The new password must be different than the current one. [Enable]

Password Aging Time:  days(Range: 0 - 365, 0 means never expire)

### Local Users

Local User Membership List

#	User Name	Group
1	cisco	admin
2	guest	guest

**User Accounts** [Apply] [Cancel]

### Add User Account

The current minimum requirements are as follows.

- Minimal password length: 8
- Minimal number of character classes: 3
- The new password must be different than the current one

User Name:

New Password:  ( Range: 8 - 127 )

New Password Confirm:

Password Strength Meter:

Group:

- Create a new IPSec profile for the L2TP server

**IPSec Profiles** [Apply] [Cancel]

Global IPSec:  Enable

### IPSec Profiles Table

Name	IKE Version	Policy	In Use
Default	IKEv1	Auto	Yes
Amazon_Web_Services	IKEv1	Auto	No
Microsoft_Azure	IKEv1	Auto	No

- Here we are going for the high security possible at this time. If you need to make different choices, apply these to the Windows 10 part of this manual.

The screenshot shows the 'IPSec Profiles' configuration page. The left sidebar contains a navigation menu with the following items: Administration, System Configuration, WAN, LAN, Routing, Firewall, VPN (highlighted), VPN Status, IPsec Profiles (highlighted), Site-to-Site, Client-to-Site, Teleworker VPN Client, PPTP Server, L2TP Server, GRE Tunnel, SSL VPN, VPN Passthrough, Security, QoS, Configuration Wizards, and License.

The main content area is titled 'IPSec Profiles' and features an 'Add a New IPsec Profile' section. The configuration options are as follows:

- Profile Name:** Most\_Secure\_Win10
- Keying Mode:**  Auto  Manual
- IKE Version:**  IKEv1  IKEv2

**Phase I Options:**

- DH Group:** Group14 - 2048 bit
- Encryption:** AES-256
- Authentication:** SHA2-256
- SA Lifetime:** 28800 sec. (Range: 120 - 86400, Default: 28800)

**Phase II Options:**

- Protocol Selection:** ESP
- Encryption:** AES-256
- Authentication:** SHA2-256
- SA Lifetime:** 3600 sec. (Range: 120 - 28800, Default: 3600)
- Perfect Forward Secrecy:**  Enable
- DH Group:** Group14 - 2048 bit

Buttons for 'Apply' and 'Cancel' are located at the top right of the configuration area.

Note: AH Protocol is not supported by Win10. Also, if you cannot select DH Group 14, you need to update your router.

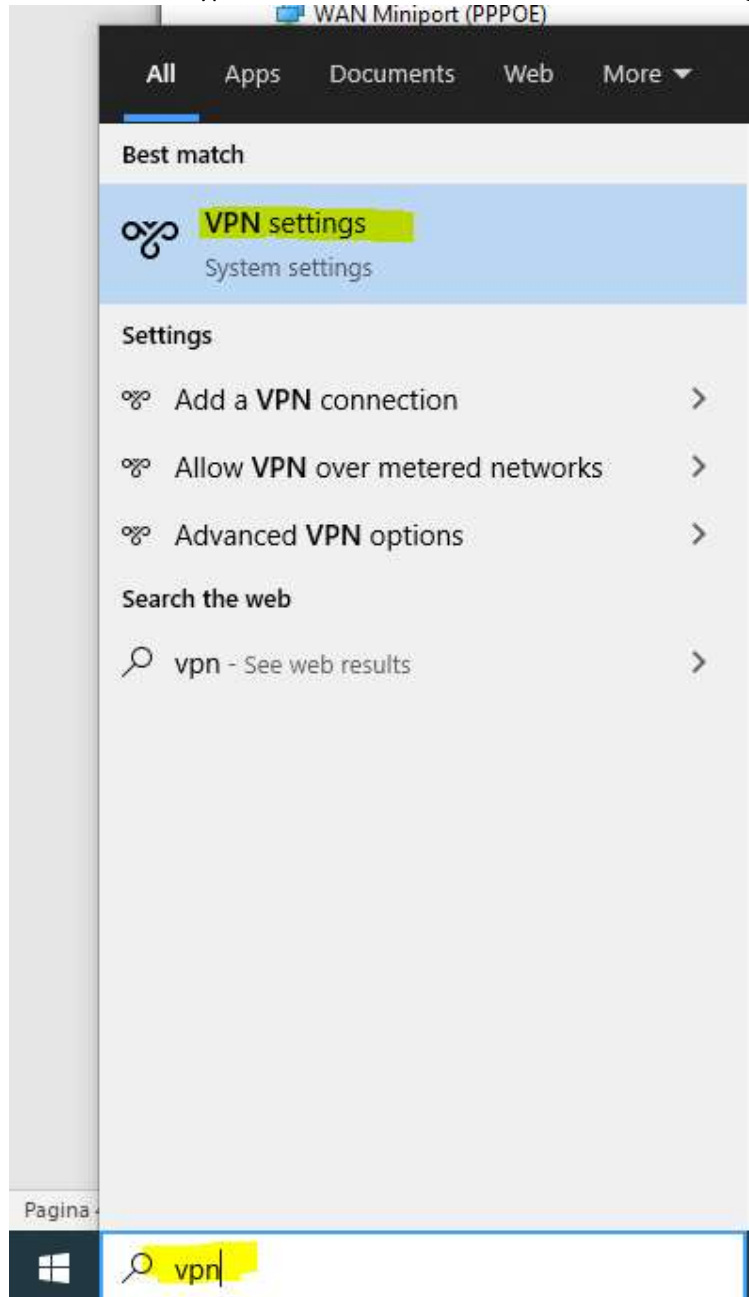
5. Now turn on the L2TP VPN server in fill in some parameters to your liking. An Ip range the users gonna use, DNS servers you like. Then select the IPsec Profile you created for this connection, optionally select the Usergroup you may have created, and fill in some pre-

shared key you made up.

The screenshot shows the configuration page for an L2TP Server. On the left is a dark sidebar with a menu containing: Status and Statistics, Administration, System Configuration, WAN, LAN, Routing, Firewall, VPN (highlighted), VPN Status, IPSec Profiles, Site-to-Site, Client-to-Site, Teleworker VPN Client, PPTP Server, L2TP Server (highlighted), GRE Tunnel, SSL VPN, VPN Passthrough, Security, and QoS. The main content area is titled 'L2TP Server' and includes an 'Apply' button and a 'Cancel' button. The configuration options are: L2TP Server:  On  Off; MTU: 1400 bytes (Range: 128-1400, Default: 1400); Address Pool: Start IP Address: 192.168.5.1, End IP Address: 192.168.5.50, DNS1 IP Address: 8.8.8.8, DNS2 IP Address: (empty); User Authentication: a list with 'admin' and 'VPN\_Users' (checked); IPSec:  On  Off; IPSec Profile: Most\_Secure\_Win10; Pre-shared Key: (masked with dots); Show Pre-shared Key:  Enable.

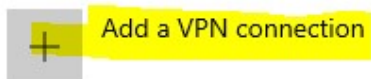
6. Ok, the server is configured now. On to Windows 10.

7. In Windows 10, type VPN in the searchbar, en click on 'VPN Settings'



8. Click on the + to create an new Connection

VPN



9. Now fill in like in the picture. Make up some Connection name, at Server Name of Address fill in the IP-address of the WAN Interface on the RV345 you intent to use. A Pre-shared key fill in the key you made up at step 5. Optionally, you can fill in the user name and password of the user you created at step 2.

## Add a VPN connection

VPN provider  
Windows (built-in) ▾

Connection name  
RV345

Server name or address  
123.123.123.123

VPN type  
L2TP/IPsec with pre-shared key ▾

Pre-shared key  
●●●●●●●●

Type of sign-in info  
User name and password ▾

User name (optional)  
[Empty text box]

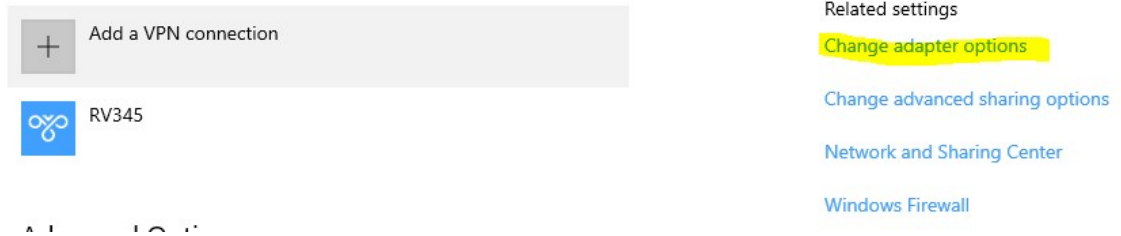
Password (optional)  
[Empty text box]

Remember my sign-in info

Save Cancel

10. When returned in the previous windows, select 'Change Adapter Options'

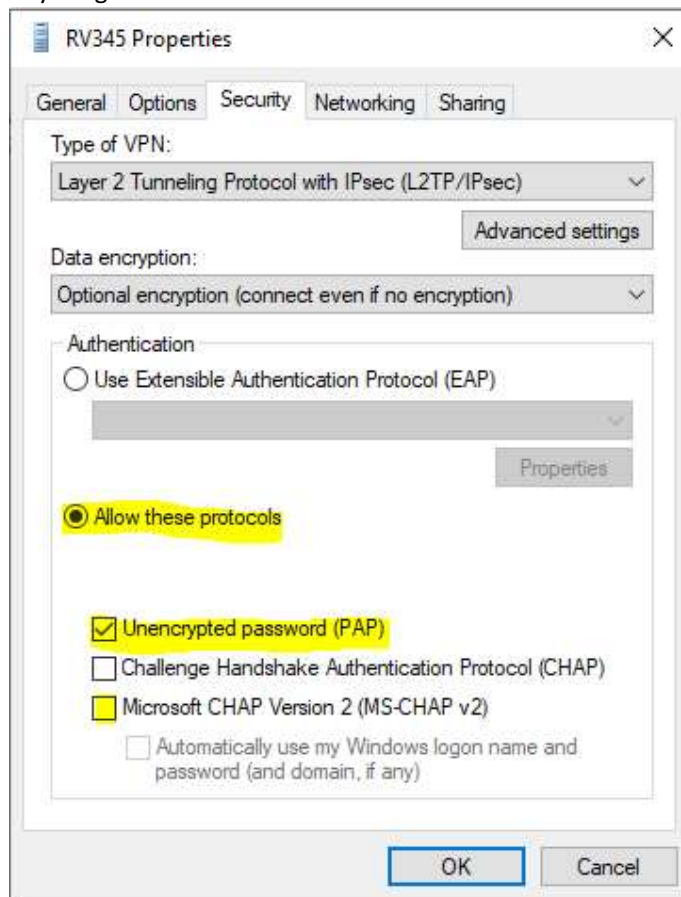
## VPN



11. Select the Connection you just created, and click 'Change settings of this connection'

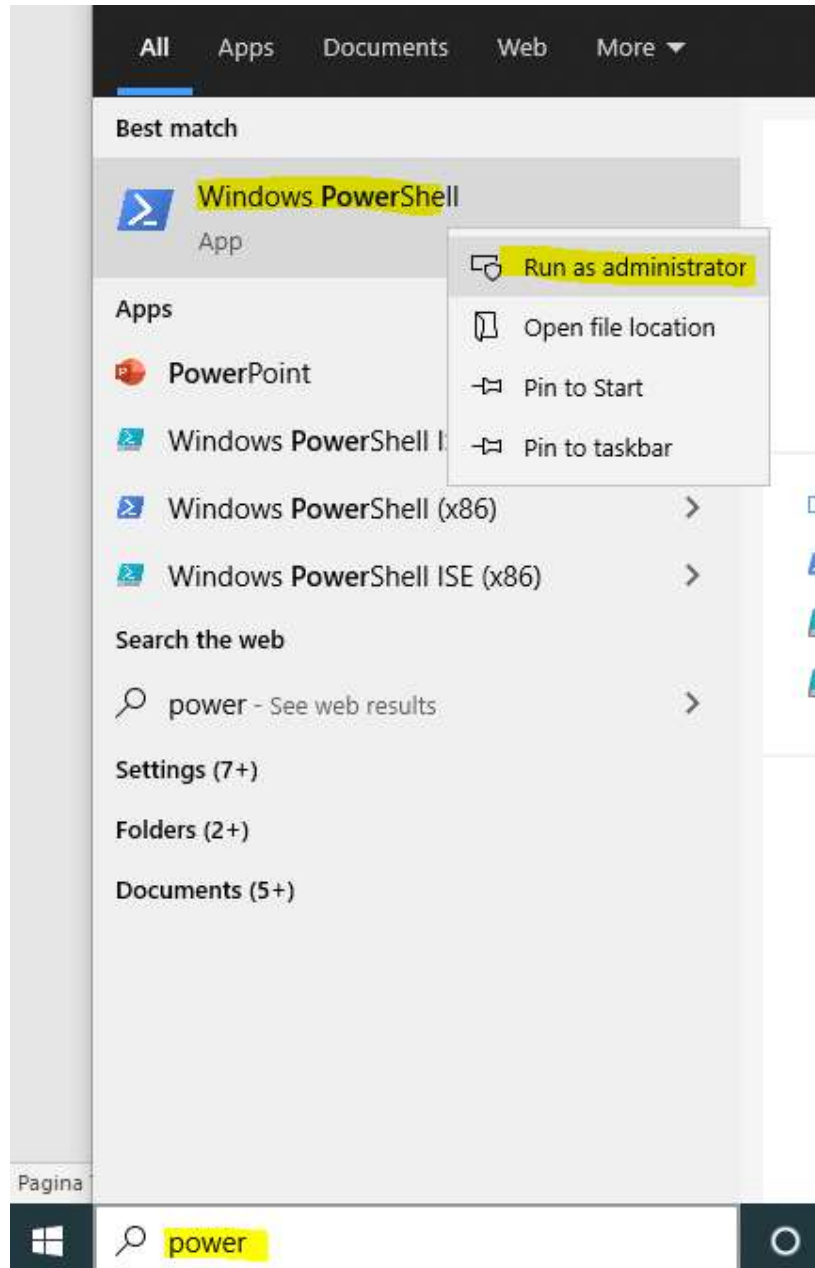


12. Select TAB 'Security' In there, select 'Allow these protocols' and check PAP, uncheck anything else.



13. Now we need to configure the IPSEC config built-in Win10. We need to do this by using Powershell. Type Powershell in the searchbar, right-click on 'Windows-Powershell' and

select 'Run as administrator'.



14. In the window, execute this command:

```
Set-VpnConnectionIPsecConfiguration -ConnectionName "RV345" -  
AuthenticationTransformConstants SHA256128 -CipherTransformConstants AES256 -  
EncryptionMethod AES256 -IntegrityCheckMethod SHA256 -PfsGroup PFS2048 -DHGroup  
Group14 -PassThru -Force
```

Where **RV345** is the name of your connection.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

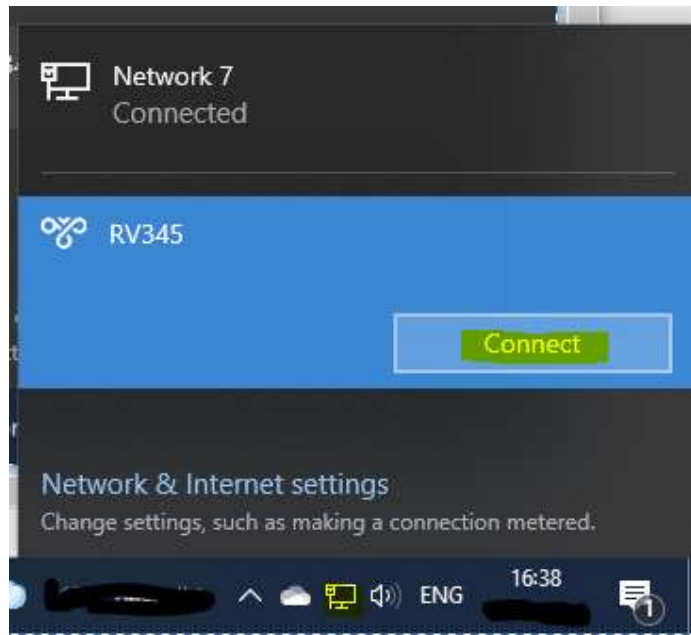
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Set-VpnConnectionIPsecConfiguration -ConnectionName "RV345" -AuthenticationTransformConstants SHA256128 -CipherTransformConstants AES256 -EncryptionMethod AES256 -IntegrityCheckMethod SHA256 -PfsGroup PFS2048 -DHGroup Group14 -PassThru -Force

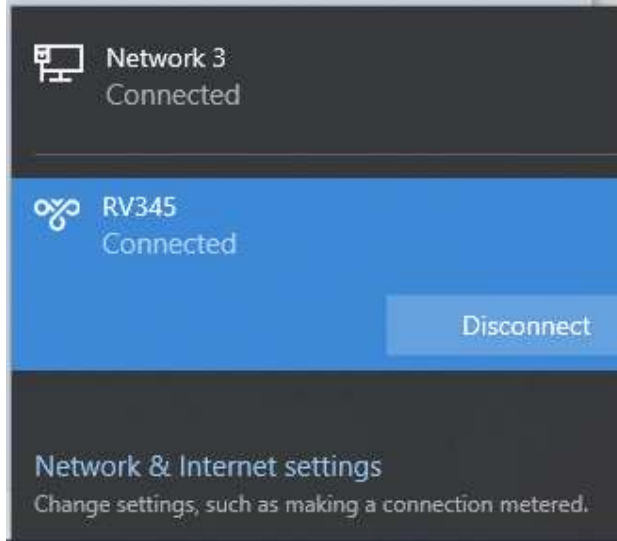
AuthenticationTransformConstants : SHA256128
CipherTransformConstants         : AES256
DHGroup                          : Group14
IntegrityCheckMethod             : SHA256
PfsGroup                         : PFS2048
EncryptionMethod                 : AES256

PS C:\WINDOWS\system32>
```

15. Now click on the network/wifi icon on the Taskbar, and select your VPN Connection, and click 'connect'



16. Enter Username/password if/when prompted. Windows 10 should connect now.



## BONUS: Command Shell parameters to RV345 IPSEC mapping table

I Made this table if you need to change the encryption parameters for some reason. You can use this to vary in the Powershell command as in step 14. Maybe it's redundant, IDK. Do/think at is as you please.

Phase I options		
Name	Option	Matching Powershell parameter
DH Group	Group 2 - 1024 bits	-DHGroup Group2
	Group 5 - 1536 bits	NA
	Group 14 - 2048 bits	-DHGroup Group14
Encryption	3DES	-EncryptionMethod DES3
	AES-128	-EncryptionMethod AES128
	AES-192	-EncryptionMethod AES192
	AES-256	-EncryptionMethod AES256
Authentication	MD5	-IntegrityCheckMethod MD5
	SHA1	-IntegrityCheckMethod SHA1
	SHA2-256	-IntegrityCheckMethod SHA256
Phase II Options		

Name	Option	Matching Powershell parameter
Protocol Selection	ESP	{Default}
	AH	NA
Encryption	3DES	-CipherTransformConstants DES3
	AES-128	-CipherTransformConstants AES128
	AES-192	-CipherTransformConstants AES192
	AES-256	-CipherTransformConstants AES256
Authentication	MD5	NA
	SHA1	-AuthenticationTransformConstants SHA196
	SHA2-256	-AuthenticationTransformConstants SHA256128
DH Group	Group 2 - 1024 bits	-PfsGroup PFS2
	Group 5 - 1536 bits	NA
	Group 14 - 2048 bits	-PfsGroup PFS2048

Some Other interesting parameters to be used in Set-VpnConnectionIPsecConfiguration:

- -RevertToDefault : Sets everything back to default, whatever that may be. You need to specify the connection name, or you will be asked for it.
- (get-VPNConnection).ipsecCustomPolicy (straight from the prompt) shows your current configured IPSEC settings. Does not show anything if everything is still or again 'default'.